DEPENDENCIA SOLICITANTE:	**DIRECCIÓN DE GESTIÓN JURÍDICA DE TIERRAS** **DIRECCIÓN DE ASUNTOS ÉTNICOS** **DIRECCIÓN DE ACCESO A TIERRAS** **SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS**
FECHA:	Julio de 2026

I. DESCRIPCIÓN DE LA CONTRATACIÓN

Brindar una solución integral para diferentes líneas de servicios y componentes tecnológicos que permitan garantizar la continuidad y adecuada operación de los Sistemas de Información de Tierras de la ANT y servicios conexos.

Alcance Objeto:

La Agencia Nacional de Tierras requiere garantizar el correcto ejercicio de las actividades propias de los servicios prestados por los centros de operación de red y seguridad, el monitoreo, la detección de amenazas, la gestión de incidentes, el análisis y gestión de vulnerabilidades, de los componentes, aplicaciones y servicios que hacen parte o están implementados sobre la infraestructura tecnológica de la Entidad.

De acuerdo con lo expuesto la Entidad pretende adquirir una solución integral de diferentes servicios y componentes que se ejecutarán de manera paralela a través de tres líneas de servicio que se detallan a continuación:

1. **Línea de servicio de Colocation (Centro de datos principal externo):** Es el servicio que brinda el alojamiento de componentes de la infraestructura tecnológica de la ANT que actualmente se encuentra operando en un centro de datos externo - NEBULA: servidores, equipos de seguridad, unidades de almacenamiento y demás componentes donde se encuentran implementadas las aplicaciones, bases de datos, componentes de georreferencia, micrositios con los que cuenta la entidad (internet, intranet) y demás aplicaciones para la operación de la entidad.

2. **Línea de servicios de monitoreo a la infraestructura TIC NOC/SOC**: Es el servicio que permite la prestación del servicio de monitoreo, correlación y reporte de eventos de seguridad en las plataformas e infraestructura on-premise y en nube y el monitoreo de las diferentes herramientas de seguridad de la Agencia, generando, y documentando las alertas, generando recomendaciones técnicas de remediación y generando informes semanales y mensuales de los eventos de Seguridad de la Información y ciberseguridad. La correlación de eventos se realizará en los sistemas de información de la Agencia dispuestos para ello y se utilizarán las matrices de escalamiento requeridas para el servicio utilizando las severidades descritas por tipo de sistema de información o de activo de información afectado, cumpliendo los ANS descritos. El servicio apoyará, las futuras integraciones de herramientas de seguridad y de infraestructura que se empiecen a utilizar por parte de la entidad durante la ejecución del contrato.

3. **Línea de conectividad de redes**: Es el servicio que permite la interconexión de alta velocidad entre las sedes de la ANT, donde se encuentran las Unidades de Gestión Territorial (UGT) y los centros de datos principales de la entidad. Este servicio incluye tecnologías contemporáneas de conectividad como INTERNET CORPORATIVO, MPLS, SERVICIO DE CONECTIVIDAD SATELITAL DE ÓRBITA BAJA (LEO) PARA UBICACIÓN FIJA, CONECTIVIDAD MÓVIL 3G – 4G – 5G y ENLACES SATELITALES DE ORBITA BAJA PORTÁTILES – MOVILIDAD TERRESTRE, entre otras. El servicio permitirá el funcionamiento adecuado de los sistemas de información, así mismo el acceso a ellos desde los diferentes puntos del territorio.

Descripción de la necesidad

Necesidad institucional de la SSIT

La Agencia Nacional de Tierras (de ahora en adelante ANT), es una agencia estatal de naturaleza especial, del sector descentralizado de la Rama Ejecutiva del Orden Nacional, con personería jurídica, patrimonio propio y autonomía administrativa, técnica y financiera, adscrita al Ministerio de Agricultura y Desarrollo Rural y establecida como la máxima autoridad de las tierras de la Nación en los temas de su competencia, la cual fue creada bajo el Decreto 2363 del 7 de diciembre de 2015.

En este sentido, de conformidad con lo dispuesto en el artículo 3° del mencionado Decreto, su objeto consiste en: "(…) *ejecutar la política de ordenamiento social de la propiedad rural formulada por el Ministerio de Agricultura y Desarrollo Rural, para lo cual deberá gestionar el acceso a la tierra como factor productivo, lograr la seguridad jurídica sobre esta, promover su uso en cumplimiento de la función social de la propiedad y administrar y disponer de los predios rurales de propiedad de la Nación".*

De igual forma, en el marco del Plan Nacional de Desarrollo 2022-2026, adoptado mediante la Ley 2294 de mayo de 2023 *"Colombia Potencia Mundial de la Vida"* y teniendo en cuenta los propósitos del Gobierno en materia de reforma rural integral y la política de tierras, el Gobierno Nacional a través del Ministerio de Agricultura y Desarrollo Rural, buscó fortalecer la capacidad institucional de la Agencia Nacional de Tierras en las diferentes regiones del país, mediante un enfoque de atención territorial; razón por la cual, la entidad cuenta con Unidades de Gestión Territorial (de ahora en adelante UGT) y Puntos de Atención de Tierras (PAT), los cuales son instrumentos operativos de la gestión misional de la ANT, y funcionan de manera complementaria y articulada con las citadas Unidades, requiriendo para esta articulación elementos tecnológicos que faciliten esta labor establecidos como enlaces entre el nivel territorial y el nivel central y los cuales tendrán como funciones las establecidas en el artículo 28 del Decreto 2363 de 2015, así como las demás que les haya señalado la ley, aquellas que le sean asignadas y las que les correspondan por su naturaleza; de esta forma, se permitirá atender los procedimientos administrativos a su cargo de una manera descentralizada, coordinada y priorizada de acuerdo con las características propias de cada territorio, con el fin de garantizar la atención de los usuarios en diferentes municipios del país.

En virtud de lo expuesto, la Dirección General de la Agencia Nacional de Tierras, presentó ante el Consejo Directivo de la entidad, propuesta para la aprobación de nuevas Unidades de Gestión Territorial - UGT´s a nivel nacional, en los términos de lo señalado en los artículos 9 y 28 del Decreto Ley 2363 de 2015, la cual, mediante Acuerdo No. 251 del 23 diciembre de 2022 del Consejo Directivo de la Agencia Nacional de Tierras – ANT, se aprobó la creación de veintitrés (23) Unidades de Gestión Territorial - UGT adicionales a las nueve (9) ya existentes.

Dicho esto, actualmente la Agencia Nacional de Tierras cuenta con cuatro (4) sedes a nivel central en la ciudad de Bogotá D.C. (CAN, Chapinero, Centro y la Bodega Américas); y a nivel territorial cuenta con veintinueve (29) UGT´s y cinco (5) sedes alternas en los municipios de Puerto López y San Martín – Meta, Carmen de Bolívar – Bolívar, Barrancabermeja - Santander y Apartadó - Antioquia, distribuidos de la siguiente manera:

No.	SEDE - Unidad de Gestión Territorial -UGT	CIUDAD
1	ANTIOQUIA	Apartadó
		Medellín
2	ARAUCA	Arauca
3	ATLÁNTICO	Barranquilla
4	BOLÍVAR	Cartagena de Indias
		Carmen de Bolivar
5	BOYACÁ	Tunja
6	CALDAS	Manizales
7	CAQUETÁ	Florencia
8	CASANARE	Yopal
9	CAUCA	Popayán
10	CESAR	Valledupar
11	CHOCÓ	Quibdó
12	CÓRDOBA	Montería
13	CUNDINAMARCA	BOGOTÁ D.C.
14	GUAINÍA	Puerto Inírida
15	GUAVIARE	San José del Guaviare
16	LA GUAJIRA	Riohacha
17	HUILA	Neiva
18	MAGDALENA	Santa Marta
19	META	Puerto López
		San Martin
		Villavicencio

20	NARIÑO	Pasto
21	NORTE DE SANTANDER	San José de Cúcuta
22	PUTUMAYO	Mocoa
23	QUINDIO	Armenia
24	RISARALDA	Pereira
25	SANTANDER	Bucaramanga
		Barrancabermeja
26	SUCRE	Sincelejo
27	TOLIMA	Ibagué
28	VALLE DEL CAUCA	Cali
29	VICHADA	Puerto Carreño

Esta distribución también obedeció al cumplimiento de uno de los pilares trazados por parte del Gobierno Nacional a través del Ministerio de Agricultura y Desarrollo Rural y la Agencia Nacional de Tierras, que consistía en: i) la adjudicación de uno punto cinco (1.5) millones de hectáreas; ii) la formalización de tres punto nueve (3.9) millones de hectáreas y la implementación; y iii) la puesta en marcha del catastro multipropósito.

Ahora bien, de acuerdo con lo señalado en el Plan Nacional de Desarrollo 2022-2026 *"Colombia Potencia Mundial de la Vida*" y de acuerdo con los objetivos estratégicos asignados al Sector Agricultura, es necesaria la generación de instrumentos que propendan por una transformación mediante la cual se adopten tecnologías digitales para mejorar sus operaciones, procesos y modelos de negocio, con el fin de cumplir las metas que se pactaron en el acuerdo de paz, y que están a cargo de la ANT. Esta transformación digital, comprende las aplicaciones que permiten que el ciudadano tenga acceso a la información relacionada con las tierras, y así prestar el servicio de información manera clara y precisa.

Para el cumplimiento de ese objetivo, se considera el uso de la tecnología como brazo articulador de la gestión en la estrategia de la entidad acorde a la política de gobierno digital en TI, lo cual conlleva a la implementación de un modelo de servicios tecnológicos que garantice de forma integral la prestación de los servicios ofrecidos por la entidad a los ciudadanos e interesados que hacen uso de este portafolio que ofrece la ANT a través de su plataforma tecnológica optimizando la gestión y la administración pública a través de estos medios electrónicos.

En concordancia con lo anterior, el Plan Estratégico de Tecnologías de la Información (PETI) 2026 de la Agencia Nacional de Tierras (ANT) define las acciones de la Subdirección de Sistemas de Información en el marco estratégico que orienta la gestión, el uso y la evolución de las tecnologías de la información y las comunicaciones de la entidad para el año 2026. Su alcance comprende la alineación de las capacidades tecnológicas con los objetivos misionales y estratégicos de la ANT, con el fin de fortalecer la ejecución de la política de ordenamiento social de la propiedad rural y mejorar la prestación de servicios a la ciudadanía.

El PETI abarca la planificación y priorización de iniciativas, proyectos y servicios de TI que soportan los procesos institucionales, la gestión de la información, la interoperabilidad, la seguridad digital y el uso de datos como activo estratégico. Asimismo, establece lineamientos para el fortalecimiento de la arquitectura tecnológica, el gobierno de TI, la analítica de datos, los datos abiertos y la transformación digital, en coherencia con la Política de Gobierno Digital y demás marcos normativos vigentes.

Participación de las dependencias aportantes y articulación institucional

La presente contratación responde a una necesidad institucional asociada al fortalecimiento, continuidad, disponibilidad y seguridad de la infraestructura tecnológica que soporta la operación de los sistemas de información de la Agencia Nacional de Tierras – ANT. En este contexto, la Subdirección de Sistemas de Información de Tierras, como dependencia adscrita a la Dirección de Gestión del Ordenamiento Social de la Propiedad, lidera la identificación de las necesidades tecnológicas requeridas para garantizar la adecuada prestación de los servicios institucionales.

De acuerdo con lo anterior, la Subdirección de Sistemas de Información de Tierras (SSIT), en ejercicio de las funciones asignadas en el artículo 18 del Decreto Ley 2363 de 2015, es la dependencia responsable de identificar, analizar, estructurar y justificar la necesidad técnica que da origen al presente proceso contractual, toda vez que tiene a su cargo

la definición de los lineamientos de infraestructura tecnológica, sistemas de información, redes, telecomunicaciones, interoperabilidad, seguridad de la información y demás componentes tecnológicos requeridos para garantizar la adecuada operación de los Sistemas de Información de Tierras de la Agencia Nacional de Tierras.

En desarrollo de dichas competencias, la SSIT realizó el análisis de la situación tecnológica actual de la Entidad, identificó los requerimientos de continuidad operativa, conectividad, ciberseguridad, monitoreo especializado, alojamiento de infraestructura tecnológica y demás servicios asociados, definiendo las especificaciones técnicas necesarias para asegurar la disponibilidad, integridad y confiabilidad de los servicios tecnológicos institucionales.

La necesidad aquí descrita fue estructurada técnicamente por la Subdirección de Sistemas de Información de Tierras, en articulación con las dependencias beneficiarias y aportantes de recursos, constituyéndose en la dependencia líder del componente técnico del presente proceso contractual.

En este sentido y de conformidad con lo dispuesto en el artículo 18 del Decreto Ley 2363 de 2015, la Subdirección de Sistemas de Información de Tierras tiene, entre otras, las siguientes funciones:

1. Diseñar e implementar las bases de datos y sistemas de información de la Agencia y garantizar su articulación e interoperabilidad con el Sistema Nacional de Gestión de Tierras.
2. Mantener actualizada la información que produzca la Agencia que permita su disponibilidad, visualización, acceso y uso para la toma de decisiones.
3. Aplicar mecanismos de evaluación y seguimiento a los sistemas de información implementados y administrados por la Agencia.
4. Garantizar la aplicación, en la Agencia, de los estándares, buenas prácticas y principios para la información estatal.
5. Aplicar los lineamientos y procesos de infraestructura tecnológica de la Agencia en materia de software, hardware, redes y telecomunicaciones, acorde con los parámetros gubernamentales para su adquisición, operación y mantenimiento.
6. Diseñar estrategias, instrumentos y herramientas con aplicación de Tecnologías de la Información y las Comunicaciones para brindar de manera constante y permanente un buen servicio al ciudadano.

En cumplimiento de estas funciones, la Subdirección de Sistemas de Información de Tierras ha definido una estrategia integral de Tecnologías de la Información (TI), alineada con el Plan Estratégico de Tecnologías de la Información (PETI) y el Plan de Acción Institucional, orientada principalmente a: i) mejorar la gestión de la información misional y ii) fortalecer la infraestructura tecnológica institucional. Estos frentes buscan optimizar la gestión de los sistemas de información geoespaciales, alfanuméricos y documentales, así como fortalecer las capacidades de infraestructura, conectividad, almacenamiento, disponibilidad y seguridad de la información.

Así mismo, en desarrollo de la Política de Gobierno Digital establecida mediante el Decreto 1008 de 2018, actualizado mediante el Decreto 767 de 2022, que subrogó el capítulo pertinente del Decreto 1078 de 2015, la ANT orienta sus esfuerzos al uso y aprovechamiento estratégico de las Tecnologías de la Información y las Comunicaciones para consolidar entornos de confianza digital, fortalecer la prestación de servicios a la ciudadanía y mejorar la eficiencia institucional. En este sentido, resulta indispensable garantizar la operación continua de los servicios de infraestructura tecnológica, monitoreo especializado, conectividad y ciberseguridad que soportan los sistemas de información institucionales.

de Tierras, la Dirección de Asuntos Étnicos, la Dirección de Acceso a Tierras y la Subdirección de Sistemas de Información de Tierras, dependencias que concurren en la financiación del contrato en razón a que los bienes y servicios objeto de contratación constituyen un soporte tecnológico esencial para el desarrollo de sus funciones misionales. La participación financiera de estas dependencias obedece a la planeación de sus necesidades, a la programación de los recursos de sus respectivos proyectos de inversión y al beneficio directo que obtienen de la infraestructura tecnológica, los servicios de conectividad, monitoreo, ciberseguridad y continuidad operativa que se contratarán.

En efecto, la Dirección de Gestión Jurídica de Tierras desarrolla actividades relacionadas con los procesos de formalización, seguridad jurídica de la propiedad rural, gestión de expedientes agrarios, análisis jurídico predial y actuaciones administrativas sobre tierras, funciones que requieren permanentemente el acceso, disponibilidad y operación continua de los sistemas de información institucionales, plataformas documentales, herramientas de interoperabilidad, almacenamiento de datos y servicios de conectividad.

De igual forma, la Dirección de Asuntos Étnicos adelanta actuaciones orientadas a la protección y materialización de los derechos territoriales de los pueblos indígenas y de las comunidades negras, afrocolombianas, raizales y palenqueras, para lo cual requiere herramientas tecnológicas que garanticen el acceso remoto a la información, la conectividad territorial, la disponibilidad de sistemas de información geográfica, el procesamiento y almacenamiento de información, la interoperabilidad institucional y el funcionamiento permanente de las plataformas tecnológicas que soportan su gestión misional.

Por su parte, la Dirección de Acceso a Tierras participa en la financiación del presente contrato, toda vez que los servicios de infraestructura tecnológica, conectividad, almacenamiento, monitoreo especializado, ciberseguridad y operación continua constituyen un soporte indispensable para la ejecución de los procesos de acceso a tierras, la administración de la información predial, la gestión de expedientes, el análisis técnico y jurídico, así como para el funcionamiento de los sistemas de información que respaldan el cumplimiento de sus competencias. En consecuencia, la asignación de recursos por parte de esta Dirección responde al beneficio directo que obtiene de los servicios contratados y a la necesidad de garantizar la disponibilidad, integridad y continuidad de las plataformas tecnológicas que soportan su gestión misional, de conformidad con su programación presupuestal y la planeación institucional.

Por lo anterior, los servicios objeto del presente proceso contractual, tales como colocation, conectividad, internet, monitoreo especializado SOC/NOC, infraestructura tecnológica, almacenamiento, ciberseguridad y continuidad operativa, constituyen herramientas transversales que permiten el adecuado desarrollo de las competencias asignadas a las diferentes dependencias de la Agencia Nacional de Tierras.

La consolidación de las necesidades de las dependencias beneficiarias en un único proceso contractual responde a criterios de eficiencia administrativa, economía y planeación contractual, en tanto permite gestionar integralmente servicios tecnológicos de carácter transversal bajo condiciones homogéneas de operación, seguridad, disponibilidad e interoperabilidad, optimizando el uso de los recursos públicos, facilitando la administración del contrato y garantizando una prestación uniforme de los servicios tecnológicos requeridos por la Entidad.

Así mismo, en atención a que el contrato será financiado con recursos provenientes de diferentes dependencias de la Agencia, durante la ejecución contractual cada área aportante realizará el seguimiento a la ejecución de los recursos de su competencia, verificando la disponibilidad presupuestal y el porcentaje de afectación correspondiente, como requisito previo para la autorización de los pagos que deban efectuarse con cargo a su respectiva fuente de financiación.

Adicionalmente, esta necesidad se encuentra articulada con las funciones asignadas a la Secretaría General en materia tecnológica. En efecto, el numeral 9 del artículo 29 del Decreto Ley 2363 de 2015 establece como función de dicha dependencia:

> *"Administrar los sistemas de información, equipos, redes y herramientas tecnológicas y brindar el soporte técnico para su funcionamiento adecuado, coordinando lo pertinente".*

De igual manera, el artículo 31 del citado Decreto asigna a la Subdirección Administrativa y Financiera competencias relacionadas con la adquisición, mantenimiento, administración y provisión de los bienes y servicios requeridos para el funcionamiento de la entidad.

En consecuencia, aunque la Dirección de Gestión Jurídica de Tierras, la Dirección de Asuntos Étnicos y la Dirección de Acceso a Tierras son beneficiarias directas de los servicios tecnológicos requeridos, a la Subdirección de Sistemas de Información de Tierras y a las dependencias responsables de la gestión administrativa y tecnológica garantizar la administración, operación, soporte y fortalecimiento de la infraestructura tecnológica institucional que permite el cumplimiento de las funciones misionales de la Agencia.

