



JUSTIFICACIÓN PARA URGENCIA INMINENTE

Proceso solicitante:	DIRECCIÓN NACIONAL DE INFORMÁTICA Y TECNOLOGÍA
Vigencia:	2023
Fecha:	20/09/2023

A continuación, a Vicepresidencia de Soporte Corporativo y la Dirección Nacional de informática y tecnología justifica la contratación a través de Urgencia Inminente, requerida para contratar Prestación de un servicio global de Data Center, hosting, nube, telecomunicaciones, conectividad, seguridad y demás servicios TI; a través de un aliado estratégico que brinde a la entidad un servicio integral y de alta disponibilidad de manera centralizada que permita la operación a nivel nacional de las diferentes sedes y aplicaciones que maneja la entidad” A continuación, la dirección nacional de informática y tecnología justifica la contratación a través de Urgencia Inminente.

1. JUSTIFICACIÓN Y DESCRIPCIÓN DE LA NECESIDAD

SERVICIOS POSTALES NACIONALES S.A.S., es una sociedad pública con el carácter de sociedad por acciones simplificada, vinculada al Ministerio de Tecnologías de la Información y las Comunicaciones, cuyo objeto social se desarrolla en un entorno de alta competencia empresarial, por lo que los procesos contractuales de la misma deben estar regulados de una manera clara y precisa respetando mandatos legales y Constitucionales propios de la Función Administrativa, permitiéndole a la vez competir en igualdad de condiciones en el mercado, para lo cual SPN tiene autonomía administrativa, patrimonial y presupuestal y ejerce sus actividades dentro del ámbito del Derecho Privado, como empresario mercantil, dando aplicación a las normas propias de las sociedades previstas en el Código de Comercio y su legislación complementaria.

Que el artículo 209 de la Constitución Política ordena que la función administrativa debe estar al servicio de los intereses generales y que se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, delegación y desconcentración de funciones.

Los Servicios Postales están bajo la titularidad del Estado, el cual, para su prestación, podrá habilitar a empresas públicas y privadas en los términos de esta ley lo que SERVICIOS POSTALES NACIONALES S.A.S. en su calidad de Operador oficial deberá, propender modelos de negocios que permitan establecer en el territorio nacional, esta actividad garantizar el cumplimiento del objeto social principal.


Que el marco jurídico antes referido le permite a SPN operar en la economía como un agente de mercado que contribuye con los fines esenciales del Estado contemplados en el artículo 2 de la Carta Política, y que cuenta la discrecionalidad derivado del derecho privado, lo cual le otorga la potestad de establecer los procesos y lineamientos generales que le permitan adelantar la selección y contratación de personas naturales y jurídicas nacionales y extranjeras para el cumplimiento de proyectos ordinarios y especiales así como el de colaboración con aliados bajo las diferentes clases de figuras y/o contratos.

En vista de lo anterior, la Dirección Nacional de Informática y Tecnología (IT), es la encargada de controlar los recursos, proveer las herramientas de trabajo para el desarrollo de la actividad misional y poner a disposición las plataformas tecnológicas de SPN, que soportan e inciden notablemente en las actividades operativas del giro ordinario de la empresa así como el ámbito comercial y administrativas, Por lo tanto y en razón a que es vital la prestación del servicio de Datacenter, Conectividad y Seguridad; para el alojamiento de las aplicaciones críticas del negocio, y asegurar la interconexión de las sedes principales de la entidad y brindar capas de seguridad a los datos, información, usuarios, plataformas, etc. de la plataforma tecnológica y de la información crítica de Servicios Postales Nacionales S.A. En este contexto este servicio no puede ni debe paralizarse y por el contrario al ser una herramienta permanente que actualmente cuenta con servicios de misión crítica, tal es el caso de los siguientes sistemas prioritarios a saber: **SIPOST, PORTAL WEB, SEVEN, KACTUS, DOMINIO, BIOMETRIA, IFS, IPS, SHERLOCK, PQR, SARL, COLPENSIONES, MULTIPAY**; la solución actualmente cuenta con un servicio integral a través de un Datacenter de alta disponibilidad que comprende servicios administrados, seguridad y un ecosistema de DRP, es necesario continuar en las condiciones técnicas con el servicio de conectividad y seguridad de dichos elementos.


En este momento se viene ejecutando el contrato número 130- 2020 cuyo objeto es Prestación de servicio de conectividad como solución integral de alta disponibilidad y el alojamiento en modalidad de nube privada, hosting físico y/o hosting virtual centralizado en un centro de datos que permita la operación a nivel nacional de las aplicaciones que maneja la entidad, este contrato finaliza el día treinta (30) de septiembre de 2023, sin posibilidad de adicionar y prorrogar para continuar prestando los componentes (Conectividad, DC Principal, DC Alterno, Servicios Administrados y Seguridad en Datacenter), la cual es del 99,93%. Pertinente sea indicar que SPN debe garantizar los servicios de Conectividad y Seguridad; para el alojamiento de las aplicaciones, necesarias para el funcionamiento operativo y administrativo y asegurar la interconexión de las sedes principales de la entidad y brindar capas de seguridad a los datos, información, usuarios, plataformas, y de la información necesaria de Servicios Postales Nacionales S.A.S

Ahora bien, es menester señalar que debido a que se han suscitado y sobrevenido diferentes situaciones que en el momento no fue posible evitar su acaecimiento ni superar sus consecuencias por parte de la S.P.N S.A.S debido a que en su mayoría obedecen a la participación de terceros y la voluntad, y hechos exógenos de fuerza mayor, que salen del resorte usual de la administración y que han impedido llevar a cabo el desarrollo normal de la contratación en las condiciones previstas de contratación inicial dada su cuantía y complejidad. Bajo este contexto se procede a indicar los hechos acaecidos y las situaciones fácticas que sustentan la necesidad de continuar el proceso para garantizar el trabajo de la empresa así mismo se puede evidenciar que no se rompió por voluntad, las condiciones para iniciar a tiempo el proceso planeado así;

Situaciones Fácticas, Jurídicas y Administrativas

-  Que por la situación precitada y teniendo en cuenta que el plazo de ejecución del contrato que se encuentra en ejecución, siendo el 30 de septiembre de 2023 la fecha que culmina sin posibilidad de adicionar o prorrogar para seguir prestando los servicio de Hosting y Conectividad con el fin de lograr administrar y controlar los servicios tecnológicos que soportan la operación como el único Operador Postal Nacional en todo el territorio nacional, y que por

esta razón SPN debe propender por buscar las soluciones más adecuadas y que cumplan con las condiciones técnicas y jurídicas para lograr superar los impedimentos y dificultades que se presenten y que conlleven a satisfacer la necesidad y por ello para garantizar el canal de conectividad a todos los funcionarios de SPN S.A.S y las aplicaciones .

 Que, en concordancia con lo anterior para llevar a cabo el proceso de selección del nuevo contratista, sin solución de continuidad de todos los servicios de hosting y conectividad a nivel nacional no es posible realizar toda esa migración de los servicios de conectividad, data center y/o otros en un mínimo tiempo, dado que debe darse cumplimiento a un cronograma dependiendo de la modalidad de selección que quizás supere más de un mes para su adjudicación. Sumado a lo anterior luego de adjudicado debe surtir la etapa de empalme la cual se requiere un tiempo aproximado de (3) tres meses para iniciar la ejecución de un contrato con las especificaciones técnicas requeridas situación que no es viable, debido a las compras de equipos, implementaciones tecnológicas, obras civiles y migraciones necesarias para la puesta en operación de los servicios; dentro de la ejecución del contrato se definen tres etapas: transición, operación y empalme.

- Respecto al proceso de Transición: Es el periodo de aprovisionamiento, implementación, migración y puesta en marcha de los diferentes servicios.
- Respecto a la Operación: Consiste en la operación de los servicios objeto del proceso correspondiente a soporte, administración, mantenimiento.
- Respecto al Empalme: Periodo en el que se realizaría el empalme con el nuevo proveedor y cierre de operaciones, así como la entrega de documentación correspondiente a ingeniería de detalle, backups, lecciones aprendidas, diagramas de red e infraestructura, planes de continuidad de negocio.
- Originalmente las etapas de Transición y de Empalme se tienen definidas de tres meses cada una y aun así en las mesas de trabajo los proveedores han manifestado que 90 días es un tiempo muy corto para la fase de transición por la complejidad y cantidad de recursos tecnológicos que deben ser adquiridos, implementados y migrados para la puesta en marcha de los servicios. Teniendo en cuenta lo anterior, diferentes proveedores nos han manifestado que un contrato para la prestación de los servicios de Hosting y Conectividad de tan solo tres meses no es viable técnicamente.
- Modelo económico: En los estudios de mercado realizados, los proveedores de tecnología nos manifestaron que el modelo económico para los servicios de hosting y conectividad objeto del cto 130-2020 no retornarían la inversión realizada o en todo caso el costo transferido a la entidad debería ser muy alto, por lo que se recomienda que el tiempo de ejecución de este tipo de contratos sea de 24 meses en adelante.

- ✚ Sumado a lo anterior, por la cuantía y necesidad de mantener en el tiempo este servicio, se requiere contar con la autorización y aprobación de vigencias futuras, las cuales son propias de La Junta. Directiva de SPN, que así mismo se vieron afectadas por situaciones administrativas tales como la Dificultad en convocar en varias oportunidades a la Junta Directiva por cambio de Administración en los Ministerios que la componen, cambio de presidencia de SPN, Actualmente no contamos con vigencias futuras para la siguiente vigencia 2024.
- ✚ De acuerdo con lo anterior, estos servicios tecnológicos no podrán verse afectado ni paralizados, así mismo, no se puede prescindir del suministro de conectividad, de lo contrario estaríamos en un alto riesgo en la prestación de los servicios postales y todo el área administrativa, sin dar cumplimiento a la misionalidad de la SPN, así como nuestra obligación comercial frente a los contratos suscritos con nuestros clientes corporativos, y en consecuencia el no ser prestados nos generaría una seria de incumplimiento con los contratos y la funcionalidad propia de la SPN teniendo en cuenta que las principales aplicaciones de la entidad se encuentran alojadas en el Datacenter de Claro como son Sipost, Seven Kactus, PQR, Portal Web, Multipay, IFS, Colpensiones y CODE; así como la conectividad de las diferentes sedes regionales. El impacto ante la detención o indisponibilidad de cualquiera de los servicios descritos sería muy alto para 4-72.
- ✚ En razón a lo anterior, se hace necesario recurrir a la modalidad de selección más expedita que pueda garantizar el servicio de la manera más ágil para superar la necesidad inminente que se está presentando y que no se paralicen los servicios para dar cumplimiento a las obligaciones empresariales, y entre ellos luego de ser analizadas las más apta a la necesidad es la modalidad de una Urgencia Inminente, con el objetivo de no, afectar la prestación del servicio a nuestros clientes y evitar un daño reputacional para la compañía, toda vez que al no tener servicios de hosting y conectividad a nivel nacional no se podrían cumplir las obligaciones que tiene Servicios Postales Nacionales S.A.S, en calidad de operador postal oficial y como contratista de clientes públicos y privados, máximo cuando esta actividad hace parte del Core del negocio y el derecho de los usuarios de los servicios postales.
- ✚ Por lo anterior, se acudió al comité de contratación y compras de SPN para realizar la justificación de acudir a esta causal de contratación directa y solicitar la recomendación para dar inicio al proceso a través de urgencia inminente, por las razones ya expuestas, la cual fue aprobada en Comité del día 22 de septiembre por todos los miembros del Comité.
- ✚ De igual manera es preciso señalar que conforme a lo establecido por el artículo 1 de la Ley 1369 de 2020 (*Por medio de la cual se establece el régimen de los servicios postales y se dictan otras disposiciones*), los servicios postales en Colombia están catalogados de **naturaleza pública** en los términos del artículo 365 de la Constitución Política.
- ✚ Dicha prestación de servicios consiste en el desarrollo de las actividades de recepción, clasificación, transporte y entrega de objetos postales a través de redes postales, dentro del

país o para envío hacia otros países o recepción desde el exterior (servicios de correo, los servicios postales de pago y los servicios de mensajería expresa); conforme al numeral 2 de la citada Ley, son prestados en calidad de **operador postal oficial** por SERVICIOS POSTALES NACIONALES S.A.S en calidad de concesionario.

- ✚ Corolario a lo anterior, no cabe duda de que en la actualidad el servicio postal es un **servicio público de carácter esencial**. Es por ello, que es imperativo traer a colación para la presente justificación, lo señalado por la honorable Corte Constitucional, mediante la sentencia C- 450 de 1995, en los siguientes términos:

“El carácter esencial de un servicio público se predica cuando las actividades que lo conforman contribuyen de modo directo y concreto a la protección de bienes o a la satisfacción de intereses o a la realización de valores, ligados con el respeto, vigencia, ejercicio y efectividad de los derechos y libertades fundamentales, ello es así, en razón de la preeminencia que se reconoce a los derechos fundamentales de la persona y de las garantías dispuestas para su amparo, con el fin de asegurar su respeto y efectividad”.

- ✚ Con todo lo anterior, es preciso señalar que, de acuerdo con el Manual de Contratación adoptado mediante el Acuerdo 05 de 2020, se cumplen los preceptos para recurrir a la contratación directa a través de la urgencia inminente, en los siguientes numerales:

1. Cuando exista una **necesidad inminente certificada por el jefe de área** requirente del servicio y el ordenador del gasto respectivo y siempre que la misma no se deba a falta de planeación de la adquisición del bien o servicio.
2. **Exista riesgo de afectar la continua y eficiente** prestación de los servicios a cargo de la empresa.
3. **Exista riesgo de afectar los compromisos u obligaciones existentes.**

- ✚ Conforme a la relación fáctica arriba expuesta se evidencian todas las actividades adelantadas por SPN para no afectar la prestación del servicio de Data Center, hosting, nube, telecomunicaciones, conectividad, seguridad y demás servicios TI.

En virtud del principio de planeación y en aras de no afectar de manera grave el cumplimiento de las obligaciones de **SERVICIOS POSTALES NACIONALES S.A.S.**, en calidad de operador postal oficial y con clientes tanto públicos como privados, a fin de proveer un servicio integral dentro del portafolio de servicios y cumplir la misionalidad de la entidad el Director Nacional de informática y tecnología solicita la **NECESIDAD INMINENTE** de contratar este servicio y así no afectar la continuidad, eficiencia y eficacia de la prestación de los servicios a cargo de la entidad, tanto para atender necesidades internas y comerciales de la compañía.

La presente justificación se encuentra en el Plan Anual de Adquisiciones Vigencia 2023

Línea	Descripción	Fecha estimada de inicio de proceso de selección	Duración del contrato	Valor total estimado
117	HOSTING Y CONECTIVIDAD	Septiembre	3 meses	\$ 1.036.902.717

2. ESPECIFICACIONES TECNICAS

Para que la SPN S.A.S satisfaga la necesidad apremiante y dada la diversificación de los modelos de negocio y el crecimiento empresarial que está teniendo Servicios Postales Nacionales S.A., se requiere contar con un servicio global de Data Center, hosting, nube, telecomunicaciones, conectividad, seguridad y demás servicios TI; a través de un aliado estratégico que brinde a la entidad un servicio integral y de alta disponibilidad.

El proveedor seleccionado deberá contar con la seriedad, la solvencia y el compromiso para suplir de manera eficiente y eficaz, los requerimientos y los mantenimientos que sean necesarios para SPN y miembros corporativos.

En disposición de la utilización de los recursos tecnológicos bajo el control de la Dirección Nacional de IT requeridos tienen un alcancen así:

I. DATACENTER

SPN S.A.S requiere de una solución de infraestructura tecnológica que garantice la prestación de los servicios de Datacenter para el alojamiento de las aplicaciones de apoyo del negocio, así como los servicios de almacenamiento, licenciamiento, administración de los sistemas operativos y motores de bases de datos, copias de respaldo (Backups) y seguridad de la plataforma tecnológica y de la información crítica de Servicios Postales Nacionales S.A.

Dentro de las especificaciones deben estar incluidos el hardware, software y sistemas de comunicaciones requeridos por SPN S.A.S, con toda la seguridad y respaldo necesario a sus actividades e información generada por sus labores diarias, para lo cual es necesario

ALOJAMIENTO DE LAS APLICACIONES:

SPN S.A.S requiere alojamiento en modalidad de nube privada, hosting físico y/o hosting virtual, centralizado en un datacenter que permita la operación a nivel nacional de:

Windows

1. Sipost
 - a. Producción
 - b. Certificación

- c. Contingencia
- 2. Seven**
 - a. Producción
 - b. Pruebas
 - c. Contingencia
- 3. Kactus**
 - a. Producción
 - b. Pruebas
 - c. Contingencia
- 4. IFS**
 - a. Producción
 - b. Pruebas
 - c. Contingencia
- 5. ERP BI**
- 6. Dominio**
 - a. Producción
 - b. Contingencia
- 7. IPS**
 - a. Producción
 - b. Contingencia
- 8. PQR**
 - a. Producción
 - b. Pruebas
 - c. Contingencia
- 9. Sherlock**
 - a. Producción
 - b. Contingencia
- 10. Restauraciones**
- 11. Repositorio**
- 12. Aranda**
- 13. FTP**
- 14. Telefónica**
- 15. Biométrico**
 - a. Producción
 - b. Contingencia
- 16. SARL**
 - a. Producción
 - b. Contingencia
- 17. ControlDoc**
- 18. Microsoft**
- 19. Movilidad**

- 20. Comercial Pro
- 21. Multipay
 - a. Producción
 - b. Certificación
 - c. Contingencia
- 22. CODE
- 23. Radius

Linux

- 24. WS pruebas de entrega y tarificador
- 25. Portal Web
 - a. Producción
 - b. Contingencia
- 26. Colpensiones
 - a. Producción
 - b. Contingencia
- 27. Datastock
- 28. CEC

Para el alojamiento de las aplicaciones anteriormente mencionadas es necesario contar con la disponibilidad de los recursos mencionados en el **Anexo No. 01 “Especificaciones Técnicas”**.