En este sentido, la presente contratación constituye un mecanismo institucional transversal que permite soportar la operación de los procesos misionales, garantizar la continuidad de los servicios institucionales, asegurar la disponibilidad de la información, mantener la interoperabilidad entre sedes, fortalecer la atención territorial y garantizar el adecuado cumplimiento de las funciones asignadas a las distintas dependencias de la ANT.

Por tanto, existe una relación funcional, técnica, administrativa y presupuestal entre las competencias desarrolladas por Por tanto, existe una relación funcional, técnica, administrativa y presupuestal entre las competencias desarrolladas

por la Dirección de Gestión Jurídica de Tierras, la Dirección de Asuntos Étnicos, la Dirección de Acceso a Tierras y la Subdirección de Sistemas de Información de Tierras, en lo relacionado con las funciones de administración tecnológica, así como con la necesidad de contratar de manera integral los servicios de colocation, conectividad, SOC y NOC, los cuales soportan la operación institucional de la Agencia Nacional de Tierras a nivel nacional.

En la actualidad, algunos de los servicios, que se mencionaran a continuación y que son partes de las líneas principales, están siendo prestado a través del **Contrato Interadministrativo No. ANT-20254760**, cuyo objeto es: "*Brindar una solución integral para diferentes líneas de servicios y componentes tecnológicos que permitan garantizar la continuidad y adecuada operación de los Sistemas de Información de Tierras de la ANT y servicios conexos*" y cuyo plazo de ejecución se encuentra establecido hasta el 31 de julio de 2026 inclusive.

A través de la ejecución de dicho contrato se garantiza actualmente la operación continua de la infraestructura tecnológica institucional alojada en un Data Center externo, incluyendo servidores, plataformas de virtualización, almacenamiento, equipos de seguridad y demás componentes críticos que soportan los sistemas de información misionales de la Entidad. Asimismo, se fortalecieron las capacidades institucionales de monitoreo y gestión de ciberseguridad mediante la prestación de servicios especializados NOC/SOC orientados a la detección de amenazas, correlación de eventos, monitoreo de plataformas tecnológicas, gestión de incidentes, análisis y gestión de vulnerabilidades sobre ambientes on-premise y nube. De igual forma, se aseguró la conectividad e interconexión de las sedes, Unidades de Gestión Territorial (UGT) y puntos de atención de tierras a nivel nacional mediante servicios MPLS, internet, internet móvil e internet satelital portátil, permitiendo garantizar la disponibilidad, acceso y adecuado funcionamiento de los sistemas de información y servicios tecnológicos requeridos para el cumplimiento de la misión institucional, la atención de usuarios y la continuidad de los procesos estratégicos y misionales de la ANT. El contrato tiene plazo hasta el 31 de julio del 2026.

La necesidad de celebrar un nuevo contrato para el segundo semestre del 2026 se encuentra plenamente justificada en la obligación de la Agencia Nacional de Tierras (ANT) de garantizar la continuidad, disponibilidad y seguridad de su infraestructura tecnológica crítica, la cual soporta el funcionamiento de los sistemas misionales relacionados con la administración, formalización y gestión de tierras a nivel nacional. En este sentido, los servicios actualmente contratados comprenden componentes esenciales de Colocation, conectividad, monitoreo SOC/NOC, los cuales se detallaran más adelante en este documento, sin los cuales la entidad entraría en un riesgo de interrupción de servicios estratégicos como el Sistema de Información de Tierras (SIT), ORFEO, bases de datos institucionales y plataformas de interoperabilidad con otras entidades públicas. La ANT reconoce expresamente que la ausencia de continuidad en dichos servicios generaría una afectación directa a la operación institucional, a la atención ciudadana y al cumplimiento de las metas del Plan Nacional de Desarrollo y de la Reforma Rural Integral.

Asimismo, la justificación para la contratación se sustenta en el crecimiento operativo y tecnológico de la ANT derivado de la expansión de las Unidades de Gestión Territorial (UGT), el incremento de servicios digitales y la necesidad de mantener altos estándares de ciberseguridad, disponibilidad y conectividad en las UGT y demás sedes de la entidad. Los documentos evidencian que la infraestructura tecnológica actual opera bajo esquemas de alta disponibilidad, redundancia y monitoreo permanente 7x24x365, elementos indispensables para prevenir incidentes de seguridad informática, garantizar la continuidad del servicio público y soportar la transformación digital institucional. Igualmente, se advierte que la conectividad nacional, los servicios satelitales y el soporte especializado permiten asegurar presencia operativa en zonas apartadas del territorio nacional, donde la ANT desarrolla funciones misionales relacionadas con acceso y formalización de tierras. En consecuencia, la contratación no constituye una necesidad nueva o discrecional, sino la continuidad de un servicio esencial y estratégico para la operación permanente de la entidad y el cumplimiento de sus funciones legales y constitucionales.

Por tanto, se hace imperativo que la entidad continue con un servicio tecnológico integral que permita:

1. Continuar con la infraestructura tecnológica alojada en este centro de datos externo para lo cual se contratará el servicio de alojamiento y demás servicios conexos que permiten su operación e interconexión con la sede central del CAN.
2. Continuar garantizando las actividades propias de los servicios prestados por los centros de operación de red y seguridad, el monitoreo, la detección de amenazas, la gestión de incidentes, el análisis y gestión de vulnerabilidades, de los componentes, aplicaciones y servicios que hacen parte o están implementados sobre la infraestructura tecnológica de la Entidad.
3. Brindar los servicios de conectividad de la entidad de manera óptima garantizando la instalación y usabilidad de la conexión en todas las sedes.

De esta manera, para la Agencia Nacional de Tierras – ANT resulta indispensable contar con una solución integral de servicios tecnológicos que garantice la conectividad y comunicación permanente entre las sedes del nivel central, las Unidades de Gestión Territorial (UGT), los Puntos de Atención de Tierras (PAT) y demás dependencias y sedes de la entidad a nivel nacional, asegurando la disponibilidad, estabilidad y continuidad de los servicios requeridos para el desarrollo de sus funciones misionales y administrativas.

Para tal fin, se requiere la prestación de servicios especializados de conectividad que permitan garantizar el acceso seguro y oportuno a los sistemas de información institucionales, plataformas tecnológicas y herramientas de colaboración, mediante una infraestructura de comunicaciones robusta y de alta disponibilidad.

Las líneas de servicio objeto del presente proceso de contratación ya se encuentran integradas y operando como parte del servicio tecnológico integral actualmente implementado en la entidad; en consecuencia, lo que se busca con el presente proceso es garantizar la continuidad de esta modalidad de prestación del servicio. El complemento y detalle de estas especificaciones técnicas se encuentra en la sección denominada "**2. COMPONENTES DEL SERVICIO".**

A continuación, una breve descripción de cada uno de ellos:

1. Línea de servicio de Colocation (Datacenter principal externo)

Es la prestación del servicio de alojamiento y operación de la infraestructura tecnológica de Agencia Nacional de Tierras - ANT bajo la modalidad de colocation en un Datacenter externo, incluyendo servidores, equipos de seguridad, unidades de almacenamiento, bases de datos, componentes de georreferenciación, micrositios institucionales y demás plataformas, aplicaciones y servicios tecnológicos requeridos para garantizar la operación de la entidad.

La continuidad en la prestación del servicio es esencial para asegurar la disponibilidad, estabilidad, seguridad, interoperabilidad y correcto funcionamiento de los servicios tecnológicos de la ANT, así como de las plataformas y componentes asociados a la infraestructura institucional actualmente desplegada en el Datacenter externo. De igual forma, este servicio permite garantizar la operación de los componentes relacionados con almacenamiento de información, administración de sistemas operativos y motores de bases de datos, mecanismos de respaldo y recuperación de información (backups), herramientas de replicación, monitoreo, conectividad y controles de seguridad de la plataforma tecnológica institucional.

En caso de no garantizar la continuidad del servicio de colocation, la entidad podría enfrentar afectaciones significativas en la prestación de sus servicios tecnológicos, incluyendo riesgos de indisponibilidad de aplicaciones y plataformas institucionales, interrupción de procesos operativos, pérdida de continuidad en los servicios de conectividad e interoperabilidad, así como impactos sobre la disponibilidad, integridad y seguridad de la información administrada por la entidad.

En este contexto, se hace necesario mantener la infraestructura tecnológica de la ANT en un Datacenter externo bajo modalidad de colocation, el cual deberá contar con condiciones de operación certificadas y alineadas con estándares internacionales de disponibilidad, continuidad, seguridad física y lógica, capacidad de interconexión y soporte especializado, permitiendo garantizar la adecuada operación y continuidad de los servicios tecnológicos que soportan las funciones estratégicas y misionales de la entidad.

Por lo anterior, la Entidad requiere contar con el servicio de alojamiento de su infraestructura tecnológica y los servicios conexos en dicho datacenter externo, con el fin de garantizar en todo momento la adecuada prestación de los servicios institucionales. Dicho servicio comprende los siguientes subcomponentes:

1.1. Arrendamiento de espacio de rack en colocación

La Agencia Nacional de Tierras - ANT requiere el arrendamiento de espacio de rack bajo la modalidad de colocation en un Datacenter externo, con el fin de garantizar el alojamiento seguro, estable y continuo de la infraestructura tecnológica que soporta los servicios institucionales de la entidad. El servicio deberá incluir las condiciones necesarias para la adecuada operación de los equipos tecnológicos, tales como suministro eléctrico regulado y redundante, climatización especializada, conectividad, monitoreo, seguridad física y lógica y capacidades de alta disponibilidad.

Así mismo, el servicio deberá contemplar la posibilidad de ampliar la capacidad instalada mediante el arrendamiento de racks adicionales, de acuerdo con las necesidades de crecimiento de la infraestructura tecnológica de la entidad durante la ejecución del contrato, incluyendo todos los costos asociados a la operación y soporte de la infraestructura propia del Datacenter.

Adicionalmente, la entidad requiere contar con servicio de manos remotas prestado por personal técnico especializado bajo esquema de atención 7x24x365, sin limitación en la cantidad de requerimientos solicitados durante la ejecución del contrato. Este servicio deberá permitir la ejecución de actividades técnicas y operativas sobre la infraestructura alojada, incluyendo, entre otras, reinicio de servidores, conexión y desconexión de cables de red, instalación y reemplazo de componentes de hardware, verificación visual de equipos y conexiones, así como apoyo en la atención de incidentes básicos de hardware, garantizando la continuidad operativa y disponibilidad de los servicios tecnológicos institucionales.

1.2. Cross Conexión fibra óptica LC-LC

La Agencia Nacional de Tierras requiere el servicio de cross conexión en fibra óptica LC LC para la interconexión de su infraestructura tecnológica en modalidad de colocation dentro del Datacenter, la cual deberá ser certificada y adjuntada, utilizando cableado multimodo tipo OM3 u OM4 (50/125 µm), con cubierta LSZH (Low Smoke Zero Halogen). Este servicio deberá garantizar alta disponibilidad, baja latencia, confiabilidad y cumplimiento de estándares técnicos, asegurando niveles adecuados de desempeño, calidad de enlace y continuidad de los servicios institucionales.

1.3. Cross Conexión UTP CAT6A

La Agencia Nacional de Tierras - ANT requiere el servicio de cross conexión en cableado UTP categoría 6A para la interconexión de su infraestructura tecnológica en modalidad de colocation dentro del Datacenter. Dicho servicio deberá emplear cableado con conductores 100 % cobre (no CCA), cubierta tipo LSZH (Low Smoke Zero Halogen) apta para entornos de Datacenter, y cumplimiento de estándares ANSI/TIA 568.2 D e ISO/IEC 11801, con características adecuadas para operación en redes de hasta 10 Gbps. Asimismo, las cross conexiones deberán ser certificadas mediante equipos de medición tipo Fluke o equivalente, garantizando parámetros de desempeño óptimos del enlace. El servicio deberá asegurar alta disponibilidad, baja latencia, confiabilidad y calidad en la transmisión de datos, contribuyendo a la continuidad operativa de los servicios tecnológicos institucionales.

1.4. Patch cord UTP CAT6A de 3 metros

La Agencia Nacional de Tierras - ANT requiere el suministro de patch cord UTP categoría 6A certificado, con conectores RJ 45 en ambos extremos, conductor 100 % cobre, cumplimiento ANSI/TIA 568 e ISO/IEC 11801, con certificación de pruebas de fábrica, tipo de chaqueta LSZH, longitud 3 metros.

1.5. Patch cord de fibra óptica LC-LC OM3/OM4 de 3 metros

La Agencia Nacional de Tierras - ANT requiere el suministro de patch cord de fibra óptica LC LC dúplex de 3 metros, multimodo OM3/OM4 (50/125 µm), pulido UPC, con cubierta LSZH, certificado de fábrica (IL/RL) y cumplimiento de normas ANSI/TIA 568.3 D e ISO/IEC 11801.

1.6. Arrendamiento solución HA de switch SAN

La Agencia Nacional de Tierras - ANT requiere el arrendamiento de una solución de Switch SAN en alta disponibilidad (HA), instalada en el Datacenter bajo modalidad de colocation, con el fin de garantizar la conectividad, disponibilidad y continuidad de los servicios de almacenamiento.

Esta solución deberá permitir la interconexión de los sistemas de almacenamiento, herramientas de backup, infraestructura de virtualización de producción y servicios asociados de respaldo, asegurando condiciones adecuadas de desempeño, redundancia y continuidad operativa.

1.7. Arrendamiento SWITCH DE CORE de distribución, en alta disponibilidad

Se requiere el suministro en modalidad de arrendamiento de dos (2) Switch Core nuevos en configuración de alta disponibilidad (HA), los cuales no deberán ser remanufacturados. Así mismo, los modelos ofertados no podrán

encontrarse catalogados por el fabricante en estado End of Life (EoL), End of Sale (EoS) o End of Support, con el fin de garantizar la continuidad, soporte y actualización de la infraestructura tecnológica de la entidad.

1.8. Transición (30 días), traslado, instalación, configuración, transición y puesta en operación de los equipos y racks alojados en modalidad de colocation

El contratista deberá garantizar la continuidad operativa de los servicios de colocation durante el inicio, ejecución y finalización del contrato, contemplando los diferentes escenarios de transición y migración que puedan presentarse sobre la infraestructura tecnológica de la Agencia Nacional de Tierras – ANT.

Para tal efecto, el contratista deberá ejecutar, cuando aplique, las actividades de traslado, instalación, configuración, reconexión, pruebas y puesta en operación de los equipos, racks y demás componentes de infraestructura tecnológica alojados bajo modalidad de colocation.

Escenarios de transición

- **Escenario 1 – Continuidad de ubicación actual**

En caso de que el contratista seleccionado continúe prestando el servicio de colocation actualmente suministrado a la ANT, deberá garantizar la continuidad operativa de los servicios sin requerir traslado físico de la infraestructura tecnológica.

El contratista deberá ejecutar todas las actividades administrativas, técnicas y operativas necesarias para garantizar la continuidad del servicio, manteniendo las condiciones de disponibilidad, conectividad, seguridad, energía, climatización y operación de la infraestructura tecnológica de la ANT, sin generar indisponibilidades no programadas.

- **Escenario 2 – Traslado de infraestructura**

En caso de que el servicio de colocation sea prestado por un nuevo contratista, este deberá realizar integralmente el proceso de transición y traslado de la infraestructura tecnológica hacia el nuevo datacenter dispuesto para la prestación del servicio.

El contratista deberá ejecutar las actividades de levantamiento de información, inventario, desinstalación, desanclaje, etiquetado, embalaje, transporte especializado, custodia, instalación, reconexión, configuración, pruebas y puesta en operación de todos los equipos y racks objeto del servicio.

El servicio incluirá, sin limitarse a:

- Elaboración y presentación del plan de traslado y transición.
- Inventario detallado de la infraestructura tecnológica.
- Gestión de riesgos y plan de contingencia.
- Pólizas y seguros asociados al traslado.
- Embalaje especializado para infraestructura TIC.
- Transporte especializado y seguro.
- Cadena de custodia y acompañamiento de seguridad.
- Gestión y coordinación con fabricantes, carriers y terceros involucrados.
- Instalación física y adecuación en el sitio destino.
- Reconexión eléctrica, de datos y fibra óptica.
- Configuración y validación funcional de los equipos.
- Plan para ejecución de pruebas técnicas, operativas y de conectividad.
- Puesta en operación de los servicios trasladados.

El proceso iniciará con el levantamiento e inventario de la infraestructura tecnológica, incluyendo, entre otros, servidores, equipos de seguridad, unidades de almacenamiento, plataformas de respaldo, elementos de conectividad y demás componentes necesarios para garantizar la operación y conectividad de la plataforma tecnológica de la ANT.

La implementación comprenderá la instalación física y configuración de los sistemas trasladados, seguida de pruebas funcionales, de conectividad y compatibilidad, con el fin de garantizar la adecuada operación e integración con la infraestructura tecnológica existente de la entidad.

El contratista deberá entregar a la supervisión del contrato un plan detallado de transición y traslado, el cual deberá contemplar como mínimo:

- Cronograma de actividades.
- Ventanas de mantenimiento.
- Procedimientos de desconexión y reconexión.
- Plan de contingencia y reversa.
- Matriz de riesgos.
- Personal técnico participante.
- Validaciones previas y posteriores al traslado.
- Procedimientos de escalamiento y atención de incidentes.

El movimiento y puesta en operación deberá ejecutarse conforme al cronograma aprobado por la entidad, estimando un tiempo máximo de ejecución de tres (3) días calendario, salvo que la ANT autorice un plazo diferente de acuerdo con la complejidad de la migración.

El valor correspondiente al servicio de traslado, instalación, configuración y puesta en operación únicamente será reconocido por la entidad en caso de materializarse alguno de los escenarios que impliquen traslado físico de la infraestructura tecnológica.

1.9. Traslado de infraestructura tecnológica a la sede de la ANT o al sitio definido por la entidad

En el evento que, terminado el contrato o durante su ejecución, se requiera que el contratista devuelva los equipos a la sede de la Agencia Nacional de Tierras – ANT o donde esta lo requiera, el contratista deberá proveer el servicio de traslado, instalación, configuración y puesta en operación de todos los equipos y racks que se encuentren en modalidad de colocation al momento de la solicitud.

El contratista deberá garantizar todas las actividades técnicas, operativas y logísticas requeridas para asegurar la continuidad y adecuado funcionamiento de la infraestructura tecnológica durante el proceso de traslado y transición.

El contratista deberá:

- Realizar el desmontaje y entrega organizada de la infraestructura tecnológica.
- Garantizar el transporte especializado y la integridad física de los equipos.
- Contar con las pólizas, seguros y coberturas necesarias que amparen los riesgos asociados al embalaje, manipulación, transporte, cargue, descargue, instalación y puesta en operación de la infraestructura tecnológica.
- Ejecutar la instalación, reconexión, configuración y puesta en operación en el sitio definido por la entidad.
- Entregar documentación actualizada de conexiones, inventario y distribución en rack.
- Realizar pruebas funcionales y de conectividad posteriores al traslado.
- Garantizar acompañamiento técnico durante la transición.

El contratista deberá asumir las actividades de levantamiento de información, desanclaje, marcación, embalaje, transporte, instalación y validación funcional de los equipos definidos por la entidad, garantizando la adecuada puesta en operación de los servicios tecnológicos en el sitio destino.