CARACTERÍSTICAS DATACENTER PRINCIPAL

El proponente deberá proveer un servicio de Datacenter principal, con el fin de prestar el servicio integral solicitado cumpliendo con los ANS solicitados, los requerimientos generales para el Datacenter Principal son las siguientes:

- El proponente debe presentar la documentación necesaria que demuestre la propiedad del Centro de Datos Principal.
- El proponente debe demostrar que el Datacenter cuenta mínimo con el nivel de certificación TIER IV de diseño y construcción (emitida por el Uptime Institute) o ICREA nivel V (emitida por el International Computer Room Experts Association - ICREA). La certificación debe estar vigente.
- La solución ofertada debe estar alojada en un Datacenter ubicado en Colombia.
- El Datacenter debe demostrar por lo menos 4 años de madurez en prestación en servicios similares desde la construcción del Datacenter, se debe adjuntar carta del representante legal, indicando la madurez de la operación del centro de datos del oferente.
- El oferente debe presentar información correspondiente a ubicación detallada del Centro de Datos Principal.
- La operación de los equipos en el Datacenter debe ser 7x24x365
- La ubicación del Datacenter Principal ofertado será en la ciudad de Bogotá D.C y/o sus alrededores, a una distancia no mayor a 50 kilómetros de la sede principal de SERVICIOS POSTALES NACIONALES S.A.S

CARACTERÍSTICAS DATACENTER ALTERNO

El oferente deberá proveer un servicio de Datacenter alternativo al principal, con el fin de atender cualquier incidente o falla parcial o total que se pueda presentar con el servicio prestado. Las condiciones generales para el Datacenter Alternativo son las siguientes:

- La solución ofertada debe estar alojada en un Datacenter que cumpla mínimo las características TIER II o ICREA Nivel III, para lo cual presentará carta de cumplimiento firmada por el representante legal o la respectiva certificación (Uptime Institute o ICREA).
- La solución ofertada debe estar alojada en un Datacenter ubicado en Colombia.
- El oferente debe presentar información correspondiente a ubicación detallada del Centro de Datos Alternativo.
- El Datacenter alternativo deberá estar ubicado en una ciudad diferente a la del Data Center principal, o en todo caso contar con una distancia mínima de 50 km entre ellos.
- El oferente deberá incluir tres (3) pruebas al año de Failover y Rollback para confirmar el correcto funcionamiento de la solución. En el momento de las pruebas programadas de DRP los recursos de procesamiento y memoria deben ser los mismos recursos del ambiente de producción.
- Las pruebas de DRP serán para las aplicaciones que SPN S.A.S defina, dentro del listado de los sistemas que tienen ambientes de contingencia.
- Las pruebas de DRP se podrán realizar por servicio, aplicación y/o total a los servicios de Datacenter.
- El oferente deberá mantener las mismas condiciones relacionadas con las actualizaciones, parchado de sistemas operativos y demás elementos que conformen la solución del Datacenter Principal, de acuerdo con los ambientes solicitados en el DRP.
- RPO: El punto de recuperación de la Información en caso de algún evento, deberá ser cumpliendo la disponibilidad en un tiempo de dos (2) horas o menor a éstas.
- RTO: El tiempo de recuperación de la funcionalidad en caso de algún evento deberá estar dado en dos (2) horas o menor a éstas.
- La holgura operacional de los sistemas del DRP de los servicios del Datacenter alternativo debe ser mínimo del 50% a nivel funcional de procesamiento y memoria, y del 100 % a nivel de almacenamiento.
- El oferente debe diseñar la solución para que las pruebas de DRP se puedan ejecutar de forma independiente por cada una de las aplicaciones que tienen esquemas de contingencia.
- Los sistemas de información que deberán ser replicados hacia el Datacenter alternativo en caso de que se requiera activar el DRP son:
 - Sipost Producción
 - Seven Producción
 - Kactus Producción
 - IFS Producción
 - Portal Web

- Dominio
- IPS
- PQR
- Sherlock
- Biométrico
- SARL
- Colpensiones
- Multipay
- CEC
- Firewall
- Sedes remotas

Nota 1: Sí durante la ejecución del contrato se adicionan nuevos servicios con esquemas de contingencia, éstos automáticamente ingresan dentro del listado del requerimiento del punto inmediatamente anterior.

Nota 2: La infraestructura para la contingencia (referencia al **Anexo No. 01 “Especificaciones Técnicas”**.) Estos sistemas de información deben ser replicados en máquina virtual o física, aplicación, bases de datos y toda unidad de almacenamiento que requiera para su correcto funcionamiento.

SOLUCIÓN IAAS Y SAAS

SPN S.A.S requiere una solución integral Datacenter con los siguientes elementos para los diversos ambientes de negocio:

1. NUBE PRIVADA FÍSICA ENTORNO BASE DE DATOS DC PRINCIPAL

Proveer mínimo cuatro (4) máquinas físicas, que formen un pool de recursos para el ambiente Core de Base de datos de producción que cumplan con las siguientes características:

- El Pool debe tener mínimo un total de 128 Core, es decir, 32 Cores por servidor.
- La frecuencia básica de cada procesador debe ser de mínimo 3.0 Ghz; sin utilizar tecnologías de aceleración.
- Los procesadores utilizados deben ser Intel Xeon Platinum y/o Gold o AMD Epyc.
- El caché de CPU debe ser de mínimo 20 MB
- Memoria total del Pool de recursos solicitado 1 TB.
- Conexiones redundantes LAN y SAN.
- Almacenamiento mínimo de 100 GB exclusivo para el SO y 100 GB exclusiva para la paginación, adicional al almacenamiento de Disco SAN del punto posterior.
- Esta nube privada física requiere de una capacidad de Disco SAN de estado Solido Total después de Raid de 25 TB usables sin mecanismos de compresión y de duplicación y soportar mínimo 30.000 IOPS.
- Conectividad hacia la SAN y capacidad de almacenamiento solicitada en el respectivo numeral.
- Las capacidades de almacenamiento entregadas deben ser en sistemas de almacenamiento que deben estar ubicados en el cuadrante mágico de gartner de almacenamiento primario como líderes con vigencia de 2021 o superior.

- Debe incluir el licenciamiento de Microsoft SQL Enterprise en modalidad de servicio para los 128 Core del Cluster de Nube Privada de Base de datos. (Esto es importante ya que las instancias de BD se requieren para lectura y escritura)
- La solución de nube privada debe prestarse de acuerdo con los ANS solicitados y están descritos en la oferta.
- Las capacidades de almacenamiento entregadas deben prestarse de acuerdo con los ANS solicitados y que están descritos en la oferta.
- Garantizar que los equipos y materiales necesarios para la implementación y operación de los servicios objeto de la contratación cuenten con el respectivo soporte y garantía oficial por parte del fabricante.

Nota: SPN S.A.S podrá virtualizar este entorno, y no se deberá incurrir en sobre costos para SPN S.A.S.

Nota: De las cuatro (4) máquinas se corresponden: tres (3) para ambientes productivos en el Datacenter principal y una (1) para ambiente de contingencia en el Datacenter alterno; el cual puede ser utilizado en modo de lectura.

2. NUBE PRIVADA VIRTUAL X86 DATACENTER PRINCIPAL

Proveer una nube privada virtual X86 para mínimo 78 máquinas virtuales (Incluyendo los servidores virtuales de SQL) para ambientes de producción, pruebas y certificación, en alta disponibilidad, almacenamiento mínimo de 100 GB exclusivo para el SO y 20 GB exclusiva para la paginación (adicional al que se solicitará en el capítulo de almacenamiento) para cada máquina virtual, se debe incluir el licenciamiento (últimas versiones liberadas en el mercado) y soporte (versiones soportadas) a los siguientes Sistemas Operativos:

- Linux (cantidad inicial solicitada: 7)
- Windows Server (cantidad inicial solicitada: 71)

Se estima una línea base inicial del pool de virtualización para el Datacenter Principal para mínimo 78 Máquinas virtuales (Incluyendo los servidores virtuales de SQL) es de 400 vCPU Máxima sobre suscripción de 1 a 8 y debe entregarse en tecnología Intel Xeon Platinum y/o Gold o AMD Epyc y 2000 GB Memoria.

A. MONITOREO Y GESTIÓN NUBE PRIVADA VIRTUAL X86:

- La solución debe contar con un sistema de Monitoreo de mínimo las siguientes métricas: procesamiento, memoria, almacenamiento y red.
- La solución debe contar con trazabilidad de actividades de la administración y gestión, y debe tener una retención de logs mínima de tres (3) meses garantizada por el oferente.
- Se debe entregar reportes mensuales de consumos y optimización del uso de los recursos.
- El Contratista debe presentar los informes solicitados en cualquier momento de acuerdo con las solicitudes de SPN S.A.S.

B. ALCANCE LICENCIAMIENTO SQL SERVER NUBE PRIVADA VIRTUAL 86

Se estima una línea inicial del pool de bases de datos (SQL Server) de 200 vCPU, distribuidas de la siguiente manera:

- SQL Server Enterprise 30 %
- SQL Server Standard 70 %

Se debe incluir el licenciamiento (últimas versiones liberadas en el mercado) y soporte (versiones soportadas) a los siguientes Motores de bases de datos; por consiguiente, es responsabilidad del contratista cumplir las siguientes métricas a nivel de bases de datos:

- Umbral de procesamiento máximo al 80%.
- Usuarios soportados 2500.
- Tiempo de respuesta máximo: 10 Milisegundos en LAN.
- Tiempo de respuesta máximo: 50 Milisegundos en la sede
- Usuarios soportados concurrentes: 1500.

A las máquinas se les debe garantizar un nivel de IOPS constante

C. SERVICIO DE ALMACENAMIENTO NUBE PRIVADA VIRTUAL X86 Datacenter Principal

Adicional a la capacidad de almacenamiento solicitada para los sistemas operativos y para la nube privada de BD física, el oferente debe proveer una plataforma robusta de almacenamiento como servicio que soporte diferentes tipos de carga de trabajo cuya capacidad mínima sea de 60 TB SSD efectivos sin mecanismos de duplicación y compresión que soporten mínimo 80.000 IOPS en arreglos de disco SAN, los cuales deben estar distribuidos en los roles de los servidores virtuales de la nube X86. Este servicio debe cumplir mínimo con las siguientes características:

- Las capacidades de almacenamiento o hiperconvergencia entregadas deben ser en sistemas de almacenamiento que estén ubicados en el cuadrante mágico de gartner como líderes con vigencia mínima 2021 o superior.
- Proveer un feature para distribuir la data de acuerdo con la concurrencia de las cargas de trabajo, garantizando que la información con mayor uso se encuentre siempre en las capas más altas de la plataforma.
- Debe ser una solución elástica que permita presentar volúmenes por demanda y en caliente.
- La solución debe tener una escalabilidad de crecimiento hasta 200 TB mínimo y hasta 100.000 IOPS en arreglo de discos, la plataforma debe soportar este crecimiento en caliente en caso de ser requerido.
- La solución de nube privada virtual debe prestarse de acuerdo con los ANS solicitados y están descritos en la oferta.
- Las capacidades de almacenamiento entregadas deben prestarse de acuerdo con los ANS solicitados y que están descritos en la oferta.

D. MONITOREO Y GESTIÓN SERVICIO DE ALMACENAMIENTO

- La solución debe contar con un sistema Monitoreo de mínimo las siguientes métricas: Capacidad, cantidad de volúmenes, IO y rendimiento de los volúmenes o pool.
- La solución debe contar con trazabilidad de actividades de la administración y gestión, y debe tener una retención de logs mínima de 3 meses garantizada por el oferente.
- Se debe entregar reportes mensuales de consumos y optimización del uso de los recursos.
- El Contratista debe presentar los informes solicitados en cualquier momento de acuerdo con las solicitudes de SPN S.A.S.

SERVICIOS ADMINISTRADOS

i. Administración Sistema Operativo

El oferente debe suministrar la administración total de todos los sistemas operativos de acuerdo con la cantidad de servidores virtuales y físicos mencionados en los capítulos de Nube Privada Física y Virtual, las características de esta administración deberán ser la siguiente:

➤ Actividades de Instalación:

- Instalación de Sistema(s) Operativo(s) en cada máquina que haga parte de la arquitectura definida.
- Configuración de Sistema(s) Operativo(s) para el correcto funcionamiento de sus servicios anexos (los que apliquen en cada caso particular):
 - Respaldo y recuperación.
 - Monitoreo (según herramienta definida).
 - Antivirus.
 - NTP.
 - Actualizaciones.
 - Endurecimiento según estándares de SPN S.A.S o mejor práctica del mercado.
 - Reglas de conectividad y seguridad.
- Reporte de Pruebas de Servicio y de Sistema Operativo - Pruebas de detención y reinicio de Servicios Críticos y de Sistemas Operativos, para confirmar su correcto funcionamiento y también de los procesos definidos.

➤ Actividades de Transición

- Ejecución de plan de acción para levantamiento de documentación faltante Documentación pendiente, según se haya definido en la fase de Recepción o Instalación.
- Implementación de planes de mantenimiento preventivo que consta de las actividades de verificación de los siguientes componentes, elementos o procesos:
 - Espacio en disco.
 - Recursos de memoria.
 - Finalización y Resultados de los Back Ups
 - Archivos de logs.
 - Conteo de sesiones activas del Sistema Operativo.
 - Balanceo de conexiones y failover para clúster.
 - Procesos en background (si se requiere).
 - Parches o actualizaciones de software emitidos desde el momento de la instalación, activación de planes de Mantenimiento en Producción, para las máquinas incluidas en la solución definida.
 - Redes y seguridad.

➤ Actividades Monitoreo

- Definición de Umbrales de Monitoreo (One Time o SNMP).
- Definición de los valores en los cuales se generarán alarmas para el uso de mínimo los siguientes recursos:
 - Disco.

- Memoria.
- Procesamiento.
- Uso de red.
- URL
- WEB Service
- Canales
- Puertos
- Cantidad de ataques
- Dependiendo de la Herramienta de Monitoreo escogida, también se podrá monitorear los logs en busca de errores o eventos con palabras clave.
- Definición Monitoreo Servicios Críticos (One Time o SNMP).
- Definición de monitoreo de aplicaciones para determinar en el menor tiempo posible si hay afectación en su disponibilidad. Esto se hace actualmente de dos maneras:
 - Detección de Procesos: Es posible detectar si existe un proceso con determinado nombre, y en caso contrario, lanzar una alarma.
 - Conexión a Puertos: Es posible también determinar si la aplicación está activa, conectándose a los puertos de red en los que responde, como por ejemplo el puerto 80 en un servidor web, lanzándose una alarma en caso de falla al responder o de ausencia de respuesta.
- Instalación y/o Configuración de Herramientas y Agentes de Monitoreo (One Time o SNMP).
- Instalación de los agentes o configuración de la herramienta; según Herramienta de Monitoreo definida, y configuración de los umbrales definidos previamente.
- Inspección Física 7x24 en tres turnos diarios Control de las alarmas físicas que se puedan presentar en un servidor, para lo cual se implementan procesos de inspección periódica en busca de estados de alarma visibles en los LED o consolas de administración de los servidores.
- Monitoreo de Umbrales y Servicios Críticos 7x24, Monitorea las variables y sus umbrales según definición previa, y genera eventos para su gestión o escalamiento.

➤ **Actividades Operación**

El Servicio de Operación de sistema operativo consiste en la realización de actividades periódicas requeridas para el mantenimiento y aprovechamiento de los servicios. El servicio de operación se enfoca en garantizar la ejecución de tareas tanto de infraestructura, como propias de los servicios que sustenta. Incluye las siguientes tareas:

- Administración de Usuarios
- Creación de Usuarios.
- Desbloqueo de Usuarios.
- Cambio de Contraseña de Usuarios.
- Cambios Estándar
- Detención/Reinicio de Servicios Apache.
- Detención/Reinicio de Servicios Tomcat.
- Detención/Reinicio de Servicios MySQL.

- Detención/Reinicio de Servicios Otras Aplicaciones (documentadas y sobre aprobación de Cambio Estándar por parte de Cambios Datacenter).
- Ejecución de Actividades Periódicas, Ejecución y Reporte de Resultados de Tareas Periódicas de Mantenimiento de Infraestructura, o de Procesos de Negocio de SPN S.A.S.
- Ejecución de Mantenimientos delegados Programados
- Ejecución de Ventanas de Mantenimiento de Actualizaciones aprobadas (los administradores definen previamente qué actualizaciones se deben aplicar, y el cliente debe aprobarlo).
- Ejecución de Ventanas de Mantenimiento delegadas (debe existir documentación e instructivos aprobados previamente por el área de Administración y el área de Operación).
- **Upgrade de SO y motores de base de datos por solicitud de SPN S.A.S sin costo.**

➤ **Administración**

- Consisten en la realización de actividades periódicas de análisis del uso de recursos y el comportamiento de los servicios, para garantizar su disponibilidad, uso óptimo y crecimiento sostenible a futuro. El servicio de administración se enfoca en garantizar la disponibilidad del sistema operativo y la integridad y estabilidad de su configuración. Incluye la atención y solución a incidentes y problemas de sistema operativo, y apoyo a la resolución de problemas de aplicaciones soportadas.
- Análisis Consumo de Recursos (Mantenimiento) Mensual (contra informe generado): Los administradores deben presentar un análisis sobre los reportes mensuales (generados automáticamente con la Herramienta de Monitoreo que se haya definido), con las recomendaciones que apliquen para optimizar el uso de los recursos de la infraestructura existente. Esto no incluye cambios a la infraestructura, arquitectura o topología, ni afinamientos por problemas evidenciados en la recepción de infraestructura preexistente.
- Revisión parches y actualizaciones (Mantenimiento) Mensual.

I. Administración Bases de Datos

La Administración de Base de Datos tiene como objetivo brindar un servicio de alta calidad a la cual debe realizarse con Ingenieros expertos y certificados en Administración de bases de datos. El oferente debe realizar la administración de las bases de datos del sitio principal y alternativo. La cantidad de instancias de bases de datos a administrar es de 35 entre las que se incluyen Bases de Datos SQL Server, MariaDB, MySQL y PostgreSQL u otros motores similares. El alcance general del servicio debe tener el siguiente alcance:

- Envío de reportes periódicos de usuarios cuyas cuentas van a expirar en un periodo próximo. Manejo y expiración de cuentas de usuario (Herramienta)
- Notificación al cliente de top process-top query, monitoreo procesos core, top five de consultas pesadas
- (Monitoreo recursos de memoria, cpu, I/O) alertados por herramienta de monitoreo
- Garantizar y monitorear que los procesos críticos sean exitosos según el core del negocio
- Validar disponibilidad de espacio de filesystems y depuración respectiva
- Validar finalización exitosa de los Backups y notificar los Backups fallidos (Revisar el reporte de inicio y finalización de los backups, apoyándose con el reporte que emite la herramienta)

- Monitoreo y envío de notificación de objetos (asociados al diccionario y/o aplicación) con estado invalido
- Monitoreo y envío de notificación de índices de la aplicación que se detecte en estado no valido. Evento que se dispara cuando un objeto de tipo índice se invalida de manera abrupta a raíz de un cambio, incidente o requerimiento de usuario final.
- Monitoreo y envío de notificación de espacios disponibles para almacenar los archive logs
- Monitoreo y envío de notificación conteo de sesiones concurrentes sobre la base de datos
- Monitoreo y envío de notificación espacio disponible en Tablespace y/o filegroups
- Monitoreo y envío de notificación disponibilidad del Listener, de las bases de datos.
- Monitoreo y envío de notificación procesos background (pmon, logwriter, dbwriter, etc) de bases de datos. Estos son procesos que garantizan que una instancia de Base de Datos esta arriba o abajo.
- Monitoreo, detección, notificación y cancelación (bajo autorización cliente) en bloqueos de base de datos. Se minimizaría aún más el tiempo si se acuerda previo con el cliente que todo bloqueo se cancele y notifique quien lo origino sin pasar por proceso de autorización
- Endurecimiento según estándares de SPN S.A.S o mejor práctica del mercado.

➤ **Atención a Incidentes**

- Atención Incidentes (caídas de: bases de datos, listener; expiración cuentas; desbloqueo de usuarios)
- Atención Incidentes (Eventos críticos de Base de Datos, apertura y seguimiento de casos a proveedores por problemas de Bug's o issues nuevos y/o desconocidos))
- Procedimientos de escalamiento y soporte a incidentes a usuarios del cliente final.
- Table Space / Disk Group (File System SQL)
- Monitoreo: Control diario que supere un 85% Warning y un 95% Critical con herramientas de gestión y de
- RDBMS
- Administración: Agregar espacio a Table Space alarmado

➤ **Seguridad**

- Creación, modificación, borrado y/o bloqueo usuario
- Creación, modificación, asignación, borrado de roles y/o perfiles
- Asignar y/o revocar privilegios sobre objetos de la BD
- Hardening de Base de Datos

➤ **Ejecución de tareas programadas y scripts básicos**

- Ejecución Scripts de alteración de estructura asociados a: Compile y replace de package, function, procedure, triggers y alter de índices y tablas, truncate. Bajo solicitud y autorización del cliente previo envío del requerimiento.
- Ejecución de Scripts para alteración de Data del cliente asociados a: Insert, Select, Delete, Update está restringida, por no conocerse el impacto de estos cambios en el negocio del cliente. Las personas autorizadas para ver y manipular la data del cliente serán sus propios administradores.

➤ **Parches**

- Evaluación, recomendaciones e instalación de aplicación de parches y actualizaciones en BDs. Nota: Este proceso se realiza una vez al año.
- Informe Estado del Servicio y Capacity Planning
- Informe Ejecutivo Semestral se va a distribuir de la siguiente forma. Incluye: estado del servicio (cantidad de requerimientos atendidos, cantidad de incidentes atendidos, niveles de servicio, tiempo de solución, SLA) y Capacity Planning (Medición de Crecimiento de Base de Datos) • Informe Mensual Automático (consumo, crecimiento usado a la fecha) • Informe Incidentes cuando se presente

iii. Control administrado

- Actividades de Planeación, Seguimiento, Control y Apoyo a Incidentes
- Implementación de las mejores prácticas en ASM
- Análisis de Objetos Fragmentado

iv. Servicio administrado en sitio

El oferente debe suministrar servicio en sitio de dos (2) ingenieros de sistemas, eléctricos, electrónicos o telecomunicaciones con experiencia mínima de tres (3) años en gestión de TI, administración de SO, red, y bases de datos.

Se requiere que estén en sitio, para lo cual SPN S.A.S suministrará el puesto de trabajo, quienes prestarán el servicio en el siguiente horario:

- Ingeniero 1 horario de lunes a viernes de 8 AM a 5 PM
- Ingeniero 2 horario de lunes a viernes de 2 PM a 10 PM


Nota: Sí durante la ejecución del contrato se adicionan nuevos servicios, éstos automáticamente ingresan dentro del esquema de prestación de servicios descritos en el presente documento: administración, soporte, backups, monitoreo, operación, seguridad, data center, conectividad, etc. Según aplique.

SERVICIO DE BACKUP ADMINISTRADO

Las soluciones de respaldo o backup solicitada debe ser implementada con respaldo directo a disco (conocido como Backup to Disk). Se debe realizar el respaldo y retención, acorde a los volúmenes de datos y a las mejores recomendaciones para estas actividades, se debe respaldar el 100% de la data de bases de datos y aplicaciones (Snapshot, imágenes) de producción y desarrollo en el Datacenter Principal.

De acuerdo con los volúmenes de la data a ser respaldada se consideran conexiones hacia la plataforma a través de la red LAN o de la red SAN; sobre esta última, para casos con grandes volúmenes de datos que impacten en tiempo las ventanas apropiadas para dicha actividad.

Las soluciones de backup deben incluir el dimensionamiento de los agentes de software apropiados para la toma en "caliente" o "frío" del respaldo de los datos o información de las aplicaciones y bases de datos. Igualmente se debe considerar las actividades de reporte, monitoreo, recuperación y administración de toda la plataforma, por parte del Oferente.

	JUSTIFICACIÓN PARA URGENCIA INMINENTE
---	--

Las políticas de backup solicitada es la siguiente:

Backup a Disco: Esta política combina el respaldo directo en disco (vía SAN o LAN)

Respaldo a disco	Diaria	Semanal	Mensual	Anual
Tipo Respaldo	Incremental	Total	Total	Total
Retención	7 días	4 semanas	Duración del Contrato	Duración del Contrato
Espacio en Disco	Si	Si	Si	No
Horario	Lunes a sábado	Sábado-Domingo	1er día del Mes	1er día del Año
	10 pm-06 am	10 pm-06 am	10 pm-06 am	10 pm-06 am


Nota: La copia de seguridad anual al finalizar el contrato debe entregarse en la nube en formato abierto por parte del contratista, esto con el fin de tener disponible inmediatamente esta información a través de un servicio web. Esta data deber estar disponible durante 3 meses luego de la liquidación del contrato, para el movimiento de información. Acompañado de un inventario de los backups disponibles para descarga.

Nota: Durante la etapa de transición, el oferente entrante debe descargar los backups anuales entregados por el oferente saliente descritos en el punto anterior; para que sean almacenados y/o custodiados en la infraestructura del oferente entrante con permanencia durante la ejecución del contrato; los cuales podrán ser solicitados por SPN S.A.S en cualquier momento durante la ejecución del contrato. El oferente entrante no será responsable de la integridad de la data descargada.

II. CONECTIVIDAD

Adicional SPN S.A.S requiere la conectividad WAN, centralizada en un Datacenter, que permita la conexión a nivel nacional de las ciudades principales de las regionales, así:

SEDES SPN 4-72 SD-WAN (MPLS e Internet)					
ITEM	Tipo	REGIONAL	DIRECCIÓN	BW (MPLS)	BW (Internet Dedicado)
1	SD-wan	REGIONAL ORIENTE	Kilómetro 4 vía Giron- Bucaramanga – Centro Empresarial el Bueno, Bodega 2	100	100
2	SD-wan	REGIONAL ORIENTE	CENTRAL DE TRATAMIENTO - BUCARAMANGA – CARRERA 26a No. 104-07	50	50
3	SD-wan	REGIONAL ORIENTE	CD CUCUTA / AVENIDA 8 # 21 NORTE – 116 ZONA INDUSTRIAL	50	50
4	SD-wan	REGIONAL OCCIDENTE	CALI LA FLORA, Av. 3Norte No 52-33	100	100
5	SD-wan	REGIONAL OCCIDENTE	Zona uno Cali / Carrera 3 No 10 - 49 edificio soho	50	50
6	SD-wan	REGIONAL SUR	IBAGUE - Kra 16 Sur No. 90 – 66 Parque Empresarial Berlín Bodegas 1 y 2	100	100
7	SD-wan	REGIONAL SUR	NEIVA / Huila Calle 29 a Sur No. 4-37 zona industrial.	30	30
8	SD-wan	REGIONAL EJE CAFETERO	CARRERA 1 Norte, número 35-11 y 35-13 La Florida, Villamaría Caldas	100	100
9	SD-wan	REGIONAL NORTE	BARRANQUILLA CTP Y ADMINISTRATIVA - LA UNION -CALLE 30 #13C-07	100	100
10	SD-wan	REGIONAL NOROCCIDENTE	RECEPCION PRINCIPAL CENTRAL DE TRATAMIENTO – MEDELLIN – Caribe CRA. 64C # 72-20	100	100
11	SD-wan	BOGOTA	SEDE PRINCIPAL BOGOTA DIAGONAL 25 G # 95 A 55	500	500
12	SD-wan	BOGOTA	SAN CAYETANO BODEGA 16 Y 17	50	50
13	SD-wan	BOGOTA	C.D MURILLO TORO – Calle 12 B # 8 A – 25	40	40
14	SD-wan	YOPAL	PO YOPAL / calle 40 No. 24 – 69	20	20
15	SD-wan	FUNZA	FUNZA / COMPLEJO INDUSTRIAL Argelia, km 3 vía Funza - Siberia, bodega 15	40	40
16	SD-wan	DATA CENTER ALTERNO	Según Diseño Técnico del oferente – RTO y RPO	500	500

	JUSTIFICACIÓN PARA URGENCIA INMINENTE
---	--

SEDES SPN 4-72 (Solo Internet)					
ITEM	Tipo	REGIONAL	DIRECCIÓN	BW	Tipo
17	Internet Dedicado	BOGOTA	CL70 13 90	20	Internet
18	Internet Dedicado	VILLAVICENCIO	CL 39 32-02 CENTRO	20	Internet
19	Internet Dedicado	NEIVA	Carrera 1d bis No 15-13	20	Internet
20	Internet Dedicado	TUNJA	carrera 6 # 64-03 Barrio Asís.	20	Internet
21	Internet Dedicado	FLORENCIA	KR 12 12-57 BARRIO CENTRO	20	Internet
22	Internet Dedicado	SANTA MARTA	CO Santa Marta Crr 7 C # 29 – 06 / (5) 4358149	20	Internet
23	Internet Dedicado	CARTAGENA	DIAG.21 # 48 - 58 EL BOSQUE	20	Internet
24	Internet Dedicado	PASTO	Calle 14 12 30 bodega 1 barrio las violetas III	20	Internet
25	Internet Dedicado	POPAYAN	CL 4 5-74	20	Internet
26	Internet Dedicado	PALMIRA	CL 31 28-45	20	Internet
27	Internet Dedicado	VALLEDUPAR	CL 16A 7-44 BAARRO CENTRO	20	Internet
28	Internet Dedicado	BUENAVENTURA	KR 5 A 1 -13	20	Internet
29	Internet Dedicado	CO.SINCELEJO	calle 38 # 7-214 Parque comercial Agrosabana	20	Internet
30	Internet Dedicado	CO.MONTERIA	Carrera 17 N° 24-09 BARRIO PASATIEMPO	20	Internet

NOTA:

SERVICIOS DE INTERENET DEDICADO, MPLS, SDWAN (sedes 1 a 16)

Sedes que incluye el servicio de conectividad a través de la red MPLS (Privada), adicionalmente incluye el servicio de Internet Dedicado para cada sede, lo que converge en doble última milla para cada una de las sedes a través del servicio de SDWAN.

ANCHO DE BANDA

El ancho de banda de cada última milla: MPLS e Internet Dedicado, debe corresponder con lo solicitado en la tabla anterior; por ejemplo:

SEDE PRINCIPAL (MPLS) = 500mbps

SEDE PRINCIPAL (Internet Dedicado) = 500mbps

SERVICIOS DE INTERNET DEDICADO (sedes 17 a 30)

Las sedes (17-30) solo requiere el servicio de Internet Dedicado sin SDWAN.

NOTA: Las cantidades y descripciones en Datacenter y comunicaciones son estimadas teniendo en cuenta la necesidad actual de SPN S.A.S las cuales serán variables durante la ejecución del contrato de acuerdo con el crecimiento y necesidades de los procesos de SPN S.A.S.

Dentro del alcance del contrato se podrán solicitar servicios adicionales o conexos, siempre y cuando guarden relación directa con el objeto y hayan sido previamente acordados entre las partes, respecto de su alcance, costo y funcionalidad.

DATOS E INTERNET

En el presente Anexo Técnico se presentan las condiciones que aplican para el presente proceso de contratación y que se debe tener en cuenta por los proponentes para la prestación de los servicios:

i. Obligaciones

- Proveer los canales de datos, de internet dedicado y conexión hacia los Data Center principal y alterno de acuerdo con lo establecido en el presente Anexo Técnico.
- Suministrar e instalar los equipos, elementos y dispositivos necesarios para el servicio de conectividad e internet dedicado.
- Presentar las siguientes certificaciones para el servicio de conectividad:
- Certificación NAP Colombia

- Certificación NAP de la Américas

ii. Condiciones Generales

Las condiciones que deben estar incluidas dentro del Servicio de Conectividad e internet para la red de alta disponibilidad y continuidad, predictiva, segura, costo eficiente y con madurez tecnológica, que responda a la transformación actual en el sector de las TIC son:

- Soporte, administración y gestión del equipamiento suministrado.
- Conectividad Datacenter Principal - Datacenter Alterno
- Conectividad Internet Datacenter
- Conectividad SD WAN Sedes

Los servicios de datos de las sedes remotas contarán con una solución de conectividad principal de Datos que concentra en el Data Center Principal como nodo principal. De igual forma, cada sede remota también contará con un enlace de internet Dedicado que a su vez funcionará como respaldo a la principal bajo arquitectura SDWAN (ambas últimas millas funcionarán en modo activo-activo), ambas bajo tecnología dedicadas 1:1, utilizando recursos y rutas de red independientes, de tal manera que la falla en un nodo de la red del CONTRATISTA no genere indisponibilidad del servicio. Este requerimiento se extiende a la inclusión del hardware y software necesario para el manejo de los dos enlaces (enrutadores y software de propósito específico). Tanto el enlace principal de Datos como el enlace de Internet dedicado de cada sede deben tener el mismo ancho de banda y a través de fibra óptica independiente. Todas las sedes remotas se concentran en el Data Center principal, donde estarán alojados los servicios de misión crítica de SPN S.A.S; servicios descritos en el capítulo de Data Center.

Se debe suministrar y garantizar el funcionamiento de los servicios de conectividad de cada sitio remoto hacia los sitios centrales, de tal manera que exista integración con Internet de navegación.

La red deberá estar implementada sobre plataforma SD-WAN, extremo a extremo para los enlaces principales y de internet dedicado de respaldo, los cuales deben estar bajo tecnología de red dedicada y soportar IPV6. Sobre dichos enlaces se debe permitir la aplicación de QoS extremo a extremo.

El contratista debe incluir los canales de internet dedicado para cada una de las sedes remotas y para la sede principal, independiente del canal de internet usado en el Data Center principal que se usa para la publicación de los servicios ubicados en el Data Center. El contratista deberá de manera proactiva, detectar un uso y/o consumo elevado de los canales WAN o Internet e informar a la persona designada por SPN S.A.S para la toma de decisiones.

OBJETO DEL SERVICIO DE CONECTIVIDAD – INTERNET DEDICADO

Contratar los servicios de diseño, implementación, puesta en operación, soporte, gestión y administración de la infraestructura de conectividad para todas las sedes de SPN S.A.S que incluya los enlaces de Internet y, a su vez, que incluya la integración con el Data Center Principal/alternativo contemplando su sistema de Disaster Recovery Plan (DRP), sus servicios y funciones de redes definidas por software, con el fin de permitir el acceso de toda la planta de personal de SPN S.A.S a las aplicaciones de misión crítica de SPN S.A.S según los sistemas establecidos en el capítulo de Data Center.

a) Objetivos específicos de Conectividad – Internet

- Diseño, configuración, instalación y gestión de los enlaces de conectividad WAN y de los canales a internet dedicado de SPN S.A.S.
- Diseño, configuración, instalación y gestión de los equipos activos relacionados con la solución de SDWAN.
- Diseño, configuración, instalación y gestión de los equipos activos relacionados con la solución de Internet dedicado.
- Detallar el diseño de la solución SD-WAN e Internet dedicado para prestar un servicio eficiente.
- Releva toda la infraestructura de telecomunicaciones actual bajo el servicio de diseño validación y migración de SD-WAN e Internet dedicado de SPN S.A.S.
- Suministrar, instalar, configurar y gestionar los equipos, cables, hardware y software necesario para la red de datos e internet dedicado de SPN S.A.S. Incluir garantías de los equipos suministrados.
- Como requerimiento de SPN S.A.S, la implementación de la conectividad WAN debe realizarse dentro de los noventa (90) días estipulados, garantizando la prestación de los servicios a partir del primer día de la etapa de operación.

b) Facturación de los Servicios de Conectividad – Internet

- La etapa de transición: Es total responsabilidad del contratista realizar la transición dentro de los noventa (90) días estipulados, garantizando la prestación de los servicios a partir del primer día.
- La etapa de Operación: Incluye la facturación mes vencido de acuerdo con el plan de pagos estipulado en la propuesta económica restando los descuentos y penalizaciones correspondientes al periodo.
- La etapa de empalme: Incluye la facturación mes vencido de acuerdo con el plan de pagos estipulado en la propuesta económica restando los descuentos y penalizaciones correspondientes al periodo.

c) Equipo Humano Requerido para la Implementación del servicio

PERSONAL REQUERIDO PARA LA EJECUCIÓN DEL CONTRATO EL CONTRATISTA deberá asignar el siguiente equipo de trabajo para el desarrollo del contrato, de conformidad con los tiempos que se indican a continuación:

Se requiere durante la ejecución del contrato con disponibilidad del cien (100%), se debe presentar Hoja de vida y soportes con la oferta

- Cantidad: Uno (1)
- Ingeniero electrónico, y/o sistemas, o carreras afines.
- Experiencia mínima diez (10) años en manejo de proyectos relacionados con el objeto contractual.
- El perfil presentado deberá contar estar certificado en ITIL Foundation V3 o superior, y Certificado en PMP.