El servicio incluirá el traslado seguro de la infraestructura de tecnologías de información y las comunicaciones (TIC), incluyendo racks, equipos, cableado y componentes de conectividad asociados.

El contratista será responsable por cualquier daño, pérdida o afectación ocasionada a la infraestructura tecnológica durante las actividades de desmontaje, embalaje, manipulación, transporte, instalación y reconexión de los equipos.

El contratista deberá entregar un plan detallado para realizar el traslado de los equipos desde el sitio de origen al sitio de destino definido por la ANT, documentando todas las actividades requeridas desde la recepción de los equipos hasta su entrega e instalación final conforme al cronograma aprobado por la entidad.

1.10. Suministro de 25 memorias ThinkSystem

La Agencia Nacional de Tierras - ANT requiere el suministro de veinticinco (25) memorias LENOVO número de parte 4ZC7A15122 - 32GB TruDDR4 DDR4-3200MHz (2Rx4 1.2V) RDIMM-A, con el fin de fortalecer y ampliar la capacidad de procesamiento y desempeño de la infraestructura tecnológica institucional, garantizando la estabilidad, disponibilidad y continuidad operativa de las plataformas y servicios tecnológicos de la entidad.

1.11. Suministro de tarjeta HBA (Host Bus Adapter) Fibre Channel

La Agencia Nacional de Tierras - ANT requiere el suministro de cuatro (4) tarjetas HBA referencia Emulex 16Gb Gen6 FC Dual-port HBA, incluyendo sus respectivos módulos SFP FC de 16Gb compatibles, con el fin de garantizar la conectividad especializada y de alto desempeño entre la infraestructura HCI y el almacenamiento SAN institucional.

1.12. Empalme, transición y continuidad del servicio

En cualquiera de los escenarios de transición definidos en el presente documento, la ANT podrá requerir actividades de empalme, transición y continuidad operativa de los servicios de colocation contratados, con el fin de garantizar la adecuada prestación del servicio durante procesos de continuidad, cambio de contratista o traslado de infraestructura tecnológica.

Para tal efecto, el contratista deberá garantizar las actividades técnicas, operativas y logísticas necesarias para asegurar la continuidad de los servicios contratados, evitando afectaciones o interrupciones en la operación de la entidad.

Las actividades de empalme, transición y continuidad del servicio deberán ejecutarse preferiblemente durante el último mes de ejecución contractual. No obstante, en caso de requerirse actividades posteriores a la finalización del contrato, el contratista deberá garantizar el acompañamiento requerido por la ANT hasta por un período de treinta (30) días calendario adicionales, sin que ello genere costos adicionales para la entidad.

Las actividades de empalme y transición podrán incluir, entre otras:

- Coordinación operativa entre las partes involucradas en la transición del servicio.
- Coordinación de ventanas de mantenimiento y actividades de traslado.
- Habilitación y continuidad de los servicios de colocation contratados.
- Acompañamiento técnico durante actividades de traslado o reconexión de infraestructura.
- Validaciones de conectividad, energía y operación de los servicios contratados.
- Entrega de información asociada a la ubicación física, distribución en rack y servicios suministrados.
- Coordinación de acceso al datacenter para ejecución de actividades autorizadas por la ANT.

En todo caso, el contratista deberá garantizar que no exista interrupción de los servicios contratados como consecuencia de la transición, cambio de contratista o traslado de infraestructura tecnológica.

2. Línea SOC (Security Operations Center) y Línea NOC (Network Operations Center)

La Entidad requiere los servicios de un Centro de Operaciones de Seguridad (Security Operations Center – SOC), y un Centro de Operaciones de Red integrado (NOC) de manera permanente en un horario 7x24, para lo cual se debe contar con un centro de monitoreo ubicado en la ciudad de Bogotá D.C. (Colombia). La conexión hacia la herramienta de correlación de la Entidad se realizará a través de una conexión segura utilizando internet. Las comunicaciones requeridas se realizarán a través de conexiones seguras VPN. La solución de monitoreo SOC se debe poder realizar en forma remota y disponer un personal en sitio cuando se requiera el cumplimiento de acuerdos de nivel de servicio para eventos o incidentes críticos. El servicio consta de los siguientes subcomponentes:

2.1 Servicio NOC (Network Operations Center):

2.1.1 SERVICIO NOC (NETWORK OPERATIONS CENTER) – MONITOREO DE INFRAESTRUCTURA TECNOLÓGICA 7X24X365 (ON-PREMISE Y SERVICIOS EN NUBE).

La Agencia Nacional de Tierras - ANT requiere contar con un servicio NOC bajo esquema 7x24x365 para el monitoreo y gestión de la infraestructura tecnológica, tanto en ambientes on-premise como en nube, con el fin de garantizar la disponibilidad, estabilidad, desempeño y continuidad de los servicios tecnológicos de la Entidad.

El servicio deberá incluir el monitoreo continuo de dispositivos de red, servidores, plataformas de virtualización, bases de datos, aplicaciones, enlaces y servicios de conectividad, así como la detección y gestión de eventos, fallas e incidentes, generación de alertas, escalamiento, seguimiento de casos hasta su normalización y generación de reportes e informes.

El contratista será responsable de suministrar, implementar, administrar y mantener la herramienta de monitoreo requerida para la prestación del servicio, incluyendo el licenciamiento y demás componentes necesarios para el monitoreo integral de la infraestructura tecnológica de la Entidad.

Las actividades del servicio deberán ejecutarse bajo las buenas prácticas de ITIL en su última versión vigente e incluir la gestión y escalamiento con terceros hasta lograr la recuperación y estabilidad de la infraestructura afectada.

2.1.2 Licenciamiento PRTG NETWORK MONITOR

La Agencia Nacional de Tierras - ANT requiere el suministro de licenciamiento oficial de la plataforma PRTG Network Monitor de Paessler, bajo modalidad de suscripción por un (1) año y con capacidad mínima de diez mil (10.000) sensores, con el fin de fortalecer las capacidades de monitoreo de la infraestructura tecnológica institucional.

El licenciamiento deberá incluir actualizaciones, parches de seguridad y soporte técnico oficial durante la vigencia de la suscripción. Así mismo, el contratista deberá realizar la instalación, configuración y puesta en funcionamiento de la solución sobre el servidor suministrado por la Entidad.

La solución deberá permitir el monitoreo de dispositivos de red, servidores, plataformas de virtualización, servicios en nube y demás componentes tecnológicos de la Entidad.

NOTA: Actualmente, la Entidad cuenta con la versión gratuita de la herramienta PRTG Network Monitor de Paessler, la cual ha permitido realizar el monitoreo de algunos componentes de la infraestructura tecnológica. Sin embargo, esta versión presenta una limitación de hasta 100 sensores, capacidad que resulta insuficiente para cubrir la totalidad de los activos tecnológicos de la Entidad. Como consecuencia de esta limitación, únicamente es posible supervisar una pequeña parte de la infraestructura, lo que reduce la visibilidad sobre el estado de los servicios tecnológicos y dificulta la identificación oportuna de fallas, degradaciones del servicio o eventos que puedan afectar la continuidad de la operación.

El suministro del licenciamiento de PRTG Network Monitor permitirá ampliar la capacidad de monitoreo e incorporar la totalidad de la infraestructura tecnológica institucional dentro de una única plataforma, centralizando la supervisión de la disponibilidad, el desempeño y el estado de los diferentes componentes de TI. Asimismo, facilitará la generación de alertas tempranas, la identificación proactiva de incidentes y el seguimiento continuo de la operación, contribuyendo a mejorar la disponibilidad y confiabilidad de los servicios tecnológicos que soportan la misión de la Entidad.

Adicionalmente, la herramienta servirá como un mecanismo independiente de supervisión y validación de la operación del Centro de Operaciones de Red (NOC), permitiendo a la Entidad verificar de manera objetiva la detección, atención y escalamiento de alertas e incidentes por parte del contratista responsable de la prestación del servicio. Esto fortalecerá las actividades de seguimiento, control y verificación del cumplimiento de los niveles de servicio establecidos contractualmente.

Desde el punto de vista técnico y económico, el licenciamiento de PRTG Network Monitor representa la alternativa más conveniente para la Entidad, ya que permite aprovechar la experiencia adquirida con la herramienta actualmente implementada, evitando procesos de migración hacia otra solución, reduciendo los tiempos de implementación, capacitación y puesta en operación, y garantizando la continuidad del esquema de monitoreo actual.

2.1.3 Servicios de Implementación y Transferencia de Conocimiento

El contratista deberá realizar una transferencia de conocimiento a 15 personas designadas por la ANT de mínimo ocho (8) horas sobre la administración y operación básica de la herramienta.

2.1.4 Suscripción Aruba Central Foundation para 71 Access Points – por un (1) año

Actualmente, esta plataforma permite la administración centralizada de la red inalámbrica institucional en las UGTs la cual tiene vigencia hasta noviembre del 2026, a partir de esta fecha la misma quedaría sin funcionamiento de toda la red WIFI de las UGTs, es por esto que es necesario la renovación de las suscripciones Aruba Central Foundation para 71 Access Points actualmente vigentes, por un (1) año, para la continuidad de las conexiones de los funcionarios y contratistas de la ANT a la red wifi mediante los Access Points instalados.

En consecuencia con lo señalado previamente, su renovación es necesaria para garantizar la continuidad de la operación, el monitoreo en tiempo real y la aplicación de actualizaciones de seguridad sobre los 71 Access Points en funcionamiento.

La no renovación generaría la pérdida de gestión centralizada, afectando directamente la estabilidad, el monitoreo, el control y la seguridad de la red WiFi ya desplegada en dichas UGTs, así como la conectividad de los usuarios.

2.1.5 Renovación de soporte para dos (2) Switches Core 5406 zl2 Foundation Care 4H Exchange – por un (1) año

Los switches core se encuentran actualmente en operación y soportan la red LAN (Local Area Network) de la sede CAN, así como la comunicación entre el colocation y dicha sede. La renovación del soporte garantiza atención especializada ante fallas, acceso a actualizaciones y el reemplazo de hardware en tiempos reducidos, lo cual permite una respuesta ágil ante incidentes que puedan afectar la infraestructura.

La no renovación dejaría a la entidad sin respaldo técnico sobre esta infraestructura crítica, incrementando el riesgo de interrupciones prolongadas en los servicios tecnológicos actualmente en funcionamiento en la sede CAN.

2.1.6 Suministro en modalidad de arrendamiento de quince (15) Access Points, soporte por un (1) año, debe incluir servicio de infraestructura para su puesta en marcha.

Se requiere el suministro en modalidad de arrendamiento de quince (15) Access Points, esto obedece a la necesidad de reemplazar los equipos inalámbricos actualmente instalados en la sede Chapinero o donde indique el supervisor del contrato, los cuales están llegado al final de su ciclo de vida útil, lo que conlleva a que el Fabricante no de más garantías y soportes, generando una obsolescencia tecnológica y riesgos de seguridad sobre la red de la Agencia al no poder realizarse actualizaciones de firmware de dichos equipos para poder realizar, por ejemplo, parcheos de seguridad.

Es necesario precisar que los Access Point actualmente instalados en la sede Chapinero han alcanzado un nivel de obsolescencia que impide su compatibilidad con las versiones más recientes del firmware del firewall. En consecuencia, la actualización del firewall en las condiciones actuales ocasionaría la pérdida de la funcionalidad de administración y gestión centralizada del servicio de red inalámbrica (WiFi) implementado en dicha sede, afectando la continuidad y operación del servicio. Por lo anterior, se hace necesario contemplar la renovación de los Access Point, con el fin de garantizar la compatibilidad tecnológica con el firewall, mantener el soporte del fabricante y permitir la actualización segura de la infraestructura de seguridad sin afectar la prestación del servicio de conectividad inalámbrica.

El arrendamiento de los nuevos equipos, junto con su soporte, instalación, configuración y puesta en funcionamiento, incluyendo la infraestructura necesaria para su correcta operación, en la sede donde sea requerido por parte del supervisor del contrato, garantizan la compatibilidad con la infraestructura tecnológica y permite la actualización de la plataforma de seguridad la cual asegurará la disponibilidad y administración centralizada de la red Wi-Fi de dicha sede o donde el supervisor lo requiera.

2.1.7 Servicio de monitoreo continuo bajo modalidad SaaS, enfocado en la Protección de Marca y la Gestión de la Superficie de Ataque Externa.

La adquisición de este servicio de monitoreo continuo bajo modalidad SaaS es fundamental para fortalecer la ciberseguridad institucional mediante la protección de marca en la Deep y Dark Web y la gestión de la superficie de ataque externa (EASM) por doce (12) meses. Esta herramienta operará de forma agentless con una puesta en marcha

máxima de diez días calendario, permitiendo la detección predictiva de incidentes de phishing y la ejecución de acciones de desactivación (takedowns) ante amenazas confirmadas. Su implementación garantiza el cumplimiento de estándares internacionales y optimiza la respuesta proactiva ante fugas de datos y el secuestro de credenciales. Finalmente, el servicio asegura soporte especializado 24/7/365 en español e inglés.

Actualmente la entidad cuenta con una seguridad perimetral, que protege la infraestructura local. Ahora bien, el servicio que se pretende contratar realiza un monitoreo continuo en la Deep y Dark Web, (espacios de Internet que no son accesibles mediante los buscadores tradicionales y donde pueden encontrarse sitios de acceso restringido o utilizados para actividades ilícitas), con el fin de identificar si la información de la Entidad ha sido expuesta, compartida o comercializada sin autorización, mediante la revisión de más de 7.700 sitios y foros especializados. Actualmente, la seguridad perimetral con la que cuenta la Entidad no realiza este tipo de funciones.

2.2 Línea SOC

2.2.1 SERVICIO SOC (SECURITY OPERATIONS CENTER) – MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA 7X24X365 (Onpremise - Servicios en Nube).

La Agencia Nacional de Tierras - ANT requiere contar con un servicio SOC bajo esquema 7x24x365 para el monitoreo y gestión de la infraestructura tecnológica, tanto en ambientes on-premise como en nube, con el fin de garantizar la disponibilidad, estabilidad, desempeño y continuidad de los servicios tecnológicos de la Entidad.

El servicio deberá incluir el monitoreo y correlación de eventos de seguridad sobre la plataforma SIEM adquirida por la Entidad, para 275 dispositivos con agente SIEM a nivel nacional y 100 agentes avanzados (FIM) durante la ejecución del contrato; entre los cuales se detallan: Servidores, Hipervisores, Firewalls, Switch de Core, Switches de Acceso, Firewall de aplicaciones y Balanceadores de carga.

De igual forma el servicio deberá incluir la atención y gestión de incidentes de interrupción del monitoreo – SOC y el correspondiente escalamiento al equipo de respuesta a incidentes de seguridad de la entidad, dando cumplimiento a los acuerdos de niveles de servicio requeridos.

2.2.2 Servicio Especializado SOC por Demanda – Bolsa de 10 horas al mes

Es el servicio de un equipo especializado de un Centro de Operaciones de Seguridad (SOC) para prestar servicios de soporte en ciberseguridad, conforme a las necesidades de la Entidad. La prestación del servicio se realizará mediante una bolsa de hasta diez (10) horas, destinadas a actividades como análisis de incidentes de seguridad, investigación de alertas, acompañamiento en la contención y respuesta a incidentes, análisis forense inicial, asesoría técnica y demás actividades especializadas asociadas a la operación de seguridad de la información.

2.2.3 Servicios especializados de análisis forense en ciberseguridad

Se deberá prestar el servicio especializado de análisis forense en ciberseguridad para realizar la investigación de incidentes de seguridad informática, con el objetivo de identificar al o los responsables, comprender el ataque y dar las recomendaciones respecto al incidente de ciberseguridad. El alcance del análisis forense en ciberseguridad podrá ser aplicado en casos como: Fraudes informáticos, Extorción, Robo de datos, Intrusión en redes informáticas.

Se contempla una bolsa de 100 horas de servicios profesionales, la cual se ejecutará por demanda, es decir en caso en que se requiera por la Entidad en el marco de la ejecución del servicio, por ningún motivo será un cobro mensual. Al momento que ocurra el hecho y se requieran los servicios especializados, se realizará una evaluación preliminar y se presentará la oferta de servicios, con el alcance técnico y económico.

2.2.4 - Un (1) equipo de cómputo o almacenamiento afín con 64gb de RAM, un CPU de 8 núcleos, y un almacenamiento de Mínimo 20TB en raid 6. Ubuntu 24.04 y Un (1) equipo de cómputo con 128gb de RAM un CPU de 16 núcleos y un almacenamiento de 2Tb. Ubuntu 24.04

El contratista deberá suministrar, instalar, configurar y poner en operación la infraestructura de cómputo requerida para soportar las actividades de gestión, monitoreo, análisis de eventos de seguridad de la información y la ejecución de

pruebas técnicas de seguridad, garantizando que los equipos cuenten con las características mínimas que se describen a continuación:

a. Equipo para almacenamiento y procesamiento de información de seguridad:
- Un (1) equipo de cómputo o servidor de almacenamiento con mínimo sesenta y cuatro (64) GB de memoria RAM.
- Procesador con mínimo ocho (8) núcleos.
- Capacidad de almacenamiento útil mínima de veinte (20) TB, configurada en RAID 6, con el fin de proporcionar tolerancia a fallos, integridad y disponibilidad de la información.
- Sistema operativo Ubuntu Server 24.04 LTS o superior compatible.

b. Equipo para análisis y ejecución de pruebas de seguridad:
- Un (1) equipo de cómputo con mínimo ciento veintiocho (128) GB de memoria RAM.
- Procesador con mínimo dieciséis (16) núcleos.
- Almacenamiento de estado sólido (SSD) con capacidad mínima de dos (2) TB.
- Sistema operativo Ubuntu 24.04 LTS o superior compatible.

2.2.5 SOAR - Subscripción Version SaaS (Cloud) por 12 Meses para 2 Administradores

Prestar el servicio de arrendamiento de licenciamiento SOAR para las integraciones con sistemas y servicios de ciberseguridad e infraestructura TI compatible con la arquitectura actual de la entidad. El servicio debe incluir puesta en operación de la herramienta y la transferencia de conocimiento asociada y requerida por la entidad para su operación.

2.2.6 Renovación Licenciamiento de dos (2) FW 1800F por (1) año.

La Entidad cuenta actualmente con dos (2) dispositivos de seguridad perimetral Firewall FortiGate 1800F ubicados en el CAN, los cuales hacen parte de la infraestructura tecnológica institucional y soportan la prestación de los servicios de seguridad de la información y ciberseguridad.

En consecuencia, este ítem corresponde a la renovación del licenciamiento de los equipos existentes y no a la adquisición de una nueva solución tecnológica. Esta necesidad obedece a la obligación de garantizar la continuidad operativa de los servicios de seguridad, el acceso a actualizaciones de software y firmas de seguridad, el soporte del fabricante y el funcionamiento de las funcionalidades actualmente implementadas.

La sustitución de los dispositivos por una solución de otro fabricante implicaría costos adicionales para la Entidad asociados, entre otros, a la adquisición de nuevo hardware, licencias, servicios de implementación, migración de configuraciones, integración con la infraestructura tecnológica existente, pruebas de funcionamiento, capacitación del personal y eventuales afectaciones a la continuidad del servicio durante el proceso de transición.

En ese sentido, la renovación del licenciamiento de los dispositivos FortiGate 1800F constituye la alternativa técnica y económicamente más eficiente, al preservar la inversión previamente realizada por la Entidad, evitar costos de reemplazo e implementación, reducir riesgos operacionales y garantizar la continuidad de los controles de seguridad actualmente desplegados.