Funciones para desempeñar: Garantizar el cumplimiento de los objetivos. o Presentar los reportes periódicos y por demanda asociados al servicio o Identificar oportunidades de mejora y asegurar su elaboración y ejecución o Identificar riesgos y asegurar su elaboración y ejecución.

JUSTIFICACIÓN PARA URGENCIA INMINENTE

Participar en los comités de cambios, calidad, riesgos y demás en los que sea requerido por SPN S.A.S.

Presentar recomendaciones a SPN S.A.S. o El personal será dedicado para la fase de transición, para las demás fases estará por demanda de SPN S.A.S.

Nota: Presentar máximo quince (15) días siguientes a la adjudicación del contrato; el perfil requerido con los respectivos soportes enunciados en los numerales.

d) Requerimientos técnicos específicos para la solución de SD-WAN


El servicio de SD-WAN y todas las funcionalidades solicitadas debe ser dimensionado en cuanto a usuarios (para mínimo 1200), conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo basado en los anchos de banda solicitados, por ende, no puede licenciarse o tener alcance basado en otros parámetros.

ESPECIFICACIONES TÉCNICAS GATEWAY SD-WAN	
Descripción	Características Generales
Generalidades	Se requiere que la solución funcione sobre una red IP basada en MPLS o enlaces de Internet. Las configuraciones de los enlaces deberán quedar en activo-activo, con capacidad de discriminación de tráfico por aplicación, priorización de tráfico, re-enrutamiento automático en caso de falla de alguno de los enlaces.
	Las soluciones deben transportar datos, voz y video manteniendo los niveles de QoS, disponibilidad y seguridad, en todos los enlaces y sitios requeridos.
	Enrutamiento Inteligente, con el fin de mantener la experiencia de usuario adecuada para las diferentes aplicaciones, la solución debe estar en capacidad de enrutar el tráfico teniendo en cuenta requerimientos mínimos como las condiciones de Jitter (variación del retardo), retardo y pérdida de paquetes en cada uno de los enlaces disponibles.
	Se requiere que las soluciones permitan controlar las políticas de enrutamiento inteligente de forma centralizada desde el controlador/orquestador de la solución, el cual puede estar ubicado en la sede principal.
	Ante falla del controlador/orquestador de la solución o de conectividad ante el mismo la solución debe poder seguir operando normalmente (no debe suspenderse el reenvío de tráfico), ni debe afectarse la capacidad de redirección del tráfico ante caída o degradación de los diferentes enlaces.
	Ante falla del controlador/orquestador de la solución o de conectividad ante el mismo la solución debe permitir hacer configuraciones de nuevas políticas de enrutamiento SD-WAN, monitores de tráfico directamente sobre los equipos SD-WAN en las diferentes ubicaciones. Una vez el controlador/orquestador se encuentre nuevamente en línea o se haya restaurado la conectividad con el mismo, debe ser posible importar en el orquestador los cambios realizados.
	La solución provista en el servicio debe estar en capacidad de hacer el monitoreo del desempeño o salud de los enlaces usando al menos los protocolos ICMP y HTTP.
	En adición al enrutamiento inteligente de tráfico, el servicio de SD-WAN en las sedes deben estar en capacidad de hacer balanceo de tráfico entre los diferentes enlaces usando cualquiera de los siguientes métodos:

JUSTIFICACIÓN PARA URGENCIA INMINENTE

ESPECIFICACIONES TÉCNICAS GATEWAY SD-WAN	
Descripción	Características Generales
	<ul style="list-style-type: none"> Ancho de banda Sesiones Spillover o desborde. IP fuente – destino
	Debe ser posible hacer enrutamiento o distribución del tráfico con base en: Dirección IP origen o destino, Usuario o grupo de usuarios (definidos localmente o mediante integración con un servidor remoto LDAP, RADIUS o TACACS, o esquemas de Single Sign On), Servicio en Internet (al menos Office 365, AWS, Azure, Adobe, Google Cloud, Youtube, Alibaba, Aol y Citrix) o Aplicaciones (debe existir una base de datos de al menos 2000 aplicaciones disponibles incluyendo VNC, Gotomeeting, Dropbox, Amazon Alexa, Logmein, SAP router y Whatsapp).
	Las soluciones deben permitir definir las preferencias en los path o caminos WAN que debe tomar una aplicación en la red.
	Dado que como parte de las alternativas de caminos WAN se pueden tener casos con WAN híbrida (enlace vía MPLS e INTERNET), se requiere que el overlay que se genere, tenga soporte de IPsec con encriptación fuerte (algoritmos AES128, AES256 con autenticación SHA256, SHA384 y SHA512), de tal manera que se proteja la información ante posibles ataques de tipo man-in-the-middle.
	La tecnología overlay soportada por la solución de SD-WAN debe estar en capacidad de crear túneles bajo demanda (ADVPN) entre sedes para enrutar eficientemente el tráfico de las aplicaciones.
	Las soluciones deben estar respaldada por un laboratorio de investigación y desarrollo que ofrezca inteligencia en tiempo real entregando actualizaciones de seguridad completas, investigadores de amenazas de seguridad, ingenieros y especialistas forenses.
	Para garantizar la protección de inversión, alineación con las tendencias tecnológicas de la industria, soporte y vigencia tecnológica y estar preparados para los requerimientos futuros, El servicio de SD-WAN debe estar basado en equipos de comunicación que correspondan a una marca o fabricante que figure como líder en el cuadrante de Cuadrante Mágico Gartner para soluciones de WAN Edge durante al menos los últimos dos años (2020 y 2021) y para su acreditación deberá presentar el informe correspondiente a cada año.
	El servicio debe incluir una capa de analítica, logs, monitoreo y reportes la cual debe garantizar una retención mínima de tres (3) meses.
	El servicio debe incluir un orquestador o gestión centralizada el cual se debe contemplar para la cantidad total de dispositivos SD-WAN
Características mínimas de calidad de servicio	El servicio de SD-WAN debe soportar traffic shaping basado en fuente (dirección IP, usuarios locales y grupos), destino (dirección IP, FQDN, URL o categoría), servicio (General, acceso web, acceso a archivos, servicios de correo y red, autenticación, acceso remoto, tunneling, VoIP, mensajería y otras aplicaciones, web proxy), aplicación, categoría de aplicaciones, categoría de URLs.
	Capacidad de poder definir ancho de banda garantizado y máximo, como un valor en kbps o como porcentaje del ancho de banda de la interfaz.

ESPECIFICACIONES TÉCNICAS GATEWAY SD-WAN	
Descripción	Características Generales
Características mínimas de manejo de paquetes	El servicio de SD-WAN en las sedes deben estar en capacidad de hacer marcado de DSCP en los paquetes.
	Capacidad de definición de shapping de entrada o de salida.
	Soporte de reglas entre interfaces, zonas (grupos de interfaces) o VLANs.
	Políticas basadas en Identidad (usuario o grupo al que pertenece el usuario)
	Definición de reglas y objetos para IPv4 e IPv6 via GUI y CLI
	La solución debe tener la capacidad de hacer captura de paquetes para luego ser exportada en formato PCAP.
	Soporte de NAT: NAT estático, NAT dinámico, PAT, NAT64, NAT46, NAT66.
	Soporte a reglas basadas en servicios cloud populares de Internet, en donde se tiene una base de datos que se actualiza dinámicamente. Esta base de datos puede usarse también en enrutamiento y balanceo de enlaces o SD-WAN.
	Soporte de PIM SM y DM para tráfico multicast.
	Soporte de Antispoofing o reverse path lookup.
Características mínimas de VPN	Soporte a reglas basadas en geolocalización.
	Soporte de VPNs IPsec sitio a sitio y cliente – sitio.
	Capacidad de establecimiento de Ipsec sitio a sitio, sin requerir de licenciamiento por VPN sin límite
	Soporte para IKEv2 e IKE Configuration Method
	Soporte de VPNs con algoritmos de cifrado: AES256, AES192, AES128.
	Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5, 14, 21 y 32.
	Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1, SHA256, SHA-384 y SHA-512.
	La cantidad de VPN site to site se requiere sin límite.
Características mínimas de filtrado web	La cantidad de VPN SSL se requiere sin límite.
	Las soluciones deben permitir filtrado de contenido web, filtrado de URLs y servicio de filtrado web basado en categorías del fabricante, para IPv4 e IPv6.
	Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
	Las soluciones deben soportar filtrado de contenido mediante la característica de “Safe Search” o “Búsqueda Segura” para prevenir imágenes y sitios web con contenido explícito en los resultados de búsqueda. Esto debe ser soportado para los siguientes sitios: Google, Yahoo, Bing y Yandex.
	El filtrado debe ser sobre tráfico HTTP y HTTPS, siendo posible exceptuar inspección de tráfico HTTPS por categoría.
Referencias de equipos	El Proveedor debe suministrar el servicio proporcionando equipos que cumplan las características solicitadas.
Características mínimas de control de aplicaciones	Debe basarse en categorías de aplicaciones que permitan seleccionar grupos de firmas basados en un tipo de categoría.
	La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
	Las soluciones deben tener un listado de al menos 4000 aplicaciones ya definidas por el fabricante.

	JUSTIFICACIÓN PARA URGENCIA INMINENTE
---	--

ESPECIFICACIONES TÉCNICAS GATEWAY SD-WAN	
Descripción	Características Generales
	El listado de aplicaciones debe actualizarse periódicamente.
	Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, hacer traffic shapping, registrar en log.
	Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
	Debe ser posible inspeccionar aplicaciones tipo Cloud como YouTube, Dropbox, Baidu, Amazon entre otras entregando información como login de usuarios, transferencia de archivos y videos visualizados.
Características de inspección de tráfico cifrado	El servicio de SD-WAN debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, prevención de Fuga de Información, Antivirus e IPS (Intrusion Prevention System).
	Debe ser posible definir si la inspección se realiza desde múltiples clientes conectando a servidores (es decir usuarios que navegan a servicios externos con SSL) o protegiendo un servidor interno de la Compañía.
	Las soluciones deben soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3.
Características de administración	El servicio de SD-WAN debe proveer a SPN S.A.S una Interface gráfica de usuario (GUI), vía Web por HTTPS e interfaz de línea de comando (CLI) con acceso de lectura de la solución, ya sea de manera centralizada o descentralizada en cada dispositivo.
	Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones que pueden modificar o visualizar.
	El servicio de SD-WAN deben tener soporte SNMP versión 3.
	Soporte de syslog.
	Soporte de Netflow y Xflow.

e) Requerimientos técnicos para el servicio de Internet

El servicio de Internet Dedicado de la sede principal, del Data Center principal y del Data Center alterno debe brindar conectividad de una manera confiable, simétrica, sin reuso sobre una red de nueva generación. Debe contar como mínimo con las siguientes características:

- Servicio provisto con Fibra Óptica, conexión directa nodo-cliente.
- Conexión directa al NAP Colombia.
- Gestión y monitoreo 7x24x365.
- Servicio con compensación por tiempos de no servicio.
- Upstream del 100%
- Downstream del 100%
- Servicio de monitoreo del tráfico de la red en tiempo real, con la consolidación de informes mensuales o cuando se requieran por SPN S.A.S para validación con el equipo de Pos-venta del Contratista y el equipo dispuesto por SPN S.A.S.
- Sobre los canales se debe realizar segmentación del ancho de banda, traffic shaping, se debe visualizar el tráfico tanto por protocolo, IP, aplicación como su consumo en un tiempo real y determinado.

- Ofrecer servicio Portal de atención al cliente que permita el registro, seguimiento y cierre de casos.
- Certificación NAP Colombia.
- Certificación NAP Américas.
- Todos los canales deben contar con reuso 1:1.
- Proveer un ancho de banda mínimo según la tabla de BW descrita en el presente Anexo Técnico como línea base; adicional en el caso de saturación del canal al 80 % el proponente deberá incrementar el ancho de banda para mitigar esta saturación, con crecimiento estimado del 30% durante el primer año sin costo adicional para SPN S.A.S. Para los años posteriores se realizará viabilidad y el contratista presentará oferta a SPN S.A.S para su aprobación. El valor de esta ampliación debe estar dentro de los parámetros ofertados por el Contratista en esta primera etapa.


El servicio Internet Dedicado para cada una de las sedes remotas de SPN S.A.S debe brindar conectividad de una manera confiable, simétrica, sin reuso sobre una red de nueva generación. Debe contar como mínimo con las siguientes características:

- Servicio provisto con Fibra Óptica, conexión directa nodo-cliente.
- Gestión y monitoreo 7x24x365.
- Servicio con compensación por tiempos de no servicio.
- Upstream del 100%
- Downstream del 100%
- Servicio de monitoreo del tráfico de la red en tiempo real, con la consolidación de informes mensuales o cuando se requieran por SPN S.A.S para validación con el equipo de Pos-venta del Contratista y el equipo dispuesto por SPN S.A.S.
- Ofrecer servicio Portal de atención al cliente que permita el registro, seguimiento y cierre de casos.
- Certificación NAP Colombia.
- Certificación NAP Américas.
- El canal debe contar con reuso 1:1.
- Proveer un ancho de banda según la tabla de BW definida en el presente anexo Técnico. En el caso de saturación del canal al 80 % el proponente deberá incrementar el ancho de banda para mitigar esta saturación, con crecimiento estimado del 30% durante el primer año sin costo adicional para SPN S.A.S. Para los años posteriores se realizará viabilidad y el contratista presentará oferta a SPN S.A.S para su aprobación. El valor de esta ampliación debe estar dentro de los parámetros ofertados por el Contratista en esta primera etapa, así:

ITEM	SEDE	ANCHO DE BANDA MÍNIMO A INTERNET
1	Sede PRINCIPAL SPN	500 Mbps
2	Data Center Principal	200 Mbps
3	Data Center Alterno	100 Mbps
4	Cada Sede Remota	Entre 20 y 100 Mbps

a) Requerimientos técnicos para el servicio de Datos.

El servicio de Datos debe ser del tipo 1:1 sin reuso, simétrico en cuanto a velocidades de carga y descarga. El ancho de banda se debe suministrar teniendo en cuenta la tabla de Ancho de Banda por sede incluida en el presente Anexo Técnico.

	JUSTIFICACIÓN PARA URGENCIA INMINENTE
---	--

Los anchos de banda definidos para cada sede son los siguientes:

SEDES SPN 4-72 SD-WAN (MPLS e Internet)					
ITEM	Tipo	REGIONAL	DIRECCIÓN	BW (MPLS)	BW (Internet Dedicado)
1	SD-wan	REGIONAL ORIENTE	Kilómetro 4 vía Giron- Bucaramanga – Centro Empresarial el Bueno, Bodega 2	100	100
2	SD-wan	REGIONAL ORIENTE	CENTRAL DE TRATAMIENTO - BUCARAMANGA – CARRERA 26a No. 104-07	50	50
3	SD-wan	REGIONAL ORIENTE	CD CUCUTA / AVENIDA 8 # 21 NORTE – 116 ZONA INDUSTRIAL	50	50
4	SD-wan	REGIONAL OCCIDENTE	CALI LA FLORA, Av. 3 Norte No 52-33	100	100
5	SD-wan	REGIONAL OCCIDENTE	Zona uno Cali / Carrera 3 No 10 - 49 edificio soho	50	50
6	SD-wan	REGIONAL SUR	IBAGUE - Kra 16 Sur No. 90 – 66 Parque Empresarial Berlín Bodegas 1 y 2	100	100
7	SD-wan	REGIONAL SUR	NEIVA / Huila Calle 29 a Sur No. 4-37 zona industrial.	30	30
8	SD-wan	REGIONAL EJE CAFETERO	CARRERA 1 Norte, número 35-11 y 35-13 La Florida, Villamaria Caldas	100	100
9	SD-wan	REGIONAL NORTE	BARRANQUILLA CTP Y ADMINISTRATIVA - LA UNION -CALLE 30 #13C-07	100	100
10	SD-wan	REGIONAL NOROCCIDENTE	RECEPCION PRINCIPAL CENTRAL DE TRATAMIENTO – MEDELLIN – Caribe CRA. 64C # 72-20	100	100
11	SD-wan	BOGOTA	SEDE PRINCIPAL BOGOTA DIAGONAL 25 G # 95 A 55	500	500
12	SD-wan	BOGOTA	SAN CAYETANO BODEGA 16 Y 17	50	50
13	SD-wan	BOGOTA	C.D MURILLO TORO – Calle 12 B # 8 A – 25	40	40
14	SD-wan	YOPAL	PO YOPAL / calle 40 No. 24 – 69	20	20
15	SD-wan	FUNZA	FUNZA / COMPLEJO INDUSTRIAL Argelia, km 3 vía Funza - Siberia, bodega 15	40	40
16	SD-wan	DATA CENTER ALTERNO	Según Diseño Técnico del oferente – RTO y RPO	500	500
SEDES SPN 4-72 (Solo Internet)					
ITEM	Tipo	REGIONAL	DIRECCIÓN	BW	Tipo
17	Internet Dedicado	BOGOTA	CL70 13 90	20	Internet
18	Internet Dedicado	VILLAVICENCIO	CL 39 32-02 CENTRO	20	Internet
19	Internet Dedicado	NEIVA	Carrera 1d bis No 15-13	20	Internet
20	Internet Dedicado	TUNJA	carrera 6 # 64-03 Barrio Asís.	20	Internet
21	Internet Dedicado	FLORENCIA	KR 12 12-57 BARRIO CENTRO	20	Internet
22	Internet Dedicado	SANTA MARTA	CO Santa Marta Crr 7 C # 29 – 06 / (5) 4358149	20	Internet
23	Internet Dedicado	CARTAGENA	DIAG.21 # 48 - 58 EL BOSQUE	20	Internet
24	Internet Dedicado	PASTO	Calle 14 12 30 bodega 1 barrio las violetas III	20	Internet
25	Internet Dedicado	POPAYAN	CL 4 5-74	20	Internet
26	Internet Dedicado	PALMIRA	CL 31 28-45	20	Internet
27	Internet Dedicado	VALLEDUPAR	CL 16A 7-44 BAARRIO CENTRO	20	Internet
28	Internet Dedicado	BUENAVENTURA	KR 5 A 1 -13	20	Internet
29	Internet Dedicado	CO.SINCELEJO	calle 38 # 7-214 Parque comercial Agrosabana	20	Internet
30	Internet Dedicado	CO.MONTERIA	Carrera 17 N° 24-09 BARRIO PASATIEMPO	20	Internet

Debe garantizar los tiempos de RTO y RPO solicitados en el capítulo del Datacenter Alterno. El oferente es responsable de definir este ancho de banda y debe cumplir los lineamientos presentados en este capítulo (Datacenter Alterno) en lo referente al acceso de aplicaciones y bases de datos.