Por lo anterior, la renovación del licenciamiento de los equipos existentes responde a criterios de eficiencia, economía, planeación y protección de los recursos públicos, al permitir el aprovechamiento de la infraestructura tecnológica instalada y asegurar la continuidad de la operación sin incurrir en inversiones adicionales que no generan un beneficio proporcional para la Entidad.

2.2.7 Atención de incidentes de interrupción del monitoreo – SOC

Se requiere un servicio para la atención de incidentes el cual, dependiendo la criticidad y la prioridad del monitoreo, se atiende el incidente.

PRIORIDAD Interrupción del monitoreo	**DESCRIPCIÓN**
CRÍTICA	Se detiene totalmente el monitoreo o su capacidad está severamente impactada de manera que no se puede continuar trabajando. Tiempo de respuesta: Identificación: 3 minutos contado a partir de su ocurrencia o del reporte efectuado por la Entidad. Análisis: 10 minutos contados a partir de la finalización del tiempo de Identificación.
ALTA	El 80% de las aplicaciones de seguridad y sistemas monitoreados experimenta perdida del servicio de monitoreo, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida. Tiempo de respuesta: Identificación: 5 minutos contados a partir de su ocurrencia o del reporte efectuado por la Entidad. Análisis: 10 minutos contados a partir de la finalización del tiempo de Identificación.
MEDIA	El 50% de las aplicaciones de seguridad y sistemas monitoreados experimenta perdida del servicio de monitoreo, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera intermitente. Tiempo de respuesta: Identificación: 10 minutos contado a partir de su ocurrencia o del reporte efectuado por la Entidad. Análisis: 10 minutos contados a partir de la finalización del tiempo de Identificación.
BAJA	El 20% de las aplicaciones de seguridad y sistemas monitoreados experimenta perdida del servicio de monitoreo, algunas características importantes no pueden ser utilizadas, no impacta la operación del programa, no se experimenta perdida del servicio y no se impide la operación de los sistemas. Tiempo de respuesta: Identificación: 15 minutos contados a partir de su ocurrencia o del reporte efectuado por la Entidad. Análisis: 10 minutos contados a partir de la finalización del tiempo de Identificación.

2.2.8 Tiempos de alertamiento y escalamiento al equipo de respuesta a incidentes de seguridad de la entidad - SOC:

- De impacto crítico: alertamiento dentro de los primeros 5 minutos y escalamiento en máximo 10 minutos.
- De impacto alto: alertamiento dentro de los primeros 15 minutos y escalamiento en máximo 20 minutos.
- De impacto moderado: alertamiento dentro de las primeras 2 horas y escalamiento en máximo 2 horas.
- De impacto bajo: alertamiento dentro de las primeras 12 horas y escalamiento en máximo 6 horas.

3. Línea de servicios de conectividad

La Agencia Nacional de Tierras - ANT requiere contar con servicios integrales de conectividad para garantizar la comunicación, interoperabilidad, disponibilidad y continuidad de los servicios tecnológicos y administrativos de la entidad a nivel nacional. Estos servicios deberán permitir la interconexión segura y estable entre las diferentes sedes, plataformas tecnológicas, usuarios y servicios institucionales, garantizando condiciones adecuadas de disponibilidad, desempeño, cobertura, continuidad operativa y redundancia para soportar la operación misional, administrativa y tecnológica de la entidad.

Dicho servicio comprende los siguientes componentes:

Servicio	Cantidad
INTERNET CORPORATIVO	56
MPLS L2 (Capa 2)	2
MPLS L3 (Capa 3)	12
SERVICIO DE CONECTIVIDAD SATELITAL DE ÓRBITA BAJA (LEO) PARA UBICACIÓN FIJA	2
CONECTIVIDAD MÓVIL 3G – 4G – 5G	5
ENLACES SATELITALES DE ORBITA BAJA PORTÁTILES – MOVILIDAD TERRESTRE – USO COLOMBIA	4

II. COMPONENTES DEL SERVICIO

1.13. Descripción de los servicios a contratar:

Las siguientes son las líneas de servicio que se deben proveer a través de esta contratación:

1. Línea de servicio de Colocation (Centro de datos principal externo).
2. Línea de servicios NOC/SOC.
3. Línea de conectividad de redes.

1.13.1. Línea de servicio de Colocation (Centro de datos principal externo)

La solución de Colocation comprende la prestación de los servicios necesarios para el alojamiento de la infraestructura tecnológica de la Agencia Nacional de Tierras – ANT en un datacenter externo, garantizando condiciones adecuadas de disponibilidad, seguridad física, conectividad, energía regulada, climatización y continuidad para la operación de los servicios institucionales soportados sobre dicha infraestructura.

La infraestructura objeto del servicio corresponde a equipos y plataformas tecnológicas de propiedad de la ANT, incluyendo servidores, equipos de seguridad, unidades de almacenamiento y demás componentes tecnológicos administrados y operados por la entidad.

El alcance del servicio incluye las actividades requeridas para el alistamiento, traslado, instalación física y puesta en operación de la infraestructura tecnológica en modalidad de Colocation, así como el suministro de los recursos asociados al alojamiento en datacenter, tales como espacio en rack, cableado, energía, climatización, conectividad y seguridad física.

La implementación contempla las actividades de instalación física, interconexión y validación de funcionamiento de la infraestructura alojada, verificando su correcta integración con las redes y servicios administrados por la ANT.

Así mismo, el contratista deberá garantizar las condiciones operativas necesarias para la continuidad del servicio, incluyendo soporte sobre la infraestructura del datacenter y atención de incidentes asociados al servicio de Colocation.

La administración, configuración, operación, mantenimiento y soporte de los sistemas operativos, aplicaciones, bases de datos, plataformas tecnológicas y demás servicios desplegados sobre la infraestructura alojada estarán exclusivamente a cargo de la ANT.

A continuación, se detallan los requerimientos relacionados con la prestación del servicio de Colocation, las condiciones de implementación y puesta en operación, así como las actividades y entregables asociados al servicio:

ESPECIFICACIONES TÉCNICAS MÍNIMAS PARA LA PRESTACIÓN DEL SERVICIO DE COLOCATION

Se deben tener en cuenta las siguientes consideraciones técnicas para el cumplimiento de los estándares de disponibilidad y continuidad exigidos por la Entidad:

Área física e infraestructura del Datacenter:

- El Datacenter deberá contar con certificación vigente ICREA Nivel IV o superior, Tier III o superior, o certificación internacional equivalente que garantice alta disponibilidad, continuidad operativa y redundancia de infraestructura crítica.
- El Datacenter deberá contar con controles de acceso físico al área blanca mediante esquemas de seguridad multinivel y autenticación biométrica.
- El contratista deberá garantizar capacidad eléctrica de hasta quince (15) kVA por rack 3 rack y uno propio.
- El servicio deberá permitir alojar un rack propiedad de la ANT con las siguientes dimensiones y requerimientos eléctricos:
    - Altura: 2 metros.
    - Ancho: 70 cm.
    - Profundidad: 120 cm.
    - Requerimiento eléctrico: 51,6 amperios a 220V equivalente a 11,352 kVA.
- El Datacenter no deberá estar ubicado en zonas que representen riesgo para la continuidad operativa, incluyendo áreas de influencia aeronáutica o zonas de alto riesgo.

Manos remotas:

- El contratista deberá prestar servicio de manos remotas mediante personal técnico especializado disponible en modalidad 7x24x365.
- El servicio de manos remotas no deberá tener limitación en la cantidad de requerimientos solicitados por la ANT durante la ejecución del contrato.
- El servicio de manos remotas deberá incluir, como mínimo, las siguientes actividades:
    - Reinicio de servidores y equipos.
    - Conexión y desconexión de cables de red y energía.
    - Validación de niveles de energía que le llegan a los dispositivos.
    - Instalación y reemplazo de componentes de hardware.
    - Verificación visual de equipos, indicadores y conexiones.
    - Apoyo en la atención de incidentes básicos de hardware.
    - Validación física de estado operativo de la infraestructura alojada.
    - Apoyo mediante el préstamo de equipo de cómputo que permita el soporte remoto especializado hacia los equipos de la Agencia Nacional de Tierras - ANT, garantizando condiciones adecuadas de acceso, administración y diagnóstico de la infraestructura tecnológica. Dichos equipos deberán contar con las capacidades técnicas necesarias para la ejecución de actividades de monitoreo, configuración, gestión de incidentes y soporte sobre la red institucional.
- El contratista deberá garantizar la atención oportuna de los requerimientos de manos remotas con el fin de contribuir a la continuidad operativa y disponibilidad de los servicios tecnológicos institucionales.

Conectividad y Cross Conexiones en Datacenter

- El contratista deberá garantizar el acceso e interconexión con los proveedores de servicios de comunicaciones utilizados por la ANT al momento de la puesta en operación del servicio.
- El servicio deberá incluir todas las conexiones y cross conexiones requeridas desde las áreas de interconexión de los carriers o proveedores de comunicaciones hasta los racks asignados a la ANT, independientemente del tipo de medio o cableado requerido.
- El contratista deberá garantizar la disponibilidad de infraestructura de cableado y conectividad necesaria para la correcta integración de los servicios de comunicaciones de la ANT.
- El contratista deberá suministrar las cross conexiones necesarias para la interconexión inicial de los racks y carriers, incluyendo los patch cord certificados de cobre y fibra óptica requeridos para la correcta conexión e integración de los equipos de la Entidad dentro del servicio de colocation.

Informe Mensual del Servicio de Colocation

- El contratista deberá entregar mensualmente a la supervisión del contrato un informe detallado de la operación y prestación del servicio de colocation correspondiente al período evaluado.

- El informe mensual deberá incluir como mínimo la disponibilidad del servicio de colocation y el detalle de las interrupciones o indisponibilidades presentadas durante el período, indicando fecha, duración, causa y acciones ejecutadas.
- El contratista deberá reportar los eventos asociados a la infraestructura de soporte del datacenter que hayan afectado o podido afectar la prestación del servicio, incluyendo eventos relacionados con sistemas eléctricos, UPS, PDU, plantas eléctricas, climatización y conectividad.
- El contratista deberá informar la relación de incidentes, requerimientos y solicitudes de soporte atendidas durante el período, incluyendo tiempos de atención, solución y estado de los casos registrados.
- El contratista deberá incluir en el informe mensual el registro de mantenimientos preventivos, correctivos o actividades programadas que hayan involucrado o impactado los servicios prestados a la ANT.
- El contratista deberá reportar los accesos físicos realizados al datacenter relacionados con la infraestructura de la ANT, indicando fecha, personal autorizado y actividad ejecutada.
- El contratista deberá presentar el estado de utilización de los recursos contratados asociados al servicio de colocation, incluyendo ocupación de racks, consumo eléctrico y capacidad disponible.
- El contratista deberá reportar el cumplimiento de los acuerdos de niveles de servicio (ANS) establecidos contractualmente, incluyendo indicadores, desviaciones, eventos relevantes y acciones de mejora implementadas.
- El contratista deberá informar cualquier riesgo, incidente o condición técnica que pueda afectar la continuidad, disponibilidad o adecuada prestación del servicio de colocation.
- El contratista deberá entregar junto con el informe mensual las recomendaciones técnicas y operativas que considere pertinentes para garantizar la adecuada prestación y continuidad del servicio.

Niveles de Servicio y Tiempos de Atención Mínimos Requeridos

- El contratista deberá garantizar una disponibilidad mensual mínima del servicio de colocation acorde con el nivel de certificación ofertado para el datacenter, la cual no podrá ser inferior al noventa y nueve punto novecientos ochenta y dos por ciento (99,982%) mensual para infraestructura Tier III o ICREA Nivel IV.
- El servicio deberá garantizar operación continua 7x24x365 sobre la infraestructura de soporte del datacenter, incluyendo suministro eléctrico, climatización, conectividad y sistemas asociados a la prestación del servicio de colocation.
- El servicio deberá contar con esquemas de redundancia eléctrica y de climatización acordes con la certificación del datacenter ofertado, incluyendo sistemas UPS, plantas eléctricas y sistemas de refrigeración redundantes.
- El servicio deberá disponer de mesa de servicio y canales de atención operativos 7x24x365 para la recepción, gestión y escalamiento de incidentes, requerimientos y solicitudes relacionadas con el servicio contratado.
- Para incidentes críticos que afecten total o parcialmente la disponibilidad del servicio de colocation, energía, climatización o conectividad asociada a los servicios contratados, el contratista deberá garantizar un tiempo máximo de atención inicial de quince (15) minutos y un tiempo máximo de escalamiento de treinta (30) minutos.
- Para incidentes de severidad alta que generen degradación parcial de los servicios contratados, el contratista deberá garantizar un tiempo máximo de atención inicial de treinta (30) minutos.
- Para incidentes de severidad media o solicitudes operativas programadas, el contratista deberá garantizar un tiempo máximo de atención inicial de cuatro (4) horas.
- Para solicitudes administrativas o requerimientos de baja severidad, el contratista deberá garantizar un tiempo máximo de atención de un (1) día hábil.
- El contratista deberá garantizar disponibilidad permanente para la coordinación y autorización de acceso al datacenter por parte del personal autorizado por la ANT.
    - El contratista deberá contar con procedimientos formales de gestión y escalamiento de incidentes, garantizando trazabilidad, registro y seguimiento de los eventos reportados.

SERVICIO DE MIGRACIÓN Y TRASLADO DE INFRAESTRUCTURA AL DATACENTER

- El plan de traslado deberá contemplar las actividades de levantamiento de información, inventario, desinstalación, desanclaje, marcación, embalaje, transporte, instalación física, reconexión y validación de conectividad de los equipos objeto de traslado.
- El contratista deberá suministrar todos los recursos técnicos, logísticos y humanos necesarios para ejecutar el traslado seguro de la infraestructura tecnológica de la ANT.
- El servicio deberá incluir el traslado de racks, servidores, equipos de comunicaciones, almacenamiento, cableado y demás componentes tecnológicos definidos por la ANT.
- El contratista deberá garantizar que la infraestructura trasladada quede instalada, conectada y organizada dentro de los racks destino conforme a los diagramas, lineamientos y especificaciones entregadas por la ANT.

- La transición y puesta en disponibilidad de la infraestructura trasladada deberá ejecutarse conforme al cronograma acordado entre las partes y aprobado por la ANT, contemplando los tiempos requeridos para las actividades de traslado, instalación, validación y estabilización inicial de la infraestructura.
- El contratista deberá coordinar con los fabricantes de los equipos o sus representantes autorizados la validación de las buenas prácticas y recomendaciones técnicas para las actividades de apagado, desinstalación, traslado, encendido y puesta en disponibilidad de la infraestructura tecnológica objeto de traslado.
- En los casos en que el fabricante determine la necesidad de acompañamiento técnico especializado durante cualquiera de las etapas del proceso de traslado o puesta en disponibilidad, el contratista deberá asumir integralmente los costos asociados a dicho acompañamiento.
- El contratista deberá mantener registro y trazabilidad de los equipos durante todas las etapas del traslado, incluyendo inventario, seriales, ubicación y responsables de custodia.
- El contratista deberá garantizar que el personal involucrado en las actividades de traslado se encuentre plenamente identificado y autorizado para el desarrollo de las actividades correspondientes.

Materiales de Embalaje

- El contratista deberá utilizar materiales y elementos de protección adecuados para garantizar la integridad física de los equipos durante las actividades de traslado.
- Como mínimo, se deberán emplear los siguientes elementos:
  - Contenedores de protección con recubrimiento interno.
  - Fundas impermeables acolchadas.
  - Bolsas plásticas de protección.
  - Cintas de seguridad.
  - Etiquetas de identificación y trazabilidad.
- Y cualquier otro elemento de protección recomendado por el fabricante o requerido según las características de la infraestructura trasladada.

Alcance de la Operación Logística

- El contratista deberá ejecutar las actividades de desconexión física de enlaces LAN, WAN, SAN, elementos activos de red y acometidas eléctricas requeridas para el traslado.
- El contratista deberá realizar el embalaje y aseguramiento del hardware en contenedores o mecanismos de protección que mitiguen riesgos de golpes, vibraciones o daños físicos durante el transporte.
- El contratista deberá disponer de equipos y herramientas necesarias para las actividades de cargue y descargue, incluyendo montacargas cuando aplique.
- Los vehículos utilizados para el traslado deberán contar con sistema de rastreo y monitoreo GPS.
- El contratista deberá implementar medidas de seguridad física y custodia para la protección de la infraestructura tecnológica durante todas las etapas del traslado.
- El contratista deberá realizar el traslado, instalación física, montaje y reconexión de todos los componentes tecnológicos en el datacenter destino.
- El contratista deberá estimar y presentar el tiempo máximo de indisponibilidad asociado al proceso de traslado, el cual deberá ser previamente aprobado por la ANT de acuerdo con la complejidad y alcance de las actividades a ejecutar.
- El contratista deberá entregar documentación e informes relacionados con las actividades planificadas, ejecutadas y validadas durante el proceso de traslado.

Póliza de Transporte

- El contratista deberá contar con una póliza de transporte que cubra los equipos objeto del traslado durante todas las etapas de movilización.
- La póliza deberá contemplar como mínimo las siguientes coberturas:
  - Valor de reposición a nuevo.
  - Huelga.
  - Pérdida total.
  - Falta de entrega.
- En caso de requerirse ampliación de cobertura o ajuste de valores asegurados, el contratista deberá informar previamente a la ANT.
- La póliza podrá contemplar un deducible máximo del diez por ciento (10%) del valor de la pérdida.

Póliza de Montaje

- El contratista deberá contar con una póliza de montaje que cubra daños ocasionados durante las actividades de desmonte, embalaje, cargue, descargue, desembalaje, instalación y montaje de los equipos.
- El valor asegurado deberá corresponder al valor de reposición a nuevo de los equipos, con el fin de evitar condiciones de infraseguro.

La póliza podrá contemplar un deducible máximo del diez por ciento (10%) del valor de la pérdida y mínimo de tres (3) SMMLV.

CROSS CONEXIONES

El contratista deberá suministrar e instalar las cross conexiones necesarias tanto en fibra óptica como en cableado UTP categoría 6A, para la interconexión entre los racks de la Agencia Nacional de Tierras - ANT y también con los proveedores de servicios de comunicaciones, equipos de red y demás infraestructura asociada dentro del Datacenter.

Las cross conexiones en fibra óptica deberán ser tipo LC LC, en configuración dúplex, utilizando fibra multimodo OM3 u OM4 (50/125 µm) con cubierta LSZH (Low Smoke Zero Halogen), adecuadas para ambientes de Datacenter. Por su parte, las cross conexiones en cobre deberán ser en cableado UTP categoría 6A, con conductores 100 % cobre (no CCA), conectores RJ 45 en ambos extremos y cubierta tipo LSZH, cumpliendo con estándares para transmisión de datos hasta 10 Gbps (10GBASE T).

Tanto las cross conexiones como los patch cords asociados deberán ser certificados de fábrica y cumplir con estándares internacionales aplicables (ANSI/TIA 568.2 D, ANSI/TIA 568.3 D e ISO/IEC 11801), garantizando parámetros óptimos de desempeño, tales como baja pérdida de inserción, adecuada pérdida de retorno y estabilidad del enlace, asegurando la calidad, confiabilidad y continuidad de los servicios en entornos de centros de datos.

Las cross conexiones adicionales, es decir, aquellas requeridas con posterioridad al montaje inicial durante la ejecución contractual, serán suministradas bajo demanda, y su costo será asumido por la Entidad, previa aprobación de la supervisión del contrato.

ARRENDAMIENTO SWITCH DE CORE DE DISTRIBUCIÓN, EN ALTA DISPONIBILIDAD

La Agencia Nacional de Tierras – ANT requiere el suministro en modalidad de arrendamiento de dos (2) Switch Core de distribución en alta disponibilidad (HA), nuevos y no remanufacturados.

Los equipos ofertados no deberán encontrarse catalogados por el fabricante como End of Life (EoL), End of Sale (EoS) o End of Support (EoS) al momento de presentación de la oferta y durante la ejecución del contrato.

Características Técnicas Mínimas

- La solución deberá permitir operación activa-activa mediante tecnologías tipo MLAG, MC-LAG, VSX, vPC o equivalente.
- La solución deberá corresponder a una línea de switching de Datacenter del fabricante.

Puertos e Interfaces

- Cada switch deberá contar como mínimo con cuarenta y ocho (48) puertos 1G/10G SFP+.
- Los puertos SFP+ deberán ser compatibles tanto con módulos SFP+ LC como con adaptadores SFP+ RJ-45.
- El contratista deberá suministrar como mínimo:
  - Cuarenta y ocho (48) módulos SFP+ LC.
  - Cuarenta y ocho (48) adaptadores o módulos SFP+ RJ-45.
- Cada switch deberá contar con mínimo cuatro (4) puertos 1/10/50G SFP o superiores para uplinks o stacking.
- El contratista deberá incluir los respectivos cables y accesorios requeridos para la configuración de stack o alta disponibilidad entre los equipos.
- Cada equipo deberá contar con al menos un (1) puerto de consola USB-C y/o USB mini y/o puerto OOBM (Out of Band Management) para administración fuera de banda.
- Los módulos SFP suministrados deberán ser del mismo fabricante de los switches ofertados, con el fin de garantizar compatibilidad y soporte integral de la solución.

Capacidad y Rendimiento

- Cada switch deberá contar con una capacidad mínima de switching de ochocientos (800) Gbps.
- Cada switch deberá contar con un throughput mínimo de seiscientos (600) Mpps.

Sistema Operativo y Actualizaciones

- El sistema operativo de los equipos deberá incluir la versión más reciente, estable y soportada por el fabricante al inicio del contrato, incluyendo todas las funcionalidades, protocolos y capacidades soportadas por la plataforma ofertada.
- El contratista deberá garantizar, durante toda la ejecución del contrato, el acceso a actualizaciones, parches de seguridad y nuevas versiones liberadas por el fabricante sin costo adicional para la ANT.
- Todas las actividades de actualización deberán realizarse conforme a los procedimientos de gestión y control de cambios establecidos por la ANT.
- Para cualquier actualización, el contratista deberá presentar previamente un plan de trabajo y el respectivo MOP (Method of Procedure), los cuales deberán ser aprobados por la Entidad antes de su ejecución.
- El sistema operativo deberá estar orientado a ambientes de Datacenter y Core de misión crítica.

Fuentes de Alimentación

- Cada switch deberá contar con doble fuente de poder redundante tipo hot-swappable.
- Los equipos deberán mantener operación normal con una sola fuente activa en caso de falla de la otra fuente de alimentación.
- Las fuentes de poder deberán estar incluidas dentro del suministro, sin requerir adquisiciones adicionales por parte de la ANT.

Licenciamiento

- El contratista deberá suministrar todas las licencias, suscripciones, software y componentes requeridos para el correcto funcionamiento de la solución durante toda la vigencia del contrato.

Accesorios

- El contratista deberá incluir todos los accesorios necesarios para la instalación y operación de los equipos, incluyendo como mínimo:
  - Cables de alimentación compatibles con estándar eléctrico colombiano tipo B.
  - Soportes metálicos para instalación en rack.
  - Elementos de fijación.
  - Cables y accesorios necesarios para stacking, administración y puesta en operación.

Garantía y Soporte

- El contratista deberá garantizar soporte técnico y garantía directa con el fabricante durante toda la vigencia del contrato.
- El soporte deberá incluir atención de incidentes, reemplazo de hardware defectuoso y escalamiento con fabricante cuando aplique.

Instalación, Configuración, Administración y Soporte

- El contratista deberá realizar la instalación, configuración, administración y soporte de los equipos en las ubicaciones definidas por el supervisor del contrato.
- El contratista deberá configurar la solución en esquema de alta disponibilidad y garantizar su correcta integración con la infraestructura tecnológica de la ANT.
  - El contratista deberá generar usuarios nombrados con privilegios de administración total para personal autorizado de la ANT, sin que ello implique que la administración operativa de la plataforma sea asumida por la Entidad.

ARRENDAMIENTO DE SOLUCIÓN DE SWITCH SAN EN ALTA DISPONIBILIDAD (HA)

La Agencia Nacional de Tierras – ANT requiere el suministro en modalidad de arrendamiento de dos (2) Switch SAN nuevos, no remanufacturados, configurados en alta disponibilidad (HA).

Los equipos ofertados no deberán encontrarse catalogados por el fabricante como End of Life (EoL), End of Sale (EoS) o End of Support (EoS) al momento de presentación de la oferta y durante la ejecución del contrato.

Sistema Operativo y Actualizaciones

- El sistema operativo de los equipos deberá incluir la última versión estable, completa y soportada por el fabricante, vigente a la fecha de inicio del contrato, incluyendo todos los protocolos, servicios y funcionalidades compatibles con la plataforma ofertada.

- El contratista deberá garantizar que, durante toda la ejecución del contrato, los equipos permanezcan actualizados con las últimas versiones, correcciones y parches de seguridad liberados por el fabricante, sin costo adicional para la ANT.
- Las actualizaciones deberán contemplar como mínimo:
  - Versiones mayores y menores.
  - Parches de seguridad.
  - Correcciones críticas recomendadas por el fabricante.
- Todas las actualizaciones deberán alinearse con las buenas prácticas de la industria y recomendaciones oficiales del fabricante.
- Cualquier actividad de actualización deberá ejecutarse conforme a los procedimientos de gestión y control de cambios vigentes en la ANT.
- Para la ejecución de actualizaciones, el contratista deberá presentar previamente:
  - Plan de trabajo.
  - MOP (Method of Procedure).

  Los documentos anteriormente mencionados deberán ser aprobados previamente por la ANT antes de su ejecución.

Arquitectura de Alta Disponibilidad

- La solución deberá suministrarse en esquema de alta disponibilidad (HA), garantizando continuidad operativa ante fallas de hardware, energía o enlaces.
- La solución deberá incluir como mínimo:
  - Redundancia de componentes críticos.
  - Capacidad de operación sin interrupción ante falla de un componente o elemento de la solución.

Fuentes de Alimentación

- Cada switch deberá contar con doble fuente de poder redundante tipo hot-swappable.
- Los equipos deberán mantener operación normal con una sola fuente activa en caso de falla de la otra fuente de alimentación.
- Las fuentes de poder deberán estar incluidas dentro del suministro, sin requerir adquisiciones adicionales por parte de la ANT.

Licenciamiento

- En caso de requerirse licencias de software, habilitación de funcionalidades avanzadas, protocolos o suscripciones, estas deberán ser suministradas por el contratista durante toda la vigencia del contrato, sin costos adicionales para la ANT.

Módulos de Fibra Óptica y Puertos SAN

- Cada Switch SAN deberá contar con mínimo veinticuatro (24) puertos Fibre Channel habilitados y licenciados para operación.
- Los puertos Fibre Channel deberán soportar velocidades mínimas de treinta y dos (32) Gbps FC por puerto, con compatibilidad hacia velocidades inferiores soportadas por el fabricante.
- La solución deberá incluir todos los módulos de fibra óptica requeridos para la correcta operación de la infraestructura SAN.
- Los módulos suministrados deberán ser compatibles y certificados por el fabricante de la solución ofertada.
- El contratista deberá suministrar la cantidad necesaria de módulos y elementos de conectividad para garantizar operación completa en ambientes productivos y configuraciones de alta disponibilidad (HA).
- La solución deberá soportar operación wire-speed y non-blocking en todos los puertos Fibre Channel habilitados simultáneamente.

Accesorios

- El contratista deberá incluir todos los accesorios necesarios para la instalación y puesta en operación de la solución, incluyendo como mínimo:
  - Cables de alimentación compatibles con estándar eléctrico colombiano tipo B.
  - Soportes metálicos tipo rack mount.
  - Elementos de fijación.
  - Cables y accesorios necesarios para la correcta instalación en los racks existentes.

Garantía y Soporte

- La solución deberá contar con garantía y soporte directo con el fabricante durante toda la vigencia del contrato.
- El contratista deberá garantizar acceso a soporte técnico especializado para atención de incidentes y requerimientos asociados a la solución.
- El soporte deberá incluir reemplazo de hardware defectuoso conforme a las políticas y tiempos establecidos por el fabricante.

Instalación, Configuración, Administración y Soporte

- El contratista deberá realizar la instalación, configuración, administración y soporte de los equipos en las ubicaciones definidas por el supervisor del contrato.
- El contratista deberá configurar la solución en esquema de alta disponibilidad y garantizar su correcta integración con la infraestructura tecnológica de la ANT.
    - El contratista deberá generar usuarios nombrados con privilegios de administración total para personal autorizado de la ANT, sin que ello implique que la administración operativa de la plataforma sea asumida por la Entidad.

SUMINISTRO DE 25 MEMORIAS THINKSYSTEM

- La Agencia Nacional de Tierras – ANT requiere el suministro de veinticinco (25) memorias ThinkSystem 32GB TruDDR4 3200MHz (2Rx4 1.2V) RDIMM-A, con el fin de fortalecer y ampliar la capacidad de procesamiento y desempeño de la infraestructura tecnológica institucional.
- Las memorias suministradas deberán ser nuevas, originales de fábrica y no remanufacturadas.
- Las memorias deberán contar con garantía directa del fabricante con una vigencia mínima de un (1) año.

SUMINISTRO DE TARJETA HBA (HOST BUS ADAPTER) FIBRE CHANNEL

- La Agencia Nacional de Tierras requiere el suministro de cuatro (4) tarjetas HBA referencia Emulex 16Gb Gen6 FC Dual-port HBA, incluyendo sus respectivos módulos SFP FC de 16Gb compatibles, con el fin de garantizar la conectividad especializada y de alto desempeño entre la infraestructura HCI y el almacenamiento SAN institucional.
- Las tarjetas HBA suministradas deberán ser nuevas, originales de fábrica y no remanufacturadas.
- Las tarjetas HBA deberán contar con garantía directa del fabricante con una vigencia mínima de un (1) año.

1.13.2. Línea de servicios NOC/SOC.

SERVICIO NOC (NETWORK OPERATIONS CENTER) – MONITOREO DE INFRAESTRUCTURA TECNOLÓGICA 7X24X365 (ON-PREMISE Y SERVICIOS EN NUBE).

Se deben tener en cuenta las siguientes consideraciones técnicas para el cumplimiento de los estándares de disponibilidad y continuidad exigidos por la Entidad:

Área física e infraestructura del Datacenter:

- El Datacenter deberá contar con certificación vigente ICREA Nivel IV o superior, Tier III o superior, o certificación internacional equivalente que garantice alta disponibilidad, continuidad operativa y redundancia de infraestructura crítica.
- El Datacenter deberá contar con controles de acceso físico al área blanca mediante esquemas de seguridad multinivel y autenticación biométrica.
- El contratista deberá garantizar capacidad eléctrica de hasta quince (15) kVA por rack 3 rack y uno propio.
- El servicio deberá permitir alojar un rack propiedad de la ANT con las siguientes dimensiones y requerimientos eléctricos:
    - Altura: 2 metros.
    - Ancho: 70 cm.
    - Profundidad: 120 cm.
    - Requerimiento eléctrico: 51,6 amperios a 220V equivalente a 11,352 kVA.
- El Datacenter no deberá estar ubicado en zonas que representen riesgo para la continuidad operativa, incluyendo áreas de influencia aeronáutica o zonas de alto riesgo.

Manos remotas:

- El contratista deberá prestar servicio de manos remotas mediante personal técnico especializado disponible en modalidad 7x24x365.
- El servicio de manos remotas no deberá tener limitación en la cantidad de requerimientos solicitados por la ANT durante la ejecución del contrato.
- El servicio de manos remotas deberá incluir, como mínimo, las siguientes actividades:

- Reinicio de servidores y equipos.
- Conexión y desconexión de cables de red y energía.
- Validación de niveles de energía que le llegan a los dispositivos.
- Instalación y reemplazo de componentes de hardware.
- Verificación visual de equipos, indicadores y conexiones.
- Apoyo en la atención de incidentes básicos de hardware.
- Validación física de estado operativo de la infraestructura alojada.
- Apoyo mediante el préstamo de equipo de cómputo que permita el soporte remoto especializado hacia los equipos de la Agencia Nacional de Tierras - ANT, garantizando condiciones adecuadas de acceso, administración y diagnóstico de la infraestructura tecnológica. Dichos equipos deberán contar con las capacidades técnicas necesarias para la ejecución de actividades de monitoreo, configuración, gestión de incidentes y soporte sobre la red institucional.

- El contratista deberá garantizar la atención oportuna de los requerimientos de manos remotas con el fin de contribuir a la continuidad operativa y disponibilidad de los servicios tecnológicos institucionales.

Conectividad y Cross Conexiones en Datacenter

- El contratista deberá garantizar el acceso e interconexión con los proveedores de servicios de comunicaciones utilizados por la ANT al momento de la puesta en operación del servicio.
- El servicio deberá incluir todas las conexiones y cross conexiones requeridas desde las áreas de interconexión de los carriers o proveedores de comunicaciones hasta los racks asignados a la ANT, independientemente del tipo de medio o cableado requerido.
- El contratista deberá garantizar la disponibilidad de infraestructura de cableado y conectividad necesaria para la correcta integración de los servicios de comunicaciones de la ANT.
- El contratista deberá suministrar las cross conexiones necesarias para la interconexión inicial de los racks y carriers, incluyendo los patch cord certificados de cobre y fibra óptica requeridos para la correcta conexión e integración de los equipos de la Entidad dentro del servicio de colocation.

Informe Mensual del Servicio de Colocation

- El contratista deberá entregar mensualmente a la supervisión del contrato un informe detallado de la operación y prestación del servicio de colocation correspondiente al período evaluado.
- El informe mensual deberá incluir como mínimo la disponibilidad del servicio de colocation y el detalle de las interrupciones o indisponibilidades presentadas durante el período, indicando fecha, duración, causa y acciones ejecutadas.
- El contratista deberá reportar los eventos asociados a la infraestructura de soporte del datacenter que hayan afectado o podido afectar la prestación del servicio, incluyendo eventos relacionados con sistemas eléctricos, UPS, PDU, plantas eléctricas, climatización y conectividad.
- El contratista deberá informar la relación de incidentes, requerimientos y solicitudes de soporte atendidas durante el período, incluyendo tiempos de atención, solución y estado de los casos registrados.
- El contratista deberá incluir en el informe mensual el registro de mantenimientos preventivos, correctivos o actividades programadas que hayan involucrado o impactado los servicios prestados a la ANT.
- El contratista deberá reportar los accesos físicos realizados al datacenter relacionados con la infraestructura de la ANT, indicando fecha, personal autorizado y actividad ejecutada.
- El contratista deberá presentar el estado de utilización de los recursos contratados asociados al servicio de colocation, incluyendo ocupación de racks, consumo eléctrico y capacidad disponible.
- El contratista deberá reportar el cumplimiento de los acuerdos de niveles de servicio (ANS) establecidos contractualmente, incluyendo indicadores, desviaciones, eventos relevantes y acciones de mejora implementadas.
- El contratista deberá informar cualquier riesgo, incidente o condición técnica que pueda afectar la continuidad, disponibilidad o adecuada prestación del servicio de colocation.
- El contratista deberá entregar junto con el informe mensual las recomendaciones técnicas y operativas que considere pertinentes para garantizar la adecuada prestación y continuidad del servicio.

Niveles de Servicio y Tiempos de Atención Mínimos Requeridos

- El contratista deberá garantizar una disponibilidad mensual mínima del servicio de colocation acorde con el nivel de certificación ofertado para el datacenter, la cual no podrá ser inferior al noventa y nueve punto novecientos ochenta y dos por ciento (99,982%) mensual para infraestructura Tier III o ICREA Nivel IV.

- El servicio deberá garantizar operación continua 7x24x365 sobre la infraestructura de soporte del datacenter, incluyendo suministro eléctrico, climatización, conectividad y sistemas asociados a la prestación del servicio de colocation.
- El servicio deberá contar con esquemas de redundancia eléctrica y de climatización acordes con la certificación del datacenter ofertado, incluyendo sistemas UPS, plantas eléctricas y sistemas de refrigeración redundantes.
- El servicio deberá disponer de mesa de servicio y canales de atención operativos 7x24x365 para la recepción, gestión y escalamiento de incidentes, requerimientos y solicitudes relacionadas con el servicio contratado.
- Para incidentes críticos que afecten total o parcialmente la disponibilidad del servicio de colocation, energía, climatización o conectividad asociada a los servicios contratados, el contratista deberá garantizar un tiempo máximo de atención inicial de quince (15) minutos y un tiempo máximo de escalamiento de treinta (30) minutos.
- Para incidentes de severidad alta que generen degradación parcial de los servicios contratados, el contratista deberá garantizar un tiempo máximo de atención inicial de treinta (30) minutos.
- Para incidentes de severidad media o solicitudes operativas programadas, el contratista deberá garantizar un tiempo máximo de atención inicial de cuatro (4) horas.
- Para solicitudes administrativas o requerimientos de baja severidad, el contratista deberá garantizar un tiempo máximo de atención de un (1) día hábil.
- El contratista deberá garantizar disponibilidad permanente para la coordinación y autorización de acceso al datacenter por parte del personal autorizado por la ANT.
    - El contratista deberá contar con procedimientos formales de gestión y escalamiento de incidentes, garantizando trazabilidad, registro y seguimiento de los eventos reportados.

LICENCIAMIENTO PRTG NETWORK MONITOR

La Agencia Nacional de Tierras – ANT requiere el suministro de licenciamiento oficial de la plataforma Paessler PRTG Network Monitor para el monitoreo y supervisión de la infraestructura tecnológica institucional.

Características mínimas requeridas

- Producto: Paessler PRTG Network Monitor.
- Cantidad mínima: Diez mil (10.000) sensores.
- Modalidad de licenciamiento: Suscripción.
- Vigencia mínima: Un (1) año.
- El licenciamiento deberá incluir derecho de actualización de versiones durante toda la vigencia contractual.
- El contratista deberá garantizar acceso a:
    - Parches de seguridad.
    - Nuevas versiones.
    - Actualizaciones liberadas por el fabricante durante la vigencia de la suscripción.
- La solución deberá contar con soporte técnico del fabricante o canal autorizado durante toda la vigencia contractual.

Funcionalidades mínimas requeridas

- La solución deberá permitir el monitoreo y supervisión de:
    - Dispositivos de red.
    - Servidores físicos y virtuales.
    - Equipos de seguridad.
    - Plataformas de virtualización.
    - Servicios en nube.
    - Aplicaciones.
    - Infraestructura tecnológica de la entidad.
- La herramienta deberá soportar como mínimo los siguientes protocolos y capacidades de monitoreo:
    - SNMP.
    - WMI.
    - ICMP.
    - NetFlow.
    - Syslog.
    - APIs y demás funcionalidades compatibles con la plataforma ofertada.
- La solución deberá permitir:
    - Generación de alertas automáticas.