El canal de Datos Sede Principal y Datacenter Alterno

Debe garantizar el acceso a todas las aplicaciones y bases de datos de la sede principal de SPN S.A.S cumpliendo con todas las características mencionadas en este capítulo, partiendo de una línea base de 500 Mbps.

Monitoreo Solución Conectividad General

El contratista debe garantizar el Monitoreo y gestión de la solución integral de Conectividad, la cual debe tener las siguientes características:

- Reporte Mensual vía email del desempeño hasta el CPE con las siguientes estadísticas:

- Disponibilidad
- Latencia
- Pérdida de paquetes
- Tráfico actual
- Consumo de ancho de banda mensual
- Consumo de memoria y CPU
- Monitoreo en línea, y con una vista de la herramienta para SPN S.A.S de solo lectura.
- Se debe realizar la gestión de mejora continua mensual de acuerdo con el comportamiento de la red.
- La solución debe contar con trazabilidad de actividades de la administración y gestión, y debe tener una retención de logs mínima de tres (3) meses garantizada por el oferente.

III. SOLUCION SEGURIDAD INTEGRAL

Se requiere un servicio de seguridad integral, el cual esté compuesto por las siguientes capas: Sistema de Protección Perimetral, IPS (Intrusion Prevention System), WAF, Antivirus, Contención y Mitigación de Ataques DDoS, Reportes, Correlación de Eventos de Seguridad, Análisis de vulnerabilidades y Ethical Hacking. Este servicio deberá contemplar como mínimo las siguientes características y las demás que considere el contratista para cumplir con el servicio requerido:

- La infraestructura de Seguridad Perimetral debe tener una disponibilidad 7x24x365, la cual debe ser dimensionada por el OFERENTE para soportar el internet de producción del Datacenter Principal y Datacenter Alterno.
- Se debe contar con un SOC (Security Operation Center) con una madurez mínima de 3 años; se debe adjuntar carta del representante legal, indicando la madurez del SOC del oferente. En caso de que se integre a un operador del servicio, el proponente deberá adjuntar la certificación emitida por el Representante Legal de dicho operador en la que lo autoriza a ofrecer su SOC para esta contratación.
- Las plataformas de seguridad que soportan el servicio deberán estar instaladas y configuradas de tal forma que protejan la integridad, disponibilidad y confidencialidad de la información de SPN S.A.S contenida en el Datacenter Principal y Datacenter Alterno.
- El servicio deberá estar alineado con las políticas de seguridad de la información de SPN S.A.S (basadas en la norma ISO 27001).
- El oferente deberá mantener actualizada la documentación de todas las actividades, cambios, instalaciones, configuraciones, labores de administración y gestión, desarrollados en todo el ambiente de seguridad.

SEGURIDAD PERIMETRAL NEXT GENERATION FIREWALL

Proveer un servicio de protección perimetral en alta disponibilidad en el Datacenter Principal y Alterno que será contratado, el cual debe contemplar como mínimo:

- Una plataforma Next Generation Firewall
- Funcionalidades Firewall Stateful, IPS, Antimalware, Application Control, Filtrado de Contenido, Inspección de Tráfico Cifrado, AntiSpam y cumplimiento 100% de la normativa IPv6 del Ministerio TIC.
- En el Datacenter Principal se debe garantizar que la solución sea en HA y en el Datacenter Alterno Stand alone.
- La solución debe contemplar la cobertura de los diferentes anchos de banda y la transaccionalidad de los usuarios de acuerdo con establecido en el capítulo de conectividad.
- La solución debe ser robusta y debe encontrar en el cuadrante mágico de gartner como líder vigencia 2021 o superior.

- La solución debe contar con trazabilidad de actividades de la administración y gestión, y debe tener una retención de logs mínima de tres (3) meses garantizada por el oferente.

SERVICIO DE PROTECCIÓN DE APLICACIONES WEB DATACENTER QUE SERÁ CONTRATADO

Proveer un servicio de Web Aplicación Firewall (WAF), en alta disponibilidad y de propósito específico, que brinde protección a los portales y aplicativos webs de SPN S.A.S, garantizando la protección frente ataques comunes y avanzados para protocolos HTTP/HTTPS. La plataforma debe contar con alto rendimiento para tráfico HTTP y HTTPS, el ancho de banda a soportar debe ser mínimo de 20 Mbps, así como soportar mínimo 5 IP's.

El servicio WAF debe dar protección a las aplicaciones web de SPN S.A.S contra las amenazas registradas en el OWASP Top Ten Vulnerabilities.

Las plataformas deberán ser entregadas con implementación de acuerdo con las necesidades de SPN S.A.S y soporte de fabricante durante el tiempo del contrato.

En el Data Center Principal se debe garantizar que la solución cumpla los ANS establecidos. No es obligatorio que El WAF se encuentre bajo el esquema de contingencia, es decir, será potestad del OFERENTE configurar el esquema de alta disponibilidad en el Datacenter Alterno.

SERVICIO DE ANTIVIRUS

Proveer un servicio de Antivirus enfocado a la protección de los diferentes servicios, servidores, FW, switches, equipos, aplicaciones, portales, etc. que hagan parte de la solución entregada por el oferente y de propósito específico, protegiendo así la infraestructura prestada a SPN S.A.S; garantizando los más altos estándares de seguridad y rendimiento, cumpliendo como mínimo con las siguientes especificaciones:

- Detección y Prevención de Amenazas:
 - Capacidad para detectar una amplia gama de amenazas, incluyendo virus, malware, ransomware, spyware y phishing.
 - Tecnologías de detección heurística y de comportamiento para identificar amenazas desconocidas.
 - Prevención de exploits y ataques de día cero.
- Rendimiento y Eficiencia:
 - Impacto mínimo en el rendimiento de los servidores y equipos. Debe ser capaz de ejecutarse sin causar ralentizaciones significativas.
 - Escaneos rápidos y eficientes que no afecten negativamente la productividad.
- Gestión Centralizada:
 - Plataforma de administración centralizada que permita gestionar y supervisar múltiples servidores y equipos desde un solo punto.
 - Capacidad para implementar políticas de seguridad y actualizaciones de manera remota y coherente.
- Actualizaciones Frecuentes:
 - Actualizaciones regulares de definiciones de virus y firmas para garantizar una protección actualizada contra las últimas amenazas.
 - Actualizaciones automáticas para minimizar el riesgo de exposición a vulnerabilidades conocidas.

JUSTIFICACIÓN PARA URGENCIA INMINENTE

- Compatibilidad:
 - Compatibilidad con una amplia gama de sistemas operativos y plataformas, incluyendo diferentes versiones de Windows, Linux, macOS, etc.
- Características de Seguridad Adicionales:
 - Cortafuegos integrado para bloquear el tráfico no deseado y las conexiones no autorizadas.
 - Protección de navegación web para evitar la visita a sitios web maliciosos.
 - Control de aplicaciones para limitar o bloquear la ejecución de programas no autorizados.
- Gestión de Amenazas:
 - Capacidad para cuarentenar o eliminar automáticamente archivos infectados.
 - Alertas y notificaciones claras sobre amenazas detectadas y acciones tomadas.
- Compatibilidad con Servidores:
 - Para los servidores, se debe asegurar de que el antivirus esté diseñado para proteger y funcionar de manera eficiente en entornos de servidores.
- Soporte Técnico:
 - Disponibilidad de soporte técnico con los fabricantes de software, que sea confiable y accesible para abordar problemas, incidentes o requerimientos a casos de uso de la entidad.
- Cumplimiento Normativo:
 - En caso de existir y/o aplicar, se debe verificar y garantizar que la herramienta de antivirus implementada cumpla con todos los estándares de seguridad requeridos y/o definidos por los entes de control.

La administración, gestión y soporte de la herramienta de antivirus es de total responsabilidad del oferente.

SERVICIO DE CONTENCIÓN Y MITIGACIÓN DE DDOS (ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDO) DATACENTER QUE SERÁ CONTRATADO

Prestar un servicio enfocado a proteger a SPN S.A.S de ataques del tipo DoS y DDoS, el cual apoye el aseguramiento de los canales de internet entregados por el oferente protegiendo así la infraestructura publicada por SPN S.A.S contra ataques especializados de Denegación de Servicio Distribuido volumétricos y de agotamiento de estado, el servicio debe contar con una capacidad de mitigación de mínimo 10 Gbps o superior.

- ✓ En el Datacenter Principal se debe garantizar que la solución cumpla los ANS establecidos y debe tener redundancia en el Datacenter Alternativo de acuerdo con las condiciones de este capítulo.
- ✓ **SERVICIO DE CORRELACIÓN DE EVENTOS DE SEGURIDAD INFORMÁTICA Y MONITOREO DE LA PLATAFORMA TI**

Suministrar un servicio de Correlación de Eventos de seguridad informática y monitoreo de la plataforma TI, Security Information and Event Manager (SIEM) debe permitir coleccionar, retener y correlacionar los eventos de seguridad de la infraestructura TI de SPN S.A.S, así como, monitorear la disponibilidad de los servicios, para un máximo de 1500 eventos por segundo con una retención de logs mínima de 3 meses garantizada por el oferente, para todos los activos propios de la solución suministrada por el oferente.

Se solicita Reporte mensual automático generado por la herramienta, descripción de evidencias, recomendaciones, por parte de los expertos de seguridad del oferente, para mitigación de los riesgos detectados en la correlación de eventos:

SIEM reporte y mitigación:

- Top 10 attacker host
- Top 10 attacked host
- Top 10 used ports
- Top 15 events
- Top 15 events by risk

SERVICIO DE SEGURIDAD ESPECIALIZADA

SPN S.A.S para fortalecer su estrategia de seguridad integral solicita los siguientes servicios:

- Servicio de análisis de vulnerabilidades; se realizará dos (2) veces al año para dos (2) direcciones IP o URL que SPN S.A.S designe.
- Servicio de Ethical Hacking debe ser manual sin uso de robots; se realizará dos (2) veces al año para dos (2) direcciones IP y URL, detallando en el análisis hasta 10 campos que SPN S.A.S designe.

Nota: Al finalizar el contrato, SPN S.A.S puede solicitar el borrado seguro de la data e infraestructura, garantizando la confidencialidad de la información, proceso que deberá ser garantizado a través de una herramienta específica para dicho proceso, sin costo para SPN S.A.S.

GESTIÓN DE LOGS Y REPORTES SEGURIDAD PERIMETRAL

Proveer un Servicio de Gestión de Logs y Reportes centralizado para el monitoreo de los sistemas de Seguridad Perimetral y Sistemas de Contención de los equipos ubicados en el Datacenter que será contratado con una retención mínima de tres (3) Meses garantizado por el oferente.

La prestación de servicios del presente proceso incluye los aspectos consignados en los anexos técnicos para los servicios de Datacenter, Conectividad y Seguridad. Los requisitos definidos son de obligatorio cumplimiento y corresponden a los mínimos exigidos por SPN (SERVICIOS POSTALES NACIONALES).

El objeto contractual deberá desarrollarse en Tres (3) etapas, según la siguiente descripción:

- ETAPA 1 TRANSICIÓN:** Esta etapa es el periodo de migración y aprovisionamiento de los servicios y tiene una duración comprendida de un (1) mes contado a partir de la suscripción del acta de inicio, no generará costo para SPN S.A.S. Adicionalmente los costos de adecuación, implementación, migración, instalación, etc. Tanto en las instalaciones del oferente entrante como del saliente, deberán correr por parte del contratista entrante sin costo para SPN S.A.S.

El detalle de los servicios se consigna en el **Anexo No. 01 “Especificaciones Técnicas”**. Esta etapa buscará estructurar, planificar, dimensionar, diseñar, alistar, instalar, configurar, desplegar/implementar, probar, poner en marcha y estabilizar los servicios objeto del presente proceso, así como la entrega de la ingeniería de detalle, políticas de seguridad establecidas, políticas de backups definidas, los diagramas de red e infraestructura definidos, un informe ejecutivo del plan de continuidad del negocio a nivel de data center y demás diseños y planes generados en la etapa de transición.

La etapa de TRANSICIÓN es 100% responsabilidad del OFERENTE

- II. ETAPA 2 OPERACIÓN:** Es total responsabilidad del contratista y consiste en la propia operación de los servicios objeto del presente proceso, así como del mantenimiento, tanto preventivo como correctivo. La duración de esta etapa será de dos (2) meses contados a partir de la finalización de la etapa de transición.
- III. ETAPA 3 EMPALME:** Se desarrollará durante los últimos tres (3) meses de ejecución contractual, en la cual se realizarán actividades como entrega de informes por servicio, informes financieros finales, cierre de operación de los servicios, empalme con el nuevo contratista, entrega de lecciones aprendidas, respaldos de la data, backups, la ingeniería de detalle, políticas de seguridad establecidas, políticas de backups definidas, los diagramas de red e infraestructura definidos, un informe ejecutivo del plan de continuidad del negocio a nivel de data center todo actualizado a la fecha, etc. Esta etapa se encuentra incluida en la etapa de operación.

ACUERDO DE NIVELES DE SERVICIO

Solución IaaS y SaaS (Datacenter Principal)

EL **CONTRATISTA** aceptará los siguientes ANS por aplicación y las sanciones por incumplimiento de los tiempos:

DISPONIBILIDAD DE SERVICIOS A: 99,93%			COMPENSACIÓN MENSUAL
	Desde	Hasta	Porcentaje de descuento sobre la facturación de los servicios específicos
	-	100%	
Mayor o igual al 99,93%	100%	99,930%	0%
Mayor o igual al 99,860% y menor al 99,930%	99,929%	99,860%	5%
Mayor o igual al 99,790% y menor al 99,859%	99,859%	99,790%	10%


Solución Conectividad SD-WAN

El nivel mínimo solicitado de disponibilidad de los canales de internet dedicado y MPLS es de 99.93 %

Rango de % de Indisponibilidad mes		Penalización sobre tarifa mensual
100,0	99,93	0%
99,93	99,8	5%
99,8	99	10%
99	90	30%
90	0	100%

Solución Conectividad solo Internet Dedicado

El nivel mínimo solicitado de disponibilidad de los canales de internet dedicado y MPLS es de 99.70 %

	JUSTIFICACIÓN PARA URGENCIA INMINENTE
---	--

Rango de % de Indisponibilidad mes		Penalización sobre tarifa mensual
100,0	99,70	0%
99,69	99	5%
98,99	90	10%
89,99	80	30%
79,99	0	100%

Solución Backup's

El OFERENTE debe garantizar que la integridad del 100% de los datos respaldados, según las políticas definidas por SPN S.A.S. En caso de que SPN S.A.S requiera entregar, restaurar, validar y/o corroborar información contenida en los respaldos y se presenten fallas de disponibilidad de los datos por parte del OFERENTE, se aplicara un ANS correspondiente al 10% de descuento sobre la tarifa mensual del servicio específico para el mes en el que se realice la solicitud; no se podrán aplicar dos ANS en meses diferentes para una misma solicitud.

Solución Servicios Administrados


En caso de que se presenten incidentes y/o fallas asociadas a monitoreo, gestión y administración de los servicios entregados por el OFERENTE; se aplicara un ANS correspondiente al 20% de descuento sobre la tarifa mensual del servicio específico.