- Dashboards y visualización gráfica.
- Generación de reportes históricos y en tiempo real.
- Configuración de umbrales y notificaciones.
- Gestión centralizada de monitoreo.

- La plataforma de monitoreo suministrada será de uso exclusivo de la ANT y deberá permanecer bajo administración y control directo de la Entidad.
- El contratista del servicio NOC no deberá contar con acceso administrativo sobre la herramienta, salvo autorización expresa de la ANT para actividades específicas de soporte técnico previamente aprobadas.
- La plataforma será utilizada por la ANT como mecanismo independiente de supervisión, validación y control de la operación del servicio NOC, permitiendo verificar la correcta detección, gestión y escalamiento de eventos, alertas e incidentes sobre la infraestructura tecnológica monitoreada.
- El contratista deberá realizar la instalación, configuración y puesta en funcionamiento de la solución sobre el servidor suministrado por la Entidad.

SERVICIOS DE IMPLEMENTACIÓN Y TRANSFERENCIA CONOCIMIENTO

El contratista deberá realizar una transferencia de conocimiento a 15 personas designadas por la ANT de mínimo ocho (8) horas sobre la administración y operación básica de la herramienta.

SUSCRIPCIÓN ARUBA CENTRAL FOUNDATION PARA SETENTA Y UN (71) ACCESS POINTS – POR UN (1) AÑO

setenta y un (71) Access Points, con vigencia de un (1) año. La suscripción deberá habilitar la administración centralizada de los dispositivos, monitoreo de la infraestructura inalámbrica, gestión de configuraciones, actualización de firmware, generación de alertas, elaboración de reportes y acceso a las funcionalidades correspondientes al licenciamiento Foundation del fabricante.

RENOVACIÓN DE SOPORTE PARA DOS (2) SWITCHES CORE ARUBA 5406 ZL2 FOUNDATION CARE 4H EXCHANGE – POR UN (1) AÑO

Renovación del servicio de soporte Foundation Care 4H Exchange para dos (2) switches Core Aruba 5406 zl2, con vigencia de un (1) año. El servicio deberá incluir soporte técnico especializado del fabricante, acceso a actualizaciones de software y firmware, gestión de incidentes y reemplazo avanzado de hardware con tiempo de respuesta de cuatro (4) horas, conforme a las condiciones del fabricante

SUMINISTRO EN MODALIDAD DE ARRENDAMIENTO DE QUINCE (15) ACCESS POINTS, SOPORTE POR UN (1) AÑO, DEBE INCLUIR SERVICIO DE INFRAESTRUCTURA PARA SU PUESTA EN MARCHA

Suministro en modalidad de arrendamiento de quince (15) Access Points Fortinet FAP431G, toda vez que actualmente la infraestructura de la agencia cada uno con su respectivo Power Injector (Inyector PoE), incluyendo soporte del fabricante por un (1) año. El contratista deberá realizar la instalación, configuración y puesta en funcionamiento, incluyendo la infraestructura necesaria para su correcta operación, de los equipos solicitados en arrendamiento en la sede donde sea requerido por parte del supervisor del contrato.

En la sede de Chapinero actualmente se cuenta con una infraestructura de red inalámbrica basada en tecnología Fortinet, donde los puntos de acceso (Access Points) son administrados de forma centralizada por los equipos de seguridad perimetral (firewalls FortiGate) ya instalados y en operación. Esta integración permite gestionar de manera unificada la configuración, monitoreo, autenticación de usuarios, aplicación de políticas de seguridad, control de acceso y actualización de los dispositivos inalámbricos.

En consecuencia, la adquisición en modalidad de arrendamiento de Access Points de una marca diferente implicaría la pérdida de compatibilidad con la plataforma de administración existente, generando la necesidad de incorporar controladores adicionales, nuevas licencias, capacitación técnica y procesos paralelos de administración, lo que incrementaría los costos operativos y la complejidad de la infraestructura tecnológica.
Adicionalmente, el uso de equipos Fortinet FAP431G garantiza la interoperabilidad con la plataforma actualmente implementada en la dicha sede permitiendo aprovechar las capacidades de gestión y seguridad ya adquiridas, mantener la estandarización tecnológica institucional y asegurar la continuidad de los servicios inalámbricos sin afectar la operación de los usuarios.

Por lo anterior, la selección de esta marca no obedece a una preferencia comercial, sino a una necesidad técnica derivada de la infraestructura existente, buscando garantizar la compatibilidad, la continuidad del servicio, la eficiencia operativa y la protección de la inversión tecnológica previamente realizada por la Entidad.

SERVICIO DE MONITOREO CONTINUO BAJO MODALIDAD SAAS, ENFOCADO EN LA PROTECCIÓN DE MARCA Y LA GESTIÓN DE LA SUPERFICIE DE ATAQUE EXTERNA

Servicio de monitoreo continuo de riesgos digitales bajo modalidad SaaS por doce (12) meses, para la protección de dos (2) dominios institucionales y sus activos asociados (subdominios, direcciones IP públicas, buckets y repositorios de código). La solución deberá operar bajo tecnología agentless, incorporando capacidades de Digital Risk Protection (DRP) y External Attack Surface Management (EASM), monitoreo de Deep Web y Dark Web, detección de phishing, typosquatting, exposición de credenciales y filtraciones de información, así como la ejecución de cuatro (4) acciones de desactivación (takedown). Deberá incluir repositorio seguro de evidencias con integridad criptográfica, paneles de monitoreo y gestión de alertas, cumplimiento de ISO/IEC 27001:2022 y alineación con NIST CSF 2.0, soporte técnico especializado 24x7x365 en español e inglés, implementación en un plazo máximo de diez (10) días calendario y cuatro (4) sesiones de transferencia de conocimiento.

SERVICIO SOC (SECURITY OPERATIONS CENTER) – MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA 7X24X365 (Onpremise - Servicios en Nube).

Monitoreo en horario 7x24X365 por la vigencia pactada.

- La Agencia Nacional de Tierras - ANT requiere contar con un servicio SOC bajo esquema 7x24x365 para el monitoreo y gestión de la infraestructura tecnológica, tanto en ambientes on-premise como en nube, con el fin de garantizar la disponibilidad, estabilidad, desempeño y continuidad de los servicios tecnológicos de la Entidad.
- El servicio deberá incluir el monitoreo y correlación de eventos de seguridad sobre la plataforma SIEM adquirida por la Entidad, para 275 dispositivos con agente SIEM a nivel nacional y 100 agentes avanzados (FIM) durante la ejecución del contrato; entre los cuales se detallan: Servidores, Hipervisores, Firewalls, Switch de Core, Switches de Acceso, Firewall de aplicaciones y Balanceadores de carga.
- De igual forma el servicio deberá incluir la atención y gestión de incidentes de interrupción del monitoreo – SOC y el correspondiente escalamiento al equipo de respuesta a incidentes de seguridad de la entidad, dando cumplimiento a los acuerdos de niveles de servicio requeridos.
- Se debe prestar acceso a la solución desde un centro de monitoreo ubicado en la ciudad de Bogotá D.C. (Colombia). La conexión hacia la herramienta de correlación de la Entidad se realizará a través de una conexión segura utilizando internet. Las comunicaciones requeridas se realizarán a través de conexiones seguras VPN.
- La solución de monitoreo SOC se debe poder realizar en forma remota y disponer un personal en sitio cuando se requiera el cumplimiento de acuerdos de nivel de servicio para eventos o incidentes críticos.
- El monitoreo se entenderá activo y vigente únicamente cuando culmine la etapa de Diseño, integración y configuración del servicio
- La Entidad requiere servicios de un Centro de Operaciones de Seguridad (Security Operations Center – SOC), el servicio de SOC será realizado sobre las herramientas SIEM adquiridas por la Entidad.
- Diseño, integración y configuración del servicio: una (1) semana contada a partir de la suscripción del acta de inicio, para lo cual deberá presentar para aprobación del supervisor del contrato, y dentro de los cinco (5) días hábiles siguientes a la fecha de suscripción del acta de inicio los siguientes documentos:
    - Plan de trabajo que contenga la relación de actividades, responsables, definición de entregables, diagramas de la prestación del servicio, etapas, resultados esperados, estrategias para la prestación del servicio SOC, allí se deberá relacionar los tiempos establecidos y describir los procesos/procedimientos, las técnicas y herramientas que se utilizarán en la ejecución del contrato.
    - Documento donde se consigne el esquema de interno de escalamiento del servicio SOC.
    - Cronograma de actividades donde se establezcan los hitos y las fechas límite para la entrega de actividades.
    - Dentro del plan de trabajo deberá especificar la metodología que utilizará para administrar, configurar, monitorear y gestionar el servicio de monitoreo objeto del presente contrato, especificando etapas, recursos, entregables, herramientas y técnicas a utilizar La Entidad se reserva el derecho de ajustar aspectos de la metodología.
- La actividad del servicio de monitoreo SOC, se centrará en el tratamiento de eventos, identificación de incidentes, los cuales contarán con un conjunto de metodologías y atención de procesos que permitirá brindar el alertamiento oportuno a los riesgos y amenazas. Por lo anterior, el personal del servicio deberá realizar el escalamiento y las comunicaciones por medio de correo electrónico y/o telefónico con el personal de seguridad de la información de la Entidad a fin de comunicar las incidencias presentadas. Adicionalmente realizará el seguimiento a los eventos e incidentes hasta que estos sean cerrados adecuada y oportunamente.
- De forma permanente el servicio de monitoreo SOC realizará una valoración de las amenazas existentes en la región y el mundo, determinando cuál de estos exponen a un riesgo a la Entidad, resumiendo los resultados en Boletines o Informes extraordinarios de SOC. Los servicios de gestión de SOC realizarán seguimiento 7x24x365 a los ataques originados desde Internet al igual que los originados al interior de la Entidad. El SOC,

debe definir la matriz de escalamiento de común acuerdo con los responsables de seguridad en la Entidad, clarificando el nivel de escalamiento según el tipo y nivel de incidente.

- El SOC debe incluir en el monitoreo las funcionalidades de: Firewall, IPS, Control de Aplicaciones, Filtrado Web, Antivirus perimetral, SDWAN y DLP, Port Security, alertar cambios de conexión y configuración, MAC Filtering, Identificar y solicitar bloqueo de direcciones MAC no conocidas. Junto con las capacidades máximas técnicas definidas por el fabricante de los appliances y servicios utilizados Se deberá proporcionar una cuenta de acceso a los servicios en modo lectura a todas las configuraciones, donde la Entidad podrá dar seguimiento a las actividades realizadas por el oferente.
- La solución SOC, debe proporcionar dos (2) equipos de cómputo para uso exclusivo del área de seguridad de la información y ciberseguridad los cuales establecen la necesidad de incluir un repositorio de análisis de servicio y un equipo de cómputo para dichos análisis, las especificaciones serían un sistema de cómputo con almacenamiento de mínimo 20TB y un equipo de cómputo para la virtualización de los ambientes para análisis. Dichos equipos deberán contar con las siguientes características:
    - Un (1) equipo de cómputo o almacenamiento afín con 64gb de RAM, un CPU de 8 núcleos, y un almacenamiento de Mínimo 20TB en raid 6. Ubuntu 24.04
    - Un (1) equipo de cómputo con 128gb de RAM un CPU de 16 núcleos y un almacenamiento de 2Tb. Ubuntu 24.04
- El contratista deberá realizar la correlación, monitoreo y casos de uso sobre la plataforma de la Entidad, de tal forma que todo el know how y parametrizaciones queden para la Entidad. En ningún caso la información de log deberá salir de la Entidad. El monitoreo se hará cumpliendo estrictamente las políticas de seguridad de la información y ciberseguridad y se ajustará a cualquier cambio que suceda en ellas dentro de la vigencia del monitoreo.
- Cuando un evento de seguridad ocurre o está en suceso, el servicio de monitoreo SOC deberá identificarlo y estar en la capacidad de relacionar de forma directa o indirecta con otros eventos de seguridad asociados, determinando el patrón de ataque. El contratista deberá administrar las soluciones SIEM que sean adquiridas por la Entidad, incluyendo la gestión de cambios sobre las soluciones SIEM y aquellas enlazadas al SIEM administradas o desplegadas por el contratista. Así mismo, deberá suministrar el servicio de monitoreo de la infraestructura tecnológica, utilizando para ello las soluciones de tipo SIEM que sean adquiridas por la Entidad, durante la vigencia del monitoreo. Para ello el contratista deberá desarrollar un plan de trabajo, dicho documento entregado y actualizado por el contratista deberá contener las etapas, resultados esperados, estrategias para asegurar el logro de los requerimientos en los tiempos establecidos y describir los procesos/procedimientos, las técnicas y herramientas que utilizará en la ejecución del contrato.
- Las herramientas SIEM que serán adquiridas por la Entidad, serán administradas y operadas por el contratista, con personal con experiencia en servicios de monitoreo de logs. La actividad de monitoreo y alertamiento se debe hacer en las instalaciones del contratista
- Las herramientas adicionales que deba utilizar el contratista deben ser compatibles con las herramientas SIEM de propiedad de la Entidad.
- La configuración de cambios o requerimientos solicitados sobre la plataforma SIEM deberán ser gestionados en máximo 24 horas, previa aceptación de la ventana. Para casos de alta complejidad se definirán los tiempos específicos para estas configuraciones.
- La solución debe permitir la integración del envío de alarmas automáticas vía correo electrónico.
- Proporcionar durante el período de la operación de los servicios un esquema de escalamiento interno en eventos de uso configuración y funcionamiento de la herramienta SIEM.
- Los procesos de gestión y operación deben estar basados en las mejores prácticas establecidas por los modelos de procesos ITIL, CSIT, ISO 27001:2022, NIST (CSF) o CERT.
- La solución deberá alinearse a las políticas, procesos, procedimientos y requerimientos de seguridad definidos por la Entidad, como mínimo deberán observarse las resoluciones, directrices y lineamientos del Ministerio del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia MINTIC y los controles del anexo A de la norma técnica ISO 27001.
- La solución debe incluir apoyo en la definición de estrategias de seguridad, que permitan fortalecer las políticas y controles de seguridad de la información y mantener el inventario actualizado de dispositivos monitoreados de la solución SIEM.
- La solución debe detectar actividades, técnicas inusuales y recolectar evidencias necesarias para determinar si se trata de un evento o incidente de seguridad, de acuerdo con los niveles de servicio.
- Las evidencias que sean recopiladas por el servicio de monitoreo SOC son propiedad de la Entidad y podrán ser solicitadas en cualquier momento para atención de requerimientos legales. El servicio debe detectar

actividades, técnicas inusuales y recolectar evidencias necesarias para determinar si se trata de un evento o incidente de seguridad, de acuerdo con los niveles de servicio.

- La solución de monitoreo SOC deberá analizar las diferentes alertas detectadas para descartar falsos positivos, antes de crear el caso/ticket en la herramienta institucional dispuesta para ello.
- Las herramientas adicionales que deba utilizar el contratista, tales como hardware, software, firmware, utilitarios o appliances, deben cumplir con la regulación de derechos de autor y propiedad intelectual. Así mismo, deben contar con soporte, mantenimientos y actualizaciones del fabricante o proveedor.
- Se deben generar alertas de otras amenazas que puedan impactar la infraestructura de la Entidad, como las identificadas en los reportes de análisis de tendencia de centros SIRT/CERT o en las bases de datos de conocimiento del contratista.
- El centro de operación del contratista debe garantizar condiciones de seguridad mínimas en aspectos de acceso al espacio físico y acceso a las herramientas de software.
- El servicio de monitoreo SOC deberá mantener sincronizados todos los relojes de la herramienta SIEM con la hora legal colombiana, suministrada por el Instituto Nacional de Metrología de Colombia (https://inm.gov.co/web/servicios/hora-legal/).
- La solución de monitoreo SOC debe ejecutar actividades permanentes para garantizar el descubrimiento y monitoreo de nuevos dispositivos en la red. - El tiempo de custodia de los reportes, estadísticas, análisis de tendencia, métricas e indicadores será por la duración del contrato. Una vez terminado el vínculo contractual, el contratista deberá entregar toda la información a la que tuvo acceso de la Entidad y posteriormente cifrarla y destruirla entregando una certificación de Borrado/Destrucción Segura, en todos los elementos técnicos utilizados para la prestación del servicio.
- Para el cumplimiento de los niveles de servicio solicitados, el contratista dispondrá del personal mínimo establecido en el presente anexo.
- En caso de requerirse personal adicional para cumplimiento de los tiempos de atención, se deberá suministrar sin costo adicional para la Entidad.
- La Agencia Nacional de Tierras - ANT, requiere para su servicio de SOC capacidades de protección la superficie de ataque externa, el cual permita identificar todos los activos conectados al internet, de la misma forma que vulnerabilidades, malas prácticas de configuración, problemas con certificados y protocolos de encriptación y conocer dominios asociados que puedan ser utilizados para realizar ataques de suplantación de identidad.

1. Infraestructura para monitorear:

Se requiere una solución de monitoreo y correlación de eventos de seguridad sobre la plataforma SIEM adquirida por la Entidad, para 275 dispositivos con agente SIEM a nivel nacional y 100 agentes avanzados (FIM) durante la ejecución del contrato.

- Servidores:
  - Servidores Windows: Todos los servidores físicos e instancias de máquina virtual y de Nube
  - Servidores Linux: Todos los servidores físicos e instancias de máquina virtual y de Nube
  - Hipervisores: Todos los nodos de Administración ESX, EXSi y similares on-prem o Nube
  - Firewalls: todos los Firewalls FortiGate
  - Switch Core: todos los Switch Core ARUBA
  - Switches de Acceso: todos los Switches de Acceso
  - Firewall de aplicaciones: todos lo WAFs

- Balanceadores de carga: todos lo Balanceadores de Carga incluyendo pero sin limitarse a:

  - FortiGate 601E
  - FortiWeb 1000E
  - FortiADC 2000F
  - FortiSIEM VM
  - FortiSandBox 1000F
  - FortiManager 200D
  - FortiDDoS 200B
  - FortiAnalyzer 400E

Se debe integrar el componente Fortinet que adquiera en el futuro la ANT conforme al licenciamiento con el que cuente el SIEM de la ANT.