Tiempos de Atención Solución General

El Contratista deberá cumplir con los siguientes tiempos de atención para cada uno de los servicios

Tiempos de atención de incidentes de Conectividad

Urgencia	Impacto	Prioridad	Descripción	Tiempo de Atención y Solución
Baja	Bajo	Baja	Se entiende como la que no afecta ni degrada la prestación del servicio. Latencia según producto.	4 horas
Media	Bajo	Media	Servicio restringido; servicio por ruta alterna de inferior velocidad; lentitud en el servicio debido a errores en los enlaces, a retransmisiones ó pérdidas de paquetes; presencia de fallas presentadas esporádicamente y que pueden causar interrupción en el servicio por periodos de tiempo cortos. El tiempo de duración de las fallas de operación degradada formará parte de la indisponibilidad, siempre y cuando sea medible y mayor a 10 segundos. Latencia según producto.	2 horas
Alta	Bajo			
Baja	Medio			
Media	Medio	Alta	Se entiende que la comunicación entre los 2 puntos de un enlace se ha interrumpido totalmente.	1 hora
Alta	Medio			

	JUSTIFICACIÓN PARA URGENCIA INMINENTE
---	--

Tiempos de atención incidentes Solución IaaS y SaaS

Urgencia	Impacto	Prioridad	Descripción	Tiempo de Atención y Solución
Baja	Bajo	Baja	Se entiende como la que no afecta ni degrada la prestación del servicio.	4 horas
Media	Bajo	Media	Servicio restringido o parcial; lentitud o intermitencia en el servicio, presencia de fallas presentadas esporádicamente y que pueden causar interrupción en el servicio por periodos de tiempo cortos. El tiempo de duración de las fallas de operación degradada formará parte de la indisponibilidad, siempre y cuando sea medible.	2 horas
Alta	Bajo			
Baja	Medio			
Media	Medio	Alta	Operación interrumpida totalmente.	1 hora
Alta	Medio			

3. REQUISITOS AMBIENTALES Y DE SEGURIDAD Y SALUD EN EL TRABAJO

FICHA 25. CRITERIOS PARA SERVICIOS CLOUD	
Proceso Responsable de la Contratación	Infraestructura Tecnológica
REQUISITOS CONTROL Y SEGURIDAD (BASC y S58)	
ETAPA PRECONTRACTUAL	
<ul style="list-style-type: none"> El oferente deberá certificar mediante oficio que cumple con todos los requisitos establecidos en la etapa contractual y que permitirá que 4-72 los solicite en cualquier momento durante la ejecución del contrato. 	
ETAPA CONTRACTUAL (EJECUCIÓN DE CONTRATO)	
<ul style="list-style-type: none"> Cumplir con lo establecido en la documentación existente del subproceso Infraestructura Tecnológica de Servicios Postales Nacionales S.A.S. Suministrar la documentación necesaria que evidencie el cumplimiento de los requisitos legales aplicables. Deberá asegurar que la información documentada generada, sea legible, completa, precisa, exacta y protegida contra modificaciones, pérdida o introducción de datos erróneos. Garantizar la protección de los sistemas de las tecnologías de la información utilizados para los servicios contratados, aplicando los controles de seguridad y ciberseguridad definidos en el alcance al cumplimiento de las normas de seguridad de la información y ciberseguridad de SPN. Contar con una política de confidencialidad, que permita salvaguardar y proteger la información, su confidencialidad y manejo, integridad y disponibilidad, en sus diferentes formas y estados. Garantizar que los servicios contratados cuenten con las medidas de seguridad necesarias para impedir que terceros accedan a la información. 	
REQUISITOS SST	
ETAPA PRECONTRACTUAL (REQUISITOS HABILITANTES)	

- Establecer e implementar un Sistema de Gestión de Seguridad y Salud en el Trabajo para sus empleados. El SG-SST debe cumplir lo que indica la Decreto 1072 de 2015 en su Capítulo VI y la Resolución 0312 de 2019.
- Presentar certificado de la evaluación no superior a 12 meses de los estándares mínimos SST según la resolución 0312 del 2019 acreditada o certificada por la ARL vigente, teniendo en cuenta lo siguiente:
 - Calificación entre 60 y 85% con plan de mejoramiento.
 - calificación >85% no requiere plan de mejora.
- La empresa contratista y/o subcontratista debe suministrar los datos de contacto de la persona encargada del Sistema de Gestión de la Seguridad y Salud en el Trabajo de acuerdo con lo siguiente:
 - Nombre de encargado seguridad y salud en el trabajo (SST)
 - Documento de identificación
 - Licencia de seguridad y salud en el trabajo (SST) y/o Curso de 50 horas del SG-SST

ETAPA CONTRACTUAL (EJECUCION DEL CONTRATO)

- El contratista y/o subcontratista debe entregar al Supervisor del contrato y al área de Seguridad y Salud en el Trabajo las planillas de pago correspondientes a ARL, EPS y AFP vigentes. Esta se deberá presentar mensualmente o con mínimo un día hábil antes de ejecutar la actividad (para actividades ocasionales).

Nota: La planilla deberá ser pagada directamente por el titular del contrato y no por terceros.

- Antes de iniciar las actividades a ejecutar en las instalaciones de la organización, los contratistas y/o subcontratistas deben recibir inducción en SST.
- Deberá garantizar la integridad física y/o seguridad de su personal, equipos propios o de la empresa, al igual que el control estricto del cumplimiento de las normas establecidas en este documento.
- El contratista deberá asegurar la entrega y el uso de los EPP de todos sus trabajadores durante la ejecución de la actividad contratada.
- El Contratista debe reportar inmediatamente al área SST de SERVICIOS POSTALES NACIONALES S.A.S. los accidentes e incidente generados durante el periodo de vigencia del contrato.
- El Contratista deberá atender las revisiones internas realizadas por SERVICIOS POSTALES NACIONALES S.A.S. y la disponibilidad de personal y recursos para el desarrollo de esta, el representante legal del Contratista debe participar en las reuniones de apertura y cierre del proceso de revisión interna en caso de ser citado.

Nota 1: Si el Contratista subcontrata todo o parte del trabajo contratado, los requerimientos de este documento se aplicarán también a los subcontratistas.

JUSTIFICACIÓN PARA URGENCIA INMINENTE

- Acatar las modificaciones o sugerencias de seguridad dadas por el Supervisor, líder de proceso contratación y/o Líder SST a los procedimientos o las actividades que adelante, cuando existan condiciones inseguras para el personal contratista, subcontratistas y para los colaboradores de SERVICIOS POSTALES NACIONALES S.A.S.
- Nota 2: en caso de que el soporte se preste de manera remota, aplicará solamente los requisitos indicados en la etapa precontractual.

4. Código de Naciones Unidas (UNSPSC).

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE
81112000	Servicios Basados en Ingeniería y tecnología	Servicios Informáticos	Servicios de datos
81112100	Servicios Basados en Ingeniería y tecnología	Servicios Informáticos	Servicios de Internet
81161700	Servicios Basados en Ingeniería y tecnología	Servicios Informáticos	Servicios de Telecomunicaciones

5. OBJETO PARA CONTRATAR O BIEN A CONTRATAR

Prestación de un servicio global de Data Center, hosting, nube, telecomunicaciones, conectividad, seguridad y demás servicios TI; a través de un aliado estratégico que brinde a la entidad un servicio integral y de alta disponibilidad de manera centralizada que permita la operación a nivel nacional de las diferentes sedes y aplicaciones que maneja la entidad.

6. AUTORIZACIONES, PERMISOS Y LICENCIAS NECESARIAS PARA LA CONTRATACIÓN.

El contratista deberá proveer un servicio de Datacenter principal, con el fin de prestar el servicio integral solicitado, cumpliendo con los ANS solicitados, los requerimientos generales para el Datacenter Principal son las siguientes

- EL CONTRATISTA debe demostrar que su Datacenter principal cuenta mínimo con el nivel de certificación TIER IV de diseño y construcción (emitida por el Uptime Institute) o ICREA nivel V (emitida por el International Computer Room Experts Association - ICREA). La certificación debe estar vigente.
- La solución ofertada debe estar alojada en un Datacenter alternativo que cumpla mínimo las características TIER II o ICREA Nivel III, para lo cual presentará carta de cumplimiento firmada por el representante legal o la respectiva certificación (Uptime Institute o ICREA).
- Certificación NAP Colombia.
- Certificación NAP Américas.
- Certificación ISO 27001

- Certificación ISO 90001
- Constancia ISAE 3402 correspondiente al último año fiscal.
- Certificado de eficiencia energética CEEDA
- Certificación ISO 20000 Servicios de Hosting y Seguridad

7. FUNDAMENTO JURÍDICO QUE SOPORTA LA MODALIDAD DE SELECCIÓN

Modalidad de contratación: De acuerdo con el Manual de Contratación de Servicios Postales Nacionales S.A.S., la modalidad de selección aplicable al presente proceso es la de contratación directa, a través de urgencia inminente, teniendo en cuenta que:

- a. Exista una necesidad inminente certificada por el jefe de área requirente del servicio y el ordenador del gasto respectivo y siempre que la misma no se deba a falta de planeación de la adquisición del bien o servicio.
- b. Exista riesgo de afectar la continua y eficiente prestación de los servicios a cargo de la empresa.
- c. Exista riesgo de afectar los compromisos u obligaciones existentes.

Dichos contratos se celebrarán bajo las siguientes reglas:

- Se podrá adelantar por una sola vez para el respectivo objeto contractual y cuando su tiempo de ejecución no sea mayor a tres (3) meses calendario.
- Para esta causal se prescindirá del estudio previo y solo justificará la procedencia de la misma mediante documento escrito, suscrito por el vicepresidente o jefe del área requirente y el ordenador del gasto.
- Deberá ser aprobada previamente por el Comité de Contratación y Compras. Podrá utilizarse para la escogencia del contratista, el registro de proveedores de que trata el presente manual.

Tipología del contrato:

8. VALOR ESTIMADO DEL CONTRATO

El presupuesto establecido para la presente contratación es por la suma de **HASTA MIL TREINTA Y SEIS MILLONES NOVECIENTOS DOS MIL SETECIENTOS DIECISIETE PESOS (\$1.036.902.717)** incluido costos directos e indirectos a que haya lugar.

9. DOCUMENTOS JURÍDICOS Y TÉCNICOS

9.1 REQUISITOS HABILITANTES

- **Carta de presentación y compromiso**, firmada por el representante legal

La carta de presentación y compromiso debe ser firmada por el representante legal de la persona jurídica, o por el representante del Consorcio o Unión Temporal conformado, según sea el caso. La cual deberá ser diligenciado de manera obligatoria o apoderado debidamente constituido, evento en el cual se debe anexar el poder autenticado donde se especifique si se otorga poder para presentar la oferta, o para presentar ésta, participar en todo el proceso de selección y suscribir el contrato en caso de resultar seleccionado.

- **Certificado de Existencia y Representación Legal del Proponente**

Las personas jurídicas nacionales o extranjeras con domicilio en Colombia, que presenten propuesta para participar en el presente proceso de selección, deberán acreditar su existencia, capacidad y representación legal mediante el Certificado de Existencia y Representación Legal expedido por la Cámara de Comercio de la ciudad donde se encuentre su domicilio o sucursal, que deberá haber sido emitido con una antelación máxima de treinta (30) días calendario a la fecha del cierre del presente proceso.

El objeto social del oferente deberá tener relación con el objeto del presente proceso de contratación.

Se debe acreditar la vigencia de la persona jurídica, la cual debe ser mínimo por el plazo de ejecución del contrato y tres (3) años más y haberse constituido como mínimo un (1) año antes del cierre del proceso.

Cuando el representante legal del oferente se encuentre limitado en sus facultades para presentar la propuesta y suscribir el contrato que resulte del presente proceso, se deberá anexar a la oferta, copia del documento en el cual conste la decisión del órgano social correspondiente que lo autoriza para la presentación de la propuesta y la suscripción del contrato.

Cuando en los documentos aportados que acreditan la existencia y representación legal de la persona jurídica extranjera no cuente con toda la información requerida, podrán adjuntar una certificación del representante legal de la sociedad extranjera con los datos que faltan, la cual se entiende formulada bajo la gravedad de juramento.

Siempre deberán cumplirse todos y cada uno de los requisitos legales relacionados con la consularización o apostille y traducidos al idioma español, exigidos para la validez y oponibilidad en Colombia de documentos expedidos en el exterior y que puedan obrar como prueba, conforme a lo dispuesto en el artículo 480 del Código de Comercio de la República de Colombia.

En el evento de la legalización de documentos emanados de autoridades de países integrantes del Convenio de la Haya de 1961, se requerirá únicamente la Apostilla como mecanismo de legalización, de conformidad con lo señalado en la Ley 455 de 1998.

Para el caso de las personas jurídicas sin ánimo de lucro pertenecientes al sector solidario, además de los documentos señalados en el presente numeral y el certificado de paz y salvo de tasas y contribución de multas expedido por la Superintendencia de la Economía Solidaria que deberá ser emitido con una antelación máxima de treinta (30) días calendario a la fecha del cierre del presente proceso.

- **Fotocopia de cédula del representante legal.**
- **Declaración de Origen de Fondos. (ANEXO No. 4)**
- **Cuenta bancaria.** Certificación de cuenta bancaria no mayor a noventa (90) días a la fecha del cierre del presente proceso, en el cual conste que el oferente sea el titular de la misma.
- **Certificado de Antecedentes Judiciales, Fiscales, Disciplinarios y Correctivas del Representante Legal, de la Persona Jurídica y del Revisor Fiscal (si aplica)**

Copia del Registro Único Tributario RUT. Las personas jurídicas proponentes o miembros de un consorcio o unión temporal deberán adjuntar a su propuesta fotocopia del Registro Único Tributario, de conformidad con lo señalado en el Decreto 788 de 2002.

Así mismo, el proponente debe tener la inscripción en el RUP en alguno de los siguientes códigos de las UNSPSC:

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE
81112000	Servicios Basados en Ingeniería y tecnología	Servicios Informáticos	Servicios de datos
81112100	Servicios Basados en Ingeniería y tecnología	Servicios Informáticos	Servicios de Internet
81161700	Servicios Basados en Ingeniería y tecnología	Servicios Informáticos	Servicios de Telecomunicaciones

Si se trata de consorcios, uniones temporales o promesa de sociedad futura, el proponente plural deberá acreditar en conjunto la totalidad de los códigos solicitados por la entidad en el presente documento y sus integrantes deberán estar inscritos en los códigos anteriormente citados.

El Registro Único de Proponentes será el documento, junto con los demás exigidos, sobre los cuales se verificarán los requisitos de orden jurídicos y técnicos relacionados con la capacidad y experiencia del proponente.

- **Certificación de Parafiscales.**

De conformidad con lo estipulado por el artículo 50 de la Ley 789 de 2002 y la Ley 828 de 2003, el proponente deberá anexar la respectiva certificación en la cual se indique que se encuentra cumpliendo y/o a paz y salvo en el pago de las contribuciones al Sistema Integral de Seguridad Social –EPS, Pensiones y ARP-, así como de los Aportes Parafiscales –SENA, ICBF, Cajas de Compensación Familiar-, y Subsidio Familiar a que haya lugar, de sus empleados a la fecha de cierre y en los 6 meses anteriores a la misma.

La certificación deberá ser suscrita por el Revisor Fiscal cuando éste exista de acuerdo con los requerimientos de ley o por el representante legal, y en este deberá constar que se encuentra al día

en dichos pagos en los seis (6) meses anteriores en un término de expedición no superior a treinta días de la fecha de presentación de la propuesta.

Cada una de las personas jurídicas, miembros de un Consorcio o Unión Temporal en forma independiente, deberán anexar esta certificación.

El oferente deberá adjuntar la planilla única de pago del último mes, se aclara que dicha nota es condicional y el aporte de la planilla aplica para aquellos que no estén obligados a tener revisoría fiscal. A la documentación deberá anexarse copia de la tarjeta profesional, copia de la cédula de ciudadanía y el Certificado de Antecedentes Disciplinarios del Revisor fiscal con expedición no mayor a tres (3) meses a la fecha de cierre de presentación de la propuesta.

- **Consorcios y/o Uniones Temporales**

En el evento de participación conjunta, el Consorcio o Unión Temporal debe conformarse de acuerdo con lo establecido en el artículo 7 de la Ley 80 de 1993 y/o sus decretos reglamentarios, lo cual acreditarán con el documento de constitución que contendrá como mínimo:

- Expresar si la participación es a título de Consorcio o Unión Temporal.
- La identificación clara y detallada de cada uno de sus integrantes o miembros.
- La designación de la persona que para todos los efectos legales tendrá la representación legal del Consorcio o la Unión Temporal, quien será el único canal de comunicación con SPN. Cualquier modificación en este sentido, deberá ser notificada por escrito a SPN.
- Las reglas básicas que regulen las relaciones de sus integrantes y su responsabilidad.
- Indicar la duración del Consorcio o de la Unión Temporal, que deberá ser como mínimo por el lapso comprendido entre el cierre de la Licitación y la liquidación del contrato, y dos años más.
- En el evento de conformarse Unión Temporal o Consorcio, además deberá indicar, los términos y extensión de la participación en la propuesta y en la ejecución del contrato, el porcentaje de participación de cada miembro del proponente plural, los cuales no podrán ser modificados sin el consentimiento previo y escrito de SPN.

- **Certificación de Composición de Socios o Accionistas.**

El proponente deberá allegar un certificado suscrito por el representante legal en el que se relacione los socios y o accionistas o asociados que tengan directa o indirectamente en el capital social, aporte o participación. La certificación debe tener fecha de expedición no superior a treinta días del cierre del presente proceso. De cada accionista se debe incluir: Nombre o razón social, identificación y porcentaje de participación.

Como anexo a la certificación el proponente deberá allegar el número o números de acta donde estén registrados los socios de la persona jurídica ante la Cámara de Comercio. La Entidad se reserva el derecho de realizar las verificaciones correspondientes.

Si la verificación da como resultado **NO CUMPLE**, la propuesta no quedará habilitada.

9.2 REQUISITOS HABILITANTES TÉCNICOS

El Representante Legal deberá presentar carta de compromiso donde manifiesta que cumplirá con todas y cada una de las especificaciones técnicas mencionadas en el subtítulo “**ESPECIFICACIONES TÉCNICAS, CANTIDADES, CALIDADES DEL BIEN Y/O SERVICIO**” del estudio previo.

9.2.1 EXPERIENCIA


Para efectos de acreditar la experiencia el proponente deberá presentar hasta tres (3) certificaciones contratos desarrollados en Colombia, ejecutados a la fecha de cierre de la presente del proceso El objeto de cada contrato deberá guardar relación directa con el objeto contractual.