- Dispositivos Adicionales: La Entidad solicitará incluir la cantidad de dispositivos adicionales que requiera hasta ocupar todo el licenciamiento de la herramienta SIEM adquirida por la Entidad. La herramienta SIEM tiene capacidad de sin limitarse a la presente descripción:
  - Rápida capacidad de respuesta ante eventos.
  - Capacidad de automatización, por medio de power app, scripts y APIs. o Escalabilidad e integraciones, con AD, ENTRA ID, IPS, Gestión de ciberexposisción, Herramientas SAST y DAST, Antivirus, Antispam,
  - AntiPhishing.
  - Cumplimiento de regulaciones de seguridad de datos, debe adherirse a los requisitos de confidencialidad y privacidad de la ANT y todos aquellos aplicables legalmente.
  - Monitoreo de infraestructuras OnPremise y en la nube de Azure

- La solución debe mantener el inventario actualizado de dispositivos monitoreados.
- El contratista realizará la integración y monitoreo de los dispositivos y activos tecnológicos que conforman la infraestructura tecnológica de la Entidad, según lo relacionado en la Infraestructura a ser monitoreada, del presente Anexo técnico.
- Una vez integrada toda la plataforma tecnológica, el contratista configurará y afinará la herramienta de correlación para mejorar su funcionalidad, tomando como base al menos los siguientes eventos:
  - Actividades asociadas a la administración de cuentas de usuario final (UserID)
  - Actividades asociadas a cuentas de altos privilegios, automáticas de procesos o asignadas a usuarios administradores (root, sa, administrator).
  - Ejecución de comandos especiales sobre sistemas operativos.
  - Ejecución de comandos especiales sobre bases de datos (dump, drop, delete, insert, update)
  - Cambios de parámetros técnicos, de configuración o de seguridad de todas las herramientas de control y monitoreo, incluyendo, pero sin limitarse a IPS, Antivirus y Antispyware/Antibot.
  - Cambios de configuración horaria.
  - Cambios no autorizados en recursos tecnológicos críticos
  - Actividades de conexión de cuentas de usuario final o administradores. o Actividades asociadas a manipulación de bitácoras técnicas (LOGs) o interrupciones en el envío de los LOGs.
  - Actividades asociadas a conexión de acceso remoto.
  - Actividades de acceso a servicios web no autorizados a nivel público, redes sociales, apps tipo cloud storage, contenidos maliciosos o prohibidos, entre otros definidos en las políticas de control de
  - navegación.
  - o Actividades que alteren, modifiquen o impidan, mediante ciberataques, el correcto funcionamiento de las aplicaciones Core de la entidad tales como ARGIS, Klic, Orfeo, CRM, Ecard, Aranda.

Servicio Especializado SOC por Demanda – Bolsa de 10 horas al mes

Es el servicio de un equipo especializado de un Centro de Operaciones de Seguridad (SOC) para prestar servicios de soporte en ciberseguridad, conforme a las necesidades de la Entidad. La prestación del servicio se realizará mediante una bolsa de hasta diez (10) horas, destinadas a actividades como análisis de incidentes de seguridad, investigación de alertas, acompañamiento en la contención y respuesta a incidentes, análisis forense inicial, asesoría técnica y demás actividades especializadas asociadas a la operación de seguridad de la información.

SERVICIOS ESPECIALIZADOS DE ANÁLISIS FORENSE EN CIBERSEGURIDAD – SERVICIO POR DEMANDA – BOLSA DE 100 HORAS

El servicio de Monitoreo SOC integrará los logs de administración de la aplicación de gestión de vulnerabilidades de la agencia, siempre que se pueda automatizar por medio de API y que el SIEM permita dicha integración, con mínimo privilegio. Para lo cual el equipo de seguridad de la Entidad establecerá los accesos pertinentes al uso exclusivo de la API, siempre que se cumplas dichas condiciones, sin conceder acceso con login interactivo a la solución.

El servicio de monitoreo SOC deberá estar en la capacidad de integrar herramientas de ciberseguridad entre las que se podrían encontrar, pero no se limitan a: Prevención de Pérdidas de datos (DLP, por sus siglas en inglés), Gestión de Acceso de Identidades (IAM, por sus siglas en inglés), Gestión de bóvedas de contraseñas, control de navegación web, ZTNA y SOAR.

- Un (1) equipo de cómputo o almacenamiento afín con 64gb de RAM, un CPU de 8 núcleos, y un almacenamiento de Mínimo 20TB en raid 6. Ubuntu 24.04

- Un (1) equipo de cómputo con 128gb de RAM un CPU de 16 núcleos y un almacenamiento de 2Tb. Ubuntu 24.04

El contratista deberá suministrar, instalar, configurar y poner en operación la infraestructura de cómputo requerida para soportar las actividades de gestión, monitoreo, análisis de eventos de seguridad de la información y la ejecución de pruebas técnicas de seguridad, garantizando que los equipos cuenten con las características mínimas que se describen a continuación:

a. Equipo para almacenamiento y procesamiento de información de seguridad:

- Un (1) equipo de cómputo o servidor de almacenamiento con mínimo sesenta y cuatro (64) GB de memoria RAM.
- Procesador con mínimo ocho (8) núcleos.
- Capacidad de almacenamiento útil mínima de veinte (20) TB, configurada en **RAID 6**, con el fin de proporcionar tolerancia a fallos, integridad y disponibilidad de la información.
- Sistema operativo **Ubuntu Server 24.04 LTS** o superior compatible.

b. Equipo para análisis y ejecución de pruebas de seguridad:

- Un (1) equipo de cómputo con mínimo ciento veintiocho (128) GB de memoria RAM.
- Procesador con mínimo dieciséis (16) núcleos.
- Almacenamiento de estado sólido (SSD) con capacidad mínima de dos (2) TB.
- Sistema operativo **Ubuntu 24.04 LTS** o superior compatible.

SOAR - Subscripción Version SaaS (Cloud) por 12 Meses para 2 Administradores

Prestar el servicio de arrendamiento de licenciamiento SOAR para las integraciones con sistemas y servicios de ciberseguridad e infraestructura TI compatible con la arquitectura actual de la entidad. El servicio debe incluir puesta en operación de la herramienta y la transferencia de conocimiento asociada y requerida por la entidad para su operación.

Renovación Licenciamiento de dos (2) FW 1800F por (1) año.

El contratista deberá gestionar y suministrar la renovación del licenciamiento por un período de un (1) año para dos (2) dispositivos Firewall FortiGate 1800F ubicados en el CAN , garantizando la continuidad de las funcionalidades de seguridad, el acceso a actualizaciones, soporte del fabricante y los servicios asociados al licenciamiento vigente.

La renovación deberá contemplar, como mínimo, la continuidad de los servicios contratados para los equipos, incluyendo las suscripciones, bases de firmas, actualizaciones de software y firmware, inteligencia de amenazas, así como las funcionalidades de seguridad habilitadas conforme al esquema de licenciamiento actualmente implementado por la Entidad.

El contratista deberá asegurar que la renovación se realice sin afectar la operación de los dispositivos, evitando interrupciones en la prestación del servicio y garantizando la vigencia ininterrumpida de las licencias durante el período contratado.

Como parte del servicio, el contratista deberá entregar la documentación que acredite la renovación, incluyendo los certificados o comprobantes de licenciamiento emitidos por el fabricante o distribuidor autorizado, así como la información correspondiente a la vigencia y cobertura del soporte asociado

CATEGORÍAS DE EVENTOS DE SEGURIDAD, MÍNIMOS PARA MONITOREAR SOC

- Cuentas Privilegiadas
  a. El SOC debe integrar sus herramientas de monitoreo con el Directorio Activo y ENTRA ID de la entidad. EL SOC debe Monitorear las integraciones con Microsoft Windows Active Directory o ENTRA ID y todas las conexiones a servicios “Single-Sign-On”.
  b. Autenticación fallida.
  c. Autenticación exitosa.
  d. Usuario agregado a grupo especial local (cambio de privilegios).
  e. Usuario eliminado de grupo especial local (cambio de privilegios).
  f. Usuario agregado a grupo especial global (cambio de privilegios).
  g. Usuario eliminado de grupo especial global (cambio de privilegios).
  h. Cuenta bloqueada.
  i. Cuenta desbloqueada.
  j. Contraseña cambiada.
  k. Cambios de perfiles y permisos de cuentas privilegiadas.
  l. Actividades de administración de cuentas (creación, eliminación, cambio de perfiles).
  m. Elevación de privilegios a usuarios.

n. Ataques de Kerberoasting y otros relacionados a ActiveDirectory/ENTRA ID
o. Deshabilitación de MFA.
p. Sesiones concurrentes en diferentes equipos o desde ubicaciones geográficas que excedan la georreferencia de las zonas de FW en las redes MPLS y redes públicas.

- Bases de datos
  a. Autenticación exitosa - cuenta ordinaria.
  b. Autenticación fallida - cuenta ordinaria.
  c. Autenticación exitosa – SA.
  d. Autenticación fallida – SA.
  e. Cuenta bloqueada.
  f. Cuenta desbloqueada.
  g. Usuario agregado al grupo de SA.
  h. Ejecución de instrucciones DML (Insert, Update y Delete) sobre tablas en producción por usuarios no autorizados
  i. Ejecución de instrucciones DDL (Copia, (dump), Create, Drop, Alter) sobre tablas en producción por usuarios no autorizados.
  j. Acceso de desarrolladores.
  k. Actualización de cuentas.
  l. Activación o uso de cuentas por defecto.

- Cambios sobre plataformas - Windows
  a. Software instalado en Servidor Windows.
  b. Software desinstalado en Servidor Windows.
  c. Archivo crítico modificado (control de integridad).
  d. Cambio en políticas del Directorio Activo y ENTRA ID.
  e. Modificación y eliminación de logs de auditoría.

- Cambios sobre plataformas - Linux
  a. Software instalado en Servidor Linux.
  b. Software desinstalado en Servidor Linux.
  c. Archivo crítico modificado (control de integridad).
  d. Modificación y eliminación de logs de auditoría.
  e. Modificación de políticas de aseguramiento y SeLinux.

- Monitoreo IAM- PAM
  a. Alertamiento y correlación de eventos relacionados con Entra ID y Office 365 en todos sus licenciamientos
  b. Monitoreo Domain Controllers, incluyendo pero sin limitarse a:
     - puertos para DCs: 88 - 53 - 3268-3269 - 389 - 135 - 137-139 - 123 - 636 - 445 - 1024-65535
     - Creación de usuario 4720
     - Eliminación de usuario 4726
     - Cambio de grupo 4728 / 4732
     - Login exitoso 4624
     - Login fallido 4625
     - Uso de privilegios 4672

- Conexiones
  a. Acceso remoto.
  b. Cantidad inusual de conexión a los dispositivos, equipos, servidores y base de datos.
  c. Tráfico inusual en protocolos SMB, SMTP, SNMP, NTLM, LLMNR de salida o entrada en servidores y otros hosts dentro de la red.

- Comportamiento sospechoso
  a. Ataques de fuerza bruta.
  b. Instalación o descarga de software no autorizado.
  c. Acceso no autorizado a carpetas restringidas.
  d. Patrones de virus informáticos o códigos maliciosos.

e. Ejecución de secuencia de operaciones y/o transacciones sobre los sistemas de información que pueden implicar fraudes
f. Modificación a los tipos de archivo permitidos en las carpetas compartidas.

- Auditoría
  a. Cambios de parámetros de seguridad
  b. Archivos críticos del sistema operativo modificados
  c. Cambios de políticas en Directorios Activos
  d. Eliminación de logs de auditoría
  e. Modificación de winlogon.exe
  f. Modificación de PAM, y otras medidas antiforense, cómo y sin limitarse a tácticas utilizadas por los ciberdelincuentes para evitar ser detectados o borrar evidencia de su presencia en la red de la entidad, incluyendo, pero sin limitarse al marco de referencia MITRE ATT&CK para Evasión de Defensa. Después de la investigación de la actividad sospechosa o incidentes de seguridad se entregará el informe final detallado del mismo.

Los servicios ofrecidos deberán poder ser visualizados a través de tableros de control que permitan ver métricas en línea de acuerdo a las necesidades de la Entidad, por ejemplo:

a. Alertas/Incidentes por tipo
b. Alertas/Incidentes nuevos y resuelto
c. Tiempo medio de creación de alertas/incidentes
d. Tiempo medio de solución
e. Tendencias y top de alertas/incidentes

Cumplimiento de acuerdos de servicio

INFORMES, MÉTRICAS Y TENDENCIAS SOC

La entrega de informes deberá efectuarse por medio de correo electrónico del equipo de Ciberseguridad, dentro de los cinco (5) primeros días hábiles del mes, salvo en las herramientas que se configure otra frecuencia: Diaria, Semanal, mensual o incluso trimestral. Los documentos entregables e informes que el contratista presente, deben exportarse de las herramientas de monitoreo, esta actividad debe evidenciarse en los logs y debe contar con un formato de presentación estándar, redacción clara, buena ortografía y en idioma español. Todos los informes que contengan información técnica de vulnerabilidades, configuraciones, detalles de incidentes y datos personales deben etiquetarse como confidenciales. Los informes de gestión deben ser sanitizados y no contener detalles técnicos o información de datos personales de personas no involucradas en la generación del reporte.

- El contratista debe informar a los equipos de Infraestructura y Soporte Tecnológico – EIST y de Seguridad de la Información de la Entidad de manera inmediata, sobre cualquier evento o incidente real que se presenten en la infraestructura tecnológica.
- La solución debe incluir la personalización de reportes que la Entidad requiera durante la vigencia pactada para el SOC por suscripción.
- El contratista deberá presentar mensualmente o cada que sea requerido, los siguientes informes de:
  1. Estado y resultados del servicio en el periodo de valoración, de tipo gerencial.
  2. Eventos de actividad sospechosa atendidos durante el periodo.
  3. Alertas, ataques, incidentes y tendencias.
  4. Comportamientos más relevantes según la correlación realizada por el contratista.
  5. Incidentes de seguridad presentados.
  6. Estadísticas de la información procesada
  7. Hallazgos realizados sobre la plataforma tecnológica
  8. Análisis y recomendaciones sobre los resultados
- La Entidad podrá solicitar los informes que considere pertinentes, en la medida en que se vayan integrando nuevas herramientas.
- El contratista deberá generar reportes de eventos y de análisis de tendencias, para tomar las acciones preventivas, tales como: instalación de parches, actualización de versiones, modificación de políticas y configuraciones. Además, debe quedar registros de cuándo, dónde y cómo se presentan los incidentes, así como definir nuevos reportes acorde a las necesidades de la Entidad.
- El contratista deberá entregar un informe preliminar de un incidente sucedido. Este debe ser remitido a la Entidad posterior a la declaración del evento o incidente y después de la investigación de la actividad sospechosa o incidentes de seguridad se entregará el informe final detallado del mismo.

- Los servicios ofrecidos deberán poder ser visualizados a través de tableros de control que permitan ver métricas en línea de acuerdo con las necesidades de la Entidad, por ejemplo:
    1. Alertas/Incidentes por tipo
    2. Alertas/Incidentes nuevos y resuelto
    3. Tiempo medio de creación de alertas/incidentes
    4. Tiempo medio de solución
    5. Tendencias y top de alertas/incidentes
    6. Cumplimiento de acuerdos de servicio
    7. Nivel de disponibilidad del servicio

ATENCIÓN DE INCIDENTES DE CIBERSEGURIDAD SOC

PRIORIDAD INCIDENTE DE CIBERSEGURIDAD	DESCRIPCIÓN
CRÍTICA	La producción está parada o severamente impactada de manera que no se puede continuar trabajando. La operación es de misión crítica para la entidad y/o está en situación de emergencia. Tiempo de respuesta: 3 minutos para identificación, 10 minutos para análisis y reporte, 1 hora para el envío de recomendaciones técnicas de contención. Soporte: De manera remota (1) hora de atención para soporte.
ALTA	Experimenta perdida del servicio, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida. Tiempo de respuesta: 5 minutos para identificación, 10 minutos para análisis y reporte, 1 hora para el envío de recomendaciones técnicas de contención. De manera remota (2) horas de atención para soporte.
MEDIA	Experimenta una pérdida de servicio menor, el impacto es un inconveniente. Tiempo de respuesta:

	10 minutos para identificación, 10 minutos para análisis y reporte, 1 hora para el envío de recomendaciones técnicas de contención. Soporte: De manera remota (8) horas de atención para soporte si es necesario.
BAJA	No impacta la operación del programa, no se experimenta perdida del servicio y no se impide la operación de los sistemas. Tiempo de respuesta: 15 minutos para identificación, 10 minutos para análisis y reporte, 1 hora para el envío de recomendaciones técnicas de contención. Soporte: De manera remota (24) horas de atención para soporte si es necesario.

SOPORTE ESPECIALIZADO SOC POR DEMANDA

Se prestará el servicio de soporte especializado, para dar acompañamiento al análisis de y causa raíz de incidentes de seguridad informática que surjan sobre la infraestructura, contribuyendo en la solución parcial y/o definitiva, con el objetivo de realizar la contención y recuperación de los servicios que han sido afectados.

Se contempla una bolsa de diez (10) horas de servicios profesionales, la cual se ejecutará por demanda, es decir en caso en que se requiera por la Entidad en el marco de la ejecución del servicio, por ningún motivo será un cobro mensual.

Los tiempos de atención remota o en sitio, según sea el caso, se realizará teniendo como base las siguientes prioridades:

- De impacto crítico: alertamiento dentro de los primeros 5 minutos y escalamiento en máximo 10 minutos.
- De impacto alto: alertamiento dentro de los primeros 15 minutos y escalamiento en máximo 20 minutos
- De impacto moderado: alertamiento dentro de las primeras 2 horas y escalamiento en máximo 2 horas
- De impacto bajo: alertamiento dentro de las primeras 12 horas y escalamiento en máximo 6 horas.

El servicio se prestará como parte de la bolsa de servicios especializados.

SERVICIOS ESPECIALIZADOS DE ANÁLISIS FORENSE EN CIBERSEGURIDAD SOC

Se prestará el servicio especializado de análisis forense en ciberseguridad para realizar la investigación de incidentes de seguridad informática, con el objetivo de identificar al o los responsables, comprender el ataque y dar las recomendaciones respecto al incidente de ciberseguridad.

El alcance del análisis forense en ciberseguridad podrá ser aplicado en casos como: Fraudes informáticos, Extorción, Robo de datos, Intrusión en redes informáticas.

Se contempla una bolsa de 100 horas de servicios profesionales, la cual se ejecutará por demanda, es decir en caso en que se requiera por la Entidad en el marco de la ejecución del servicio, por ningún motivo será un cobro mensual.

Al momento que ocurra el hecho y se requieran los servicios especializados, se realizará una evaluación preliminar y se presentará la oferta de servicios, con el alcance técnico y económico.

NOTIFICACIÓN DE EVENTOS DE INTERRUPCIÓN DEL MONITOREO - SOC.

PRIORIDAD Interrupción del monitoreo	**DESCRIPCIÓN**
CRÍTICA	Se detiene totalmente el monitoreo o su capacidad está severamente impactada de manera que no se puede continuar trabajando. Tiempo de respuesta: Identificación: 3 minutos contado a partir de su ocurrencia o del reporte efectuado por la Entidad. Análisis: 10 minutos contados a partir de la finalización del tiempo de Identificación.
ALTA	El 80% de las aplicaciones de seguridad y sistemas monitoreados experimenta perdida del servicio de monitoreo, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida. Tiempo de respuesta: Identificación: 5 minutos contados a partir de su ocurrencia o del reporte efectuado por la Entidad. Análisis: 10 minutos contados a partir de la finalización del tiempo de Identificación.
MEDIA	El 50% de las aplicaciones de seguridad y sistemas monitoreados experimenta perdida del servicio de monitoreo, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera intermitente. Tiempo de respuesta: Identificación: 10 minutos contado a partir de su ocurrencia o del reporte efectuado por la Entidad. Análisis: 10 minutos contados a partir de la finalización del tiempo de Identificación.
BAJA	El 20% de las aplicaciones de seguridad y sistemas monitoreados experimenta perdida del servicio de

	monitoreo, algunas características importantes no pueden ser utilizadas, no impacta la operación del programa, no se experimenta perdida del servicio y no se impide la operación de los sistemas. <u>Tiempo de respuesta:</u> Identificación: 15 minuto contado a partir de su ocurrencia o del reporte efectuado por la Entidad. Análisis: 10 minutos contados a partir de la finalización del tiempo de Identificación.	