Las certificaciones y/o documentación del contrato a suscribir, deberán contener como mínimo la siguiente información:

- ✓ Nombre del contratista: Debe indicarse claramente el nombre, así como la información básica de la persona natural o jurídica que desarrolló o ejecutó el contrato.
- ✓ Nombre de la entidad contratante: Debe indicarse claramente el nombre de la entidad contratante. De igual forma la documentación allegada debe venir suscrita por quien tenga la facultad para la misma.
- ✓ Objeto: debe cumplir las características mencionadas anteriormente.
- ✓ Lugar o lugares de ejecución
- ✓ Valor del Contrato: Se debe especificar el valor del contrato, incluido IVA y demás impuestos y costos a que haya lugar.
- ✓ Término de duración del contrato: debe quedar clara la fecha de inicio y terminación y ejecución del contrato ejecutado. No se aceptan contratos en ejecución.
- ✓ Recibo a satisfacción, certificación de desempeño y/o satisfacción, liquidación y/o paz y salvo: en la certificación y/o contrato ejecutado la entidad contratante debe dejar claro que el contrato terminado y/o liquidado fue recibido a satisfacción en su totalidad y que la ejecución se realizó de manera satisfactoria.

Registro TIC

- ✓ Conforme a lo establecido por el artículo 10 de la Ley 1341 de 2009, el Registro de TIC expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones, es obligatorio para todos los proveedores de redes y servicios de Telecomunicaciones; por lo tanto, los oferentes individuales y todos los integrantes del oferente plural que sean proveedores de redes y telecomunicaciones deberán anexar dicho documento vigente dentro de la propuesta.

	JUSTIFICACIÓN PARA URGENCIA INMINENTE
---	--

10. TÉRMINO DE EJECUCIÓN

El plazo de ejecución del contrato será de **TRES (3) MESES** contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución, aprobación de las pólizas solicitadas y suscripción de acta de inicio.

11. LUGAR DE EJECUCIÓN

En todo el territorio nacional.

12. ANÁLISIS DE RIESGOS


ANÁLISIS PRELIMINAR DE RIESGOS													
CLASE DE RIESGO	N o.	IDENTIFICACIÓN DEL RIESGO	MEDICION ANTES DE CTROL			CONTROL (PREVENTIVO)	MEDICION DESPUES DE CTROL			TRATAMIENTO (CORRECTIVO)	¿A QUIÉN SE LE ASIGNA?		
			ALT O	MEDI O	BAJ O		ALT O	MEDI O	BAJ O		SERVICIOS POSTALES NACIONALES	PROPO NENTE Y/O CONTRATISTA	COMPANIA ASEGURADORA Y/O GARANTIA
ADMINISTRATIVO	1	Desistimiento de la oferta o no firma el contrato		X		* Analizar la viabilidad de solicitar póliza de seriedad/Invitación formal basado en fuentes confiables de proveedores		X		* Afectar la póliza de seriedad * Iniciar proceso litigioso		X	X
	2	Declaratoria Desierta del proceso		X		* Definir las condiciones mínimas a exigir conforme a la realidad del mercado y del sector (Indicadores financieros, capacidad jurídica y requisitos técnicos)		X		* Revisión y modificación de los aspectos (Financieros, jurídicos, técnicos y económicos) que llevaron a la declaratoria de desierto, para la futura invitación.	X		
	3	Sobrevaloración o subestimación de los precios propuestos por el contratista		X		* Analizar la viabilidad de solicitar póliza de seriedad. * Adelantar un adecuado estudio de mercado y del sector * Señalar en los términos de invitación como causal de rechazo			X	* Afectar la póliza de seriedad * Rechazar la oferta con precios artificiales		X	X
	4	Incumplimiento de obligaciones del marco contractual y disposiciones de la propuesta		X		*Adecuada supervisión del contrato con verificaciones periódicas. * Estipular cláusulas de descuentos por incumplimiento * Solicitud de pólizas de garantías		X		* Afectar las pólizas de garantías * Aplicar los descuentos por incumplimientos pactados	X	X	X

JUSTIFICACIÓN PARA URGENCIA INMINENTE

ANÁLISIS PRELIMINAR DE RIESGOS													
CLASE DE RIESGO	N o.	IDENTIFICACIÓN DEL RIESGO	MEDICION ANTES DE CTROL			CONTROL (PREVENTIVO)	MEDICION DESPUES DE CTROL			TRATAMIENTO (CORRECTIVO)	¿A QUIÉN SE LE ASIGNA?		
			ALT O	MEDI O	BAJ O		ALT O	MEDI O	BAJ O		SERVIC IOS POSTA LES NACIONALES	PROPO NENTE Y/O CONTR ATISTA	COMPAN IA ASEGUR ADORA Y/O GARANTI A
JURÍDICO S – LEGALES	5	Pérdida de capacidad jurídica para la ejecución del contrato (personas naturales y jurídicas, fallecimiento, detención, extinción y liquidación de la persona jurídica, etc.)		X		* Incluir en la invitación formal disposiciones que permitan adjudicar al contrato al segundo evaluado. * Invitación formal basado en fuentes confiables de proveedores/consulta de listas restrictivas y publicación en página web y Secop II * Indicadores Financieros		X		* Aplicar las cláusulas al segundo mejor calificado. * Suspensión, terminación o cesión del contrato.	X	X	
FINANCIE ROS	6	Insolvencia del Contratista por indebida estipulación de indicadores financieros o por aporte de información inexacta.	X			* Incluir en la invitación formal disposiciones que permitan adjudicar al contrato al segundo evaluado. * Invitación formal basado en fuentes confiables de proveedores/consulta de listas restrictivas. * Indicadores Financieros conforme a la realidad del mercado y del sector.		X		* Aplicar las cláusulas al segundo mejor calificado. * Suspensión, terminación o cesión del contrato. * Actualización y revisión periódica de los estudios que dan lugar a estipular los indicadores financieros y apoyo en documentos de consulta de CCE. * Dar traslado a las autoridades administrativas y/o judiciales competentes. * Eliminar al proveedor respectivo del directorio de la Entidad.		X	X
ECONÓMI CO	7	La fluctuación negativa de la moneda (TRM) o fenómenos inflacionarios.		X		* Contar con inversiones a corto plazo. * Realizar un estudio técnico y económico del impacto del riesgo en la ecuación del contrato que permita definir las medidas pertinentes (adición, suspensión, prórrogas, terminación del contrato, cesión del contrato.)			X	* Recurrir a la venta de la inversión o reestructuración del contrato que garantice su viabilidad	X	X	
	8	Cambios en la normatividad legal vigente que		X		* Contar con inversiones a corto plazo.			X	* Recurrir a la venta de la inversión o	X		

JUSTIFICACIÓN PARA URGENCIA INMINENTE

ANÁLISIS PRELIMINAR DE RIESGOS													
CLASE DE RIESGO	N o.	IDENTIFICACIÓN DEL RIESGO	MEDICION ANTES DE CTROL			CONTROL (PREVENTIVO)	MEDICION DESPUES DE CTROL			TRATAMIENTO (CORRECTIVO)	¿A QUIÉN SE LE ASIGNA?		
			ALT O	MEDI O	BAJ O		ALT O	MEDI O	BAJ O		SERVIC IOS POSTA LES NACIO NALES	PROPO NENTE Y/O CONTR ATISTA	COMPAN IA ASEGUR ADORA Y/O GARANT IA
		genere una mayor carga impositiva				* Realizar un estudio técnico y económico del impacto del riesgo en la ecuación del contrato que permita definir las medidas pertinentes (adición, suspensión, prórrogas, terminación del contrato, cesión del contrato.)				reestructuración del contrato que garantice su viabilidad			
TÉCNICOS	9	Incumplimiento de la cobertura de Garantías por defectos de fábrica o mantenimiento propios del bien o servicio adquirido.		X		* Darle el adecuado uso de los bienes allegados y cumplir con las recomendaciones del manual de usuario (mantenimientos preventivos y correctivos). * Estipular tanto en los términos de la invitación como en los contratos el otorgamiento de las garantías propias del bien o servicio adquirido.			X	* Aplicar las cláusulas del incumpliendo pactadas en el contrato. * Iniciar el procedimiento administrativo ante el órgano de vigilancia y control competente en el marco del estatuto general del consumidor.		X	X
	10	Obsolescencia en el mercado o programada de los bienes y/o servicios adquiridos			X	* Mantener una eficaz comunicación entre el supervisor, el proveedor y fabricante. * Estipular cláusulas contractuales que contemple la viabilidad del reemplazo de los bienes o servicios por iguales o mejores características técnicas.			X	* Afectar las pólizas de garantías otorgadas. * Contar con disponibilidad presupuestal para los imprevistos del contrato.	X	X	X
FUERZA MAYOR	11	Circunstancias de fuerza mayor, caso fortuito o imprevisibles que lleven a la paralización del contrato	X			* Contar con una adecuada planeación de las necesidades a satisfacer (mantener un stock mínimo de insumos requeridos). * Herramientas tecnológicas que permitan mantener.		X		* Suspensión, terminación o cesión del contrato. * Restauración de Back up	X	X	X

	JUSTIFICACIÓN PARA URGENCIA INMINENTE
---	--

ANÁLISIS PRELIMINAR DE RIESGOS													
CLASE DE RIESGO	N o.	IDENTIFICACIÓN DEL RIESGO	MEDICION ANTES DE CTROL			CONTROL (PREVENTIVO)	MEDICION DESPUES DE CTROL			TRATAMIENTO (CORRECTIVO)	¿A QUIÉN SE LE ASIGNA?		
			ALT O	MEDI O	BAJ O		ALT O	MEDI O	BAJ O		SERVIC IOS POSTA LES NACIO NALES	PROPO NENTE Y/O CONTR ATISTA	COMPAN IA ASEGUR ADORA Y/O GARANTI A
						conservar y/o recuperar la información.							

13. ESTUDIO DE MERCADO Y ANÁLISIS DEL SECTOR

El presente estudio de mercado fue realizado de conformidad al Manual de Contratación vigente de Servicios Postales Nacionales S.A.S; para lo cual se recibieron dos (2) cotizaciones por ende se realizó el estudio comparativo de las ofertas con las cotizaciones allegadas de acuerdo con la necesidad de la empresa.

Descripción	Unidad de Medida	Cantidad	UNE EPM TELECOMUNICACIONES S.A.		COMUNICACIÓN CELULAR S.A. COMCEL S.A.	
			Valor Unitario	Valor Total	Valor Unitario	Valor Total
Servicio de Datacenter	Mes	3	\$401.203.333	\$1.203.609.999	\$272.032.409	\$816.097.227
Servicio de Conectividad	Mes	3	\$278.994.444	\$836.983.332	\$46.880.146	\$140.640.438
Servicio de Seguridad	Mes	3	\$101.546.667	\$304.640.001	\$-	\$-
SUBTOTAL				\$2.345.233.332		956.737.665
IVA			216.908.433	650.725.299	26.721.684	80.165.052
TOTAL				2.995.958.631		\$1.036.902.717

Nota: El oferente **COMUNICACIÓN CELULAR COMCEL S.A.**, presento una oferta correspondiente al objeto contractual.

Nota: en vista de lo anterior el oferente **COMUNICACIÓN CELULAR COMCEL S.A** cumple con las especificaciones técnicas y económicas requeridas y en razón a su oferta se evidencia el precio más bajo para la empresa lo cual se procederá a realizar la solicitud de disponibilidad presupuestal

Teniendo en cuenta que En este momento se viene ejecutando el contrato número 130 – 2020 cuyo objeto es Prestación de servicio de conectividad como solución integral de alta disponibilidad y el alojamiento en modalidad de nube privada, hosting físico y/o hosting virtual, centralizado en un centro

de datos que permita la operación a nivel nacional de las aplicaciones que maneja la entidad. este contrato finaliza su plazo de ejecución el día treinta (30) de septiembre 2023, y en aras de garantizar eficiencia, gestión, administración, monitoreo, disponibilidad y eficacia en la utilización de los recursos tecnológicos y financieros para la operación de la plataforma tecnológica, SPN S.A.S

Motivo por el cual se requiere llevar a cabo el proceso de selección del contratista, sin solución de continuidad de todos los servicios tecnológicos con las mismas condiciones técnicas que comprenden la prestación de servicios IT en tres grandes grupos así: Datacenter, Conectividad y Seguridad; para la interconexión de las sedes de SPN S.A.S, y el alojamiento de las aplicaciones que actualmente son de vital funcionalidad para SPN S.A.S.

Pertinente se indicar que la empresa se encuentra en proceso de austeridad del gastos y minimización de recursos relacionados con prestaciones de servicios a nivel general es por ello que se realiza el comparativo en líneas atrás citado con el fin de verificar el costo y beneficio del proceso contractual cuyos valores se encuentran asociados al servicio de conectividad, datacenter es por ello que SPN S.A.S requiere continuar con el alojamiento en modalidad de nube privada, hosting físico y/o hosting virtual, centralizado en un datacenter que permita la operación a nivel nacional de:

Sipost (Producción, Certificación Contingencia) **Seven** (Producción, pruebas, contingencia) **Kactus** (Producción, Pruebas, Contingencia) **IFS** (Producción, Pruebas Contingencia) **ERP BI** (Dominio, producción, contingencia) **IPS** (Producción, contingencia) **PQR** (Producción, Pruebas Contingencia) CEC. Entre otras.

Nota: Para el alojamiento de las aplicaciones anteriormente mencionadas es necesario contar con la disponibilidad de los recursos mencionados en el **Anexo No. 01 “Especificaciones Técnicas”**.

En virtud de lo anterior, se arroga como resultado que los valores de un inicio proceso Vrs la permanencia del proveedor actual quien mantiene los mismo valores y condiciones bajo esta premisa se anexa las cotizaciones realizadas en el citado proceso.

14. GARANTÍAS

De conformidad con el Manual de Contratación de la Entidad, para efectos de la expedición de garantías serán admisibles uno de los siguientes tipos de garantías:

- **Póliza de seguro** expedida a favor de entidades públicas con régimen privado de contratación que identifique como único beneficiario a Servicios Postales Nacionales S.A.S.
- **Garantías bancarias**, para tal efecto deberá allegar constancia emitida por una entidad bancaria autorizada por la Superfinanciera que ampare las vigencias y el valor asegura según lo exigido para el presente proceso, para la cual en dicho documento se deberá identificar el objeto, la vigencia, el amparo, el valor asegurado y el número del contrato.
- **Fiducia mercantil en garantías**, para tal efecto deberá allegar constancia emitida por una entidad autorizada por la Superfinanciera que ampare las vigencias y el valor asegura según lo exigido para el presente proceso, para la cual en dicho documento se deberá identificar el objeto, la vigencia, el amparo, el valor asegurado y el número del contrato.

El proponente adjudicatario se encuentra en la obligación de suscribir el contrato dentro del plazo establecido en el cronograma del proceso, en dicho evento procederá la aplicación de lo establecido en el capítulo 38 listas de elegibilidad.

El contratista dentro de los **tres (3) días hábiles siguientes** a la suscripción del contrato deberá expedir el amparo contractual teniendo en cuenta los amparos y su cobertura que se indican a continuación:

1. **Cumplimiento**, en cuantía equivalente al veinte (20%) del valor del contrato con una vigencia igual a la de este y seis (6) meses más contados a partir de la fecha de suscripción del contrato.
2. **Calidad del servicio**, en cuantía equivalente al veinte (20%) del valor del contrato con una vigencia igual a la de este y seis (6) meses más contados a partir de la fecha de suscripción del contrato
3. **Salarios, Prestaciones Sociales e Indemnizaciones Laborales**: en cuantía equivalente al cinco (5%) del valor del contrato con una vigencia igual a la de este y tres (3) años más, contados a partir de la suscripción del contrato.
4. **Responsabilidad Civil Extracontractual**, en cuantía equivalente al veinte (20%) del valor del contrato con una vigencia igual a la de este: en la cual cuente con los siguientes amparos como mínimo: daños patrimoniales y extrapatrimoniales sin sub límites, responsabilidad civil patronal sin sub límites, vehículos propios y no propios sin sublímites.

Parágrafo primero: Si EL CONTRATISTA se negare a prorrogar las garantías o a reponer el valor cuando este sea afectado, SPN dará por terminado el contrato en el estado en que se encuentre, sin que por este hecho deba reconocer el pago de suma alguna en favor del CONTRATISTA.

Parágrafo segundo: En todo caso las garantías se mantendrán vigentes hasta la liquidación del contrato, ajustándose a los límites, existencia, y extensión del riesgo amparado.

Parágrafo tercero: La reposición del valor asegurado no disminuirá por cada evento que reclame Servicios Postales Nacionales S.A.S.

Parágrafo cuarto: La constitución de la presente póliza no exime de responsabilidad al contratista de las pérdidas, averías, expoliciones o detrimento patrimonial derivado de las actuaciones de sus trabajadores.

Parágrafo quinto: Para todas y cada una de las garantías requeridas, el oferente deberá adjuntar a la misma el recibo original donde conste el pago de la prima. No es válido que se certifique que las pólizas no vencerán por falta de pago, porque contraviene lo estipulado en el artículo 1068 del código de comercio.