TIEMPOS DE ALERTAMIENTO Y ESCALAMIENTO AL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA ENTIDAD - SOC

• De impacto crítico: alertamiento dentro de los primeros 5 minutos y escalamiento en máximo 10 minutos.
• De impacto alto: alertamiento dentro de los primeros 15 minutos y escalamiento en máximo 20 minutos
• De impacto moderado: alertamiento dentro de las primeras 2 horas y escalamiento en máximo 2 horas
• De impacto bajo: alertamiento dentro de las primeras 12 horas y escalamiento en máximo 6 horas.

1.13.3. Línea de conectividad de redes.

La Agencia Nacional de Tierras - ANT requiere contar con servicios integrales de conectividad que garanticen la comunicación, interoperabilidad, disponibilidad y continuidad de los servicios tecnológicos y administrativos a nivel nacional, a continuación, se relacionan los servicios y características:

Ítem	Servicio	UGT/SEDE	CIUDAD	Capacidad (Mbps)	Disponibilidad Mensual	IP's Publicas	Observaciones
1	INTERNET CORPORATIVO	ANTIOQUIA	APARTADO_ISP1	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
2	INTERNET CORPORATIVO	ANTIOQUIA	APARTADO_ISP2	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de

							Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
3	INTERNET CORPORATIVO	ARAUCA	ARAUCA_ISP1	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
4	INTERNET CORPORATIVO	ARAUCA	ARAUCA_ISP2	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
5	INTERNET CORPORATIVO	QUINDÍO	ARMENIA_ISP 1	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
6	INTERNET CORPORATIVO	QUINDÍO	ARMENIA_ISP 2	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace

							cuente con su propio bloque de direccionamiento.
7	INTERNET CORPORATIVO	ATLANTICO	BARRANQUILLA_ISP1	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
8	INTERNET CORPORATIVO	ATLANTICO	BARRANQUILLA_ISP2	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
9	INTERNET CORPORATIVO	VALLE DEL CAUCA	CALI_ISP1	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
10	INTERNET CORPORATIVO	VALLE DEL CAUCA	CALI_ISP2	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace

							cuente con su propio bloque de direccionamiento.
11	INTERNET CORPORATIVO	BOLÍVAR	CARTAGENA_ISP1	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
12	INTERNET CORPORATIVO	BOLÍVAR	CARTAGENA_ISP2	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
13	INTERNET CORPORATIVO	CAQUETÁ	FLORENCIA_ISP1	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
14	INTERNET CORPORATIVO	CAQUETÁ	FLORENCIA_ISP2	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.

15	INTERNET CORPORATIVO	CALDAS	MANIZALES_ISP1	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
16	INTERNET CORPORATIVO	CALDAS	MANIZALES_ISP2	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
17	INTERNET CORPORATIVO	PUTUMAYO	MOCOA_ISP1	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
18	INTERNET CORPORATIVO	PUTUMAYO	MOCOA_ISP2	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.

19	INTERNET CORPORATIVO	HUILA	NEIVA_ISP1	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
20	INTERNET CORPORATIVO	HUILA	NEIVA_ISP2	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
21	INTERNET CORPORATIVO	NARIÑO	PASTO_ISP1	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
22	INTERNET CORPORATIVO	NARIÑO	PASTO_ISP2	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.

23	INTERNET CORPORATIVO	RISARALDA	PEREIRA_ISP 1	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
24	INTERNET CORPORATIVO	RISARALDA	PEREIRA_ISP 2	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
25	INTERNET CORPORATIVO	CHOCO	QUIBDO_ISP1	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
26	INTERNET CORPORATIVO	CHOCO	QUIBDO_ISP2	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.

27	INTERNET CORPORATIVO	GUAJIRA	RIOHACHA_ISP1	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
28	INTERNET CORPORATIVO	GUAJIRA	RIOHACHA_ISP2	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
29	INTERNET CORPORATIVO	GUAVIARE	SAN JOSE DEL GUAVIARE_ISP1	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
30	INTERNET CORPORATIVO	GUAVIARE	SAN JOSE DEL GUAVIARE_ISP2	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.

31	INTERNET CORPORATIVO	MAGDALENA	SANTA MARTA_ISP1	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
32	INTERNET CORPORATIVO	MAGDALENA	SANTA MARTA_ISP2	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
33	INTERNET CORPORATIVO	CESAR	VALLEDUPAR_ISP1	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
34	INTERNET CORPORATIVO	CESAR	VALLEDUPAR_ISP2	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.

35	INTERNET CORPORATIVO	CASANARE	YOPAL_ISP1	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
36	INTERNET CORPORATIVO	CASANARE	YOPAL_ISP2	30	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
37	INTERNET CORPORATIVO	SUCRE	SINCELEJO_ISP2	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
38	INTERNET CORPORATIVO	SUCRE	SINCELEJO_ISP2	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.

39	INTERNET CORPORATIVO	TOLIMA	IBAGUE_ISP2	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
40	INTERNET CORPORATIVO	TOLIMA	IBAGUE_ISP2	40	99,5%	/30	En caso de no poder garantizar dos (2) ISP diferentes, el canal de internet a proveer debe ser la suma de los dos canales solicitados. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
41	INTERNET CORPORATIVO	SANTANDER	BARRANCABERMEJA	20	99,5%	/30	Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
42	MPLS L3 (Capa 3)	SANTANDER	BUCARAMANGA	40	99,5%	No aplica	Un (1) enlace de conectividad a través de red MPLS L3 (Capa 3), provisto por un único operador, en esquema activo, que garantice la interconexión segura y permanente con la red corporativa, así como la continuidad del servicio conforme al porcentaje de disponibilidad establecido.
43	INTERNET CORPORATIVO	SANTANDER	BUCARAMANGA	40	99,5%	/30	Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
44	MPLS L3 (Capa 3)	NORTE DE	CUCUTA	40	99,5%	No aplica	Un (1) enlace de conectividad a través de red MPLS L3 (Capa 3), provisto por un único operador, en esquema activo, que garantice la

		SANTANDER					interconexión segura y permanente con la red corporativa, así como la continuidad del servicio conforme al porcentaje de disponibilidad establecido.
45	INTERNET CORPORATIVO	NORTE DE SANTANDER	CUCUTA	40	99,5%	/30	Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
46	MPLS L3 (Capa 3)	ANTIOQUIA	MEDELLIN	40	99,5%	No aplica	Un (1) enlace de conectividad a través de red MPLS L3 (Capa 3), provisto por un único operador, en esquema activo, que garantice la interconexión segura y permanente con la red corporativa, así como la continuidad del servicio conforme al porcentaje de disponibilidad establecido.
47	INTERNET CORPORATIVO	ANTIOQUIA	MEDELLIN	40	99,5%	/30	Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
48	MPLS L3 (Capa 3)	CÓRDOBA	MONTERIA	40	99,5%	No aplica	Un (1) enlace de conectividad a través de red MPLS L3 (Capa 3), provisto por un único operador, en esquema activo, que garantice la interconexión segura y permanente con la red corporativa, así como la continuidad del servicio conforme al porcentaje de disponibilidad establecido.
49	INTERNET CORPORATIVO	CÓRDOBA	MONTERIA	40	99,5%	/30	Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
50	MPLS L3 (Capa 3)	CAUCA	POPAYAN	40	99,5%	No aplica	Un (1) enlace de conectividad a través de red MPLS L3 (Capa 3), provisto por un único operador, en esquema activo, que garantice la interconexión segura y permanente con la red corporativa, así como la continuidad del servicio conforme

							al porcentaje de disponibilidad establecido.
51	INTERNET CORPORATIVO	CAUCA	POPAYAN	40	99,5%	/30	Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
52	MPLS L3 (Capa 3)	BOYACÁ	TUNJA	40	99,5%	/30	Un (1) enlace de conectividad a través de red MPLS L3 (Capa 3), provisto por un único operador, en esquema activo, que garantice la interconexión segura y permanente con la red corporativa, así como la continuidad del servicio conforme al porcentaje de disponibilidad establecido.
53	INTERNET CORPORATIVO	BOYACÁ	TUNJA	40	99,5%	/30	Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
54	MPLS L3 (Capa 3)	META	VILLAVICENCIO	40	99,5%	/30	Un (1) enlace de conectividad a través de red MPLS L3 (Capa 3), provisto por un único operador, en esquema activo, que garantice la interconexión segura y permanente con la red corporativa, así como la continuidad del servicio conforme al porcentaje de disponibilidad establecido.
55	INTERNET CORPORATIVO	META	VILLAVICENCIO	40	99,5%	/30	Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
56	MPLS L3 (Capa 3)	BOGOTÁ D.C.	SEDE AMERICAS	40	99,5%	No aplica	Un (1) enlace de conectividad a través de red MPLS L3 (Capa 3), provisto por un único operador, en esquema activo, que garantice la interconexión segura y permanente con la red corporativa, así como la continuidad del servicio conforme al porcentaje de disponibilidad establecido.

57	INTERNET CORPORATIVO	BOGOTÁ D.C.	SEDE AMERICAS	40	99,5%	/30	Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
58	MPLS L3 (Capa 3)	BOGOTÁ D.C.	SEDE CHAPINERO	200	99,5%	No aplica	Un (1) enlace de conectividad a través de red MPLS L3 (Capa 3), provisto por un único operador, en esquema activo, que garantice la interconexión segura y permanente con la red corporativa, así como la continuidad del servicio conforme al porcentaje de disponibilidad establecido.
59	INTERNET CORPORATIVO	BOGOTÁ D.C.	SEDE CHAPINERO_ISP1	500	99,5%	/29	SEDE CHAPINERO_ISP1: Un (1) enlace de Internet dedicado, provisto por un único operador (ISP), que garantice acceso permanente a Internet, con disponibilidad mínima del 99,5% mensual (SLA), asegurando la continuidad del servicio. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
60	INTERNET CORPORATIVO	BOGOTÁ D.C.	SEDE CHAPINERO_ISP2	500	99,5%	/29	ISP diferente al ítem 59 - SEDE CHAPINERO_ISP1 SEDE CHAPINERO_ISP2: Un (1) enlace de Internet dedicado, provisto por un único operador (ISP), que garantice acceso permanente a Internet, con disponibilidad mínima del 99,5% mensual (SLA), asegurando la continuidad del servicio. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.

61	MPLS L3 (Capa 3)	BOGOTÁ D.C.	CENTRO - ED. SAN JUAN DE DIOS	150	99,5%	No aplica	Un (1) enlace de conectividad a través de red MPLS L3 (Capa 3), provisto por un único operador, en esquema activo, que garantice la interconexión segura y permanente con la red corporativa, así como la continuidad del servicio conforme al porcentaje de disponibilidad establecido.
62	INTERNET CORPORATIVO	BOGOTÁ D.C.	CENTRO - ED. SAN JUAN DE DIOS_ISP1	150	99,5%	/29	CENTRO - ED. SAN JUAN DE DIOS_ISP1: Un (1) enlace de Internet dedicado, provisto por un único operador (ISP), que garantice acceso permanente a Internet, con disponibilidad mínima del 99,5% mensual (SLA), asegurando la continuidad del servicio. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
63	INTERNET CORPORATIVO	BOGOTÁ D.C.	CENTRO - ED. SAN JUAN DE DIOS_ISP2	150	99,5%	/29	ISP diferente al ítem 62 - CENTRO - ED. SAN JUAN DE DIOS_ISP1 CENTRO - ED. SAN JUAN DE DIOS_ISP2: Un (1) enlace de Internet dedicado, provisto por un único operador (ISP), que garantice acceso permanente a Internet, con disponibilidad mínima del 99,5% mensual (SLA), asegurando la continuidad del servicio. Las direcciones IP públicas y sus respectivas máscaras deberán ser asignadas de manera independiente para cada canal de Internet suministrado, garantizando que cada enlace cuente con su propio bloque de direccionamiento.
64	MPLS L3 (Capa 3)	TOCANCIPÁ CUNDINAMARCA	COLOCATION_to_UGT / SEDE	700	99.95%	No aplica	Un (1) servicio de conectividad mediante red MPLS L3 (Capa 3), implementado a través de dos (2) enlaces, cada uno con capacidad de 800 Mbps, provistos sobre infraestructura física independiente y con equipos de acceso (CPE) separados, en esquema de redundancia activo–

							pasivo, que garantice la interconexión segura y permanente con la red corporativa. El servicio deberá asegurar una disponibilidad mínima del 99,95% mensual (SLA), garantizando que, ante la falla de uno de los enlaces, el enlace restante soporte el 100% de la capacidad contratada sin degradación del servicio y sin puntos únicos de falla en la última milla. Los equipos de enrutamiento (routers) a suministrar deberán contar con fuentes de poder redundantes (dual PSU), garantizando la continuidad de operación ante la falla de una de ellas. Este servicio corresponde al punto central de concentración de las conexiones MPLS provenientes de las diferentes sedes de la entidad (MEDELLIN, TUNJA, POPAYAN, MONTERIA, VILLAVICENCIO, CUCUTA, BUCARAMANGA, SINCELEJO, IBAGUE, SEDE AMERICAS, SEDE CHAPINERO_ISP1, CENTRO - ED. SAN JUAN DE DIOS).
65	SERVICIO DE CONECTIVIDAD SATELITAL DE ÓRBITA BAJA (LEO) PARA UBICACIÓN FIJA	VICHADA	PUERTO CARREÑO	Plan 1TB	99,9%	No aplica	No aplican direcciones IP públicas para este servicio.
66	SERVICIO DE CONECTIVIDAD SATELITAL DE ÓRBITA BAJA (LEO)	GUAINÍA	INIRIDA	Plan 1TB	99,9%	No aplica	No aplican direcciones IP públicas para este servicio.

	PARA UBICACIÓN FIJA						
67	INTERNET CORPORATIVO	BOGOTÁ D.C.	SEDE CAN_ISP1	1024	99,5%	/28	SEDE CAN_ISP1: Un (1) enlace de Internet dedicado, provisto por un único operador (ISP), que garantice acceso permanente a Internet, con disponibilidad mínima del 99,5% mensual (SLA), asegurando la continuidad del servicio. El direccionamiento IP público suministrado deberá encontrarse libre de registros en listas negras (blacklists) o en cualquier otra base de datos que pueda afectar la reputación, disponibilidad o correcta navegación de los servicios.
68	INTERNET CORPORATIVO	BOGOTÁ D.C.	SEDE CAN_ISP2	1024	99,5%	/28	ISP diferente al ítem 67 - SEDE CAN_ISP1 SEDE CAN_ISP2: Un (1) enlace de Internet dedicado, provisto por un único operador (ISP), que garantice acceso permanente a Internet, con disponibilidad mínima del 99,5% mensual (SLA), asegurando la continuidad del servicio. El direccionamiento IP público suministrado deberá encontrarse libre de registros en listas negras (blacklists) o en cualquier otra base de datos que pueda afectar la reputación, disponibilidad o correcta navegación de los servicios.
69	INTERNET CORPORATIVO	COLOCATION	COLOCATION_ISP1	1024	99.95%	/25	Un (1) servicio de conectividad a Internet dedicado con capacidad de 1024 Mbps (1 Gbps), implementado mediante dos (2) enlaces provistos por diferentes operadores (ISP), sobre infraestructura física independiente y en esquema de redundancia activo–pasivo, con equipos de acceso (CPE) independientes por cada enlace, que garantice acceso permanente a Internet. El servicio deberá asegurar una disponibilidad mínima del 99,95% mensual (SLA), garantizando que, ante la falla del enlace principal, el enlace

							secundario soporte el 100% de la capacidad contratada sin degradación del servicio y sin puntos únicos de falla en la última milla. El direccionamiento IP público suministrado deberá encontrarse libre de registros en listas negras (blacklists) o en cualquier otra base de datos que pueda afectar la reputación, disponibilidad o correcta navegación de los servicios. Los equipos de enrutamiento (routers) a suministrar deberán contar con fuentes de poder redundantes (dual PSU), garantizando la continuidad de operación ante la falla de una de ellas. Las direcciones IP públicas pueden entregarse en uno o dos bloques (subredes), siempre que sumen el total requerido.
70	INTERNET CORPORATIVO	COLOCATION	COLOCATION_ISP2	1024	99,9%	/27	ISP diferente al ítem 69 - COLOCATION_ISP1 Un (1) enlace de Internet dedicado con capacidad de 1024 Mbps (1 Gbps), provisto por un único operador (ISP), que garantice acceso permanente a Internet, con disponibilidad mínima del 99,9% mensual (SLA), asegurando la continuidad del servicio. El direccionamiento IP público suministrado deberá encontrarse libre de registros en listas negras (blacklists) o en cualquier otra base de datos que pueda afectar la reputación, disponibilidad o correcta navegación de los servicios. Los equipos de enrutamiento (routers) a suministrar deberán contar con fuentes de poder redundantes (dual PSU), garantizando la continuidad de operación ante la falla de una de ellas.

71	MPLS L2 (Capa 2)	BOGOTÁ D.C.	CAN_to_COLOCATION_ISP1	2048	99,9%	No aplica	ISP1: Canal capa 2 conectividad entre el CAN y el Colocation. El servicio deberá soportar mínimo 2000 direcciones MAC, sin degradación del servicio.
72	MPLS L2 (Capa 2)	BOGOTÁ D.C.	CAN_to_COLOCATION_ISP2	1024	99,9%	No aplica	ISP diferente al ítem 71 - CAN_to_COLOCATION_ISP1 ISP2: Canal capa 2 conectividad entre el CAN y el Colocation. El servicio deberá soportar mínimo 2000 direcciones MAC, sin degradación del servicio. Nota: Se aclara que la capacidad del canal de los dos servicios MPLS L2 es diferente.
73	CONECTIVIDAD MÓVIL 3G – 4G – 5G	Cantidad: Cinco (5) Enlaces de Conectividad Móvil - Internet Móvil de 100 GB que se puedan compartir con otros usuarios de forma inalámbrica - Con Terminal Modem Mifi - cobertura a nivel Nacional.					
74	ENLACES SATELITALES DE ORBITA BAJA PORTÁTILES:	Cantidad: Cuatro (4) Prestación del servicio de conectividad satelital mediante tecnología de órbita baja (LEO) para operación en campo y movilidad terrestre, con capacidad mínima de 500 GB mensuales para uso en territorio nacional y posibilidad de operación en desplazamientos regionales. El servicio estará orientado a soportar actividades de topografía y trabajo técnico en zonas rurales o de difícil acceso. El servicio deberá incluir el suministro de un kit de usuario en modalidad portátil y como mínimo los siguientes elementos por cada unidad suministrada: • Antena satelital. • Base o soporte de instalación. • Equipo de enrutamiento (router). • Cable de conexión entre antena y router con longitud mínima de 15 metros. • Cable de alimentación eléctrica con longitud mínima de 1.8 metros. • Estuche o maletín de transporte, resistente y adecuado para la protección y movilización del equipo en campo. • Los equipos deberán entregarse en condiciones operativas y funcionales para su utilización en ambientes de trabajo móvil y operación en campo. El contratista deberá mantener vigente durante la ejecución contractual una póliza Todo Riesgo Equipos Electrónicos Portátiles que ampare los equipos tecnológicos suministrados para la prestación del servicio, incluyendo cobertura por hurto calificado, daño accidental, transporte, eventos eléctricos, humedad, eventos naturales y operación fuera de predios, así como póliza de Responsabilidad Civil Extracontractual por daños ocasionados a terceros. Los equipos deberán permanecer asegurados tanto durante su operación como en su transporte y almacenamiento temporal en zonas rurales o de difícil acceso.					

Legislación aplicable al objeto del proceso

Elaborado por: Paula Morales Contratista SSIT

Aprobado por: Diana Lucia Herrera Riaño – Subdirectora SSIT