15. INTERVENTORÍA O SUPERVISIÓN

La Supervisión la ejercerá **SPN** a través del Director Nacional de Informática y Tecnología, o quien el ordenador del gasto designe, para el efecto se deberá notificar al contratista su designación. Así mismo, el supervisor del contrato podrá designar como supervisores de apoyo al Gerente, Profesional de Transport

é y Profesional de Distribución de Servicios Postales Nacionales S.A.S. de la respectiva regional. Así como aquellos profesionales de otras áreas de SPN encargados de supervisar la correcta ejecución en temas ambientales, riesgos y seguridad postal. En consecuencia, tendrá las siguientes atribuciones: **1.** Suscribir la respectiva Acta de Inicio y Finalización y demás inherentes a la ejecución del contrato, si hubiere lugar a ello. **2.** Verificar que EL CONTRATISTA cumpla con las obligaciones descritas en el presente contrato. **3.** Requerir al CONTRATISTA sobre el cumplimiento y obligaciones en los términos estipulados en el contrato, y efectuar el seguimiento de la ejecución de este. **4.** Informar a SPN, respecto de las demoras o incumplimiento de las obligaciones del CONTRATISTA, así como a la Secretaría General de Servicios Postales Nacionales S.A.S. **5.** Recibir la correspondencia del CONTRATISTA, y hacer las observaciones que estime convenientes. **6.** Solicitar la suscripción de contratos adicionales, prórrogas o modificatorios, previa la debida y detallada sustentación y conveniencia para el CONTRATISTA. **7.** En caso de que se presenten situaciones que requieran conceptos jurídicos especializados, de los cuales no tenga el suficiente conocimiento, así lo hará saber a la Secretaría General de SPN, con miras a lograr la mejor decisión para las partes. **8.** Verificar por que EL CONTRATISTA cumpla con lo indicado en su propuesta y respecto a la calidad de los servicios contratados y aplicar los descuentos en la facturación por Acuerdos de Niveles de Servicio - ANS pactados entre las partes, y su aplicación de acuerdo con los porcentajes y formulas establecidas. **9.** Estudiar las situaciones particulares que se presenten en desarrollo del contrato, conceptuar sobre su desarrollo general y los requerimientos para su mejor ejecución, manteniendo siempre el equilibrio contractual. **10.** Certificar respecto al cumplimiento del CONTRATISTA. Dicha certificación se constituye en requisito previo para el pago que deba realizar SPN. **11.** Solicitar la liquidación del contrato cuando finalice su ejecución adjuntando los soportes correspondientes, **12.** Las demás inherentes a la función desempeñada y contempladas en el manual de supervisión e interventoría de la SPN.

16. CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL

La presente contratación está amparada presupuestalmente por el Certificado de Disponibilidad Presupuestal No. 79537 21 de septiembre de 2023 por la suma de \$ 1,036,902,717.00 incluidos todos los impuestos y costos a que haya lugar, del cual para la presente contratación se comprometerá hasta la suma de \$ 1,036,902,717.00 incluidos todos los impuestos y costos a que haya lugar.

17. FORMA DE PAGO

Se efectuarán pagos mensuales vencidos de conformidad con el servicio global de DataCenter, hosting, nube, telecomunicaciones, conectividad, seguridad y demás servicios TI; a través de un aliado estratégico que brinde a la entidad un servicio integral y de alta disponibilidad de manera centralizada que permita la operación a nivel nacional de las diferentes sedes y aplicaciones que maneja la entidad. Prestación de un servicio global de Data Center, hosting, nube, telecomunicaciones, conectividad, seguridad y demás servicios TI; a través de un aliado estratégico que brinde a la entidad un servicio integral y de alta disponibilidad de manera centralizada que permita la operación a nivel nacional de las diferentes sedes y aplicaciones que maneja la entidad.

Nota: En todo caso el valor a pagar al contratista no podrá superar el monto establecido como disponibilidad presupuestal para ejecución del presente contrato.

PARÁGRAFO PRIMERO: Los pagos serán efectuados a los sesenta (60) días siguientes a la correcta presentación de la factura en las instalaciones de SPN S.A - Diagonal 25G No. 95A – 55 Bogotá D.C, término que no podrá ser afectado por el proceso interno de correspondencia de SPN, adjuntando los siguientes documentos: a) Constancia suscrita por el supervisor del contrato, en la que se señale que EL CONTRATISTA cumplió a satisfacción de LA ENTIDAD, con las obligaciones pactadas. b) Certificación expedida por el Revisor Fiscal o Representante Legal, que acredite que EL CONTRATISTA se encuentra a paz y salvo por concepto de pago de las contribuciones al Sistema Integral de Seguridad Social y de los Aportes Parafiscales a que haya lugar de los empleados a su cargo, adjuntando el soporte resumen de pago de la planilla única PILA de acuerdo con lo señalado en la Ley 789 de 2002. c) Certificación bancaria con fecha de expedición no mayor a noventa (90) días. d) Certificado y Control de Ejecución. e) Informe de supervisión.

EL CONTRATISTA deberá remitir la factura electrónica de venta (representación gráfica y XML) al correo radicacion.facturaelectronica@4-72.com.co

PARÁGRAFO SEGUNDO - EL CONTRATISTA no podrá adelantar actividad alguna que implique mayores gastos directos e indirectos hasta que se perfeccione la respectiva modificación contractual y esta cuente con su respectivo registro presupuestal.

18. OBLIGACIONES DE LAS PARTES

OBLIGACIONES GENERALES DEL CONTRATISTA

1. Dar cumplimiento a todos los requerimientos técnicos de la infraestructura y servicios estipulados en el **Anexo No. 01 “Especificaciones Técnicas”**.
2. Cumplir con la etapa de transición, la cual incluye la migración de todos los servicios y bases de datos hacia el Data Center del contratista.
3. Garantizar la disponibilidad y correcta operación de los componentes y servicios descritos en el **Anexo No. 01 “Especificaciones Técnicas”**.
4. Prever e incluir todos los costos de logística, traslados de materiales, elementos, equipos, administración y seguridad a los que haya lugar, durante la etapa de transición.
5. Prestar los servicios de alojamiento de la información recibida de SPN S.A.S en plataforma técnica propia del contratista, que ofrezca las más altas especificaciones en materia de alojamiento y servicios; que garanticen la disponibilidad y acceso a dichos sistemas en forma óptima por parte de los usuarios de SPN.
6. Garantizar que los equipos y materiales necesarios para la implementación y operación de los servicios objeto de la contratación cuenten con el respectivo soporte y garantía oficial por parte del fabricante.
7. Garantizar la continuidad de la operación de los servicios durante las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año (24x365), así como el debido funcionamiento de los sistemas de información de SPN. Para la etapa de posventa, el contratista debe contar con mínimo un equipo de trabajo de dos (2) profesionales con especialización en áreas afines al

presente proceso de contratación. Las funciones de estos profesionales estarán atadas a procesos de posventa tanto administrativa (Facturación, trámites, conciliación) como técnica (Gestión y seguimiento a casos técnicos de los servicios de SPN S.A.S). Se realizarán mínimo dos (2) reuniones de seguimiento mensuales con los dos (2) profesionales designados para los procesos de conciliación y seguimiento técnico.

8. Garantizar la seguridad de la información y de los datos procesados o sin procesar obtenidos en desarrollo y abstenerse de incorporarlos a redes nacionales o internacionales de transmisión de datos.
9. Garantizar que el hardware y software y en general toda la tecnología necesaria para la prestación de los servicios objeto de esta contratación no se encuentren en versiones de prueba, demo o beta y garantizar que el software ofertado cuente con las actualizaciones correspondientes durante la vigencia del contrato y/o prórrogas si hay lugar a ellas.
10. Prestar los servicios con profesionales idóneos, con la debida experiencia de modo que se garantice el buen resultado de los servicios contratados.
11. Cumplir con los tiempos, recursos y cronogramas establecidos para el desarrollo y puesta en producción de las actividades programadas.
12. Garantizar la correcta transición de los servicios del actual proveedor a las plataformas del contratista seleccionado. Es necesario tener en cuenta que esta transición puede comprender prestación de servicios adicionales temporales (las cuales no deben generar costo adicional para SPN S.A.S) como pueden ser: realizar la conectividad entre data center, aumento de las capacidades sobre la línea base, entre otros, con el fin de no generar afectación en la operación de SPN S.A.S y garantizar el tiempo de la etapa de transición.
13. Garantizar la correcta transición de los servicios tecnológicos hacia el nuevo proveedor finalizando la presente vigencia contractual.
14. La solución integral solicitada a nivel de Datacenter, Conectividad, Seguridad y otros servicios IT se debe implementar sobre IPV6 y soportar Dual Stack en convivencia con IPV4.
15. Suministro de Infraestructura y servicios conexos que corresponden a un modelo de consumo de Recursos y Servicios por Demanda, los cuales comprenden:
 - Características Data Center Principal.
 - Características Data Center Alterno (DRP).
 - Solución IAAS y SAAS con elasticidad
 - Crecimiento y decrecimiento
 - Aprovisionamiento de Recursos de Procesamiento Y Memoria
 - Aprovisionamiento de Almacenamiento
 - Servicio Copias de Seguridad Datacenter
 - Servicios Administrados
 - Servicio de Backup
 - Equipo de trabajo en Sede
 - Solución Seguridad Integral
 - Servicio de Seguridad Perimetral Full UTM

- Servicio de Seguridad Aplicaciones
- Servicio de Antivirus
- Servicio AntiDDos
- Servicio de Seguridad Avanzada
- Switches Conectividad Datacenter
- Solución SDWAN
- Conectividad Internet Dedicado
- Conectividad MPLS
- Consultoría DRP
- Gestión del servicio

OBLIGACIONES ESPECIFICAS DEL CONTRATISTA

Se debe garantizar dentro de los componentes de la solución como servicio los siguientes puntos requeridos:

- Incluir licenciamiento y/o suscripciones de Sistemas Operativos, Bases de Datos, antivirus, etc. en últimas versiones de acuerdo con lo solicitado por SPN S.A.S
- Gestión de la Infraestructura de Procesamiento de Datos, Almacenamiento, Copias de Seguridad, Conectividad, Seguridad, y servicios adicionales solicitados.
- Operación 7x24x365 de la totalidad de la Infraestructura.
- Monitoreo de: Infraestructura, Aplicaciones, Bases de Datos, Copias de Seguridad, Conectividad, Seguridad y servicios adicionales solicitados.
- La Infraestructura y los servicios involucrados en su totalidad serán responsabilidad directa del OFERENTE.
- Flexibilidad para incrementar o disminuir los servicios y/o incluso modificar las cantidades en las cuales serán determinadas por el dinamismo propio del negocio de SPN S.A.S. Para garantizar un modelo económico viable para el OFERENTE, la disminución de servicios no podrá ser mayor al 15% anual sobre la línea base.
- Realizar el levantamiento de requerimientos, diseño, implementación, pruebas, operación y documentación que garantice el cumplimiento de los ANS.
- Proveer los servicios de seguridad física de acceso y seguridad de la información e informática para la infraestructura alojada y los servicios de comunicación buscando garantizar la confidencialidad, integridad y disponibilidad de la información y de los servicios alojados incluyendo las comunicaciones provistas desde los Datacenter
- El oferente deberá contar con una política de seguridad física y una política de seguridad de la información.
- El oferente deberá crear y/o contar con procesos de gestión documentados (procedimientos, manuales, formatos, políticas, guías) tales como:
 - Gestión de las capacidades
 - Gestión de incidentes

- Gestión de requerimientos
- Gestión de problemas
- Gestión de cambios
- Gestión de accesos
- Plan de continuidad de negocio
- Plan de actualizaciones
- Plan de mantenimientos
- Procedimiento de copias de respaldo
- El oferente debe contar con SOC (Security Operation Center) y debe enviar documento general de procesos y carta firmada por el representante legal o quien haga las veces de OFERENTE, que certifique lo solicitado. En caso de integrar a un operador que preste el servicio de SOC, el OFERENTE deberá adjuntar la certificación emitida por el representante legal de dicho operador en la que se exprese la disponibilidad del SOC y la autorización de uso en la oferta.
- Implementar políticas para seguridad de la información en el Datacenter.
- Incluir un sistema de gestión en el que se permita monitorear, administrar y gestionar todos los dispositivos que técnicamente lo permitan y que formen parte de los servicios ofrecidos a SPN S.A.S. Se solicita vista de lectura de la aplicación del sistema de gestión y/o monitoreo a nivel de Datacenter, Conectividad y Seguridad, para los servicios entregados a SPN S.A.S por el OFERENTE.
- Incluir todos los equipos, materiales y accesorios necesarios para el correcto montaje y funcionamiento de los sistemas solicitados.
- Prever e incluir todos los costos de logística, traslados de materiales, elementos y equipos, administración y seguridad a los que haya lugar.
- Los equipos deben operar 7x24x365.
- Los reportes e informes asociados a los servicios serán concertados conjuntamente al inicio de la ejecución del contrato, y se verá reflejado en el modelo operativo del servicio.
- Revisar cuidadosamente los trabajos a realizar, su naturaleza y sus características, y es entendido que todos los factores, favorables y desfavorables, que puedan afectar el costo o el plazo para la ejecución de los trabajos, fueron tenidos en cuenta por el oferente al formular su propuesta.
- Los componentes, elementos, dispositivos, equipos, sistemas y soluciones implementados deben contar con las condiciones técnicas que permitan dar cumplimiento a los ANS. Igualmente deben contar con garantías y contratos de soporte.
- Entregar a SPN S.A.S la documentación de los diseños de las soluciones que soportan la operación.
- Realizar las bitácoras de manera digital de las actividades y eventos ocurridos en los servicios TIC y deberán ser entregados en informes de gestión mensual.
- Elaborar y entregar un procedimiento que defina el proceso a seguir cuando se encuentre evidencia de alteración o manipulación de dispositivos o información.

- Los trabajos realizados por el OFERENTE con ocasión de este contrato deben garantizar la seguridad e integridad física de las personas de SPN S.A.S, del proveedor y de los contratistas que intervengan, así como la de las instalaciones y los equipos de SPN S.A.S además de la información lógica contenidas en estos.

OBLIGACIONES DEL CONTRATANTE

1. Pagar al CONTRATISTA el valor del contrato dentro del término y condiciones pactadas, previa certificación de cumplimiento expedida por el supervisor de este.
2. Supervisar que el CONTRATISTA cumpla con el objeto y obligaciones del contrato dentro del término de ejecución.
3. Suministrar de manera oportuna al CONTRATISTA la información requerida para el adecuado cumplimiento de sus obligaciones, así como el acceso a la infraestructura o plataformas tecnológicas que se requieran para el cumplimiento del objeto del contrato.
4. Convocar a las reuniones a que haya lugar para el desarrollo de las actividades inherentes al objeto del contrato.
5. Expedir las certificaciones a que haya lugar.
6. Liquidar el contrato en el término establecido en el contrato y en la ley.
7. Las demás que se desprendan en desarrollo del contrato.

19. CLÁUSULA DE CONFIDENCIALIDAD

Las partes se obligan a mantener confidencialidad respecto de toda información que a partir de la fecha reciben los empleados, personal vinculado o asesores de cada una de ellas, de manera directa o indirecta, en forma verbal o escrita, gráfica, en medio magnético o bajo cualquier otra forma. En consecuencia, EL CONTRATISTA adoptará las medidas necesarias para que la información no llegue a manos de terceros en ninguna circunstancia, y se obligan a no utilizarla para ningún objeto diferente al de adelantar las tareas que se deriven directamente del cumplimiento.

20. CLÁUSULA DE PROTECCION DE DATOS PERSONALES.

En caso de que **EL CONTRATISTA** tenga la condición de *encargado del tratamiento*, de conformidad con el artículo 3 literal d) de la Ley Estatutaria 1581 del 17 de octubre de 2012, en adelante LEPD, en la medida que el objeto del contrato pueda implicar el tratamiento de datos personales a cargo de **SERVICIOS POSTALES NACIONALES S.A.S.** por parte de **EI CONTRATISTA**, éste último se obliga y compromete, con base al artículo 25 del Decreto 1377 de 2013, a una serie de aspectos identificados a continuación:

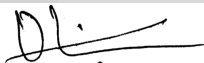
1. **EL CONTRATISTA** se compromete y obliga a guardar secreto de todos los datos personales que conozca y a los que tenga acceso en virtud del presente contrato.
2. Custodiará e impedirá el acceso a los datos personales a cualquier usuario no autorizado o persona ajena a su organización. Las anteriores obligaciones se extienden en cualquier fase del tratamiento que de esos datos pudiera realizarse y subsistirán aún después de terminados los mismos.

EL CONTRATISTA únicamente tratará los datos conforme a las instrucciones que reciba expresamente de **SERVICIOS POSTALES NACIONALES, S.A.S.**, y no los destinará, aplicará o utilizará con fin distinto al que figure en el presente contrato. Así mismo, se compromete a no revelar, transferir, ceder o de otra forma comunicar los bases de datos o datos contenidos en ellos, ya sea verbalmente o por escrito, por medios electrónicos, papel o mediante acceso informático, ni siquiera para su conservación, a otras personas; salvo que previa indicación expresa de **SERVICIOS POSTALES NACIONALES, S.A.S.**, comunique los datos a un Tercero designado por aquél, al que hubiera encomendado la prestación de un servicio. **EL CONTRATISTA** manifiesta conocer las obligaciones derivadas la ley de protección de datos personales. Así mismo, garantiza el mantenimiento de las medidas de Seguridad; así como cualesquiera otras que le fueren impuestas por parte de **SERVICIOS POSTALES NACIONALES S.A.S.**, de índole técnica y organizativa, necesarias para garantizar la seguridad de los datos de carácter personal. **SERVICIOS POSTALES NACIONALES S.A.S.**, previa solicitud, podrá facilitar un extracto de las medidas de seguridad que el contratista debe acatar en cumplimiento de las obligaciones descritas en esta cláusula. Finalizada la prestación del servicio contratado, los datos personales serán destruidos o devueltos a **SERVICIOS POSTALES NACIONALES S.A.S.**, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando a **SERVICIOS POSTALES NACIONALES S.A.S.** dicha conservación. El contratista podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con **SERVICIOS POSTALES NACIONALES, S.A.S.** En cualquier caso, el contratista comunicará a **SERVICIOS POSTALES NACIONALES, S.A.S.** cualquier incidencia que se produzca en ejecución del presente contrato, que pueda afectar la confidencialidad, integridad y disponibilidad de los datos personales, dentro del plazo de dos (2) días hábiles contados a partir desde la fecha en que se hubiese producido la incidencia o hubiese tenido conocimiento de la misma, para que se adopten las medidas correctivas de forma oportuna. Del mismo modo, el contratista pondrá en conocimiento del personal a su servicio las obligaciones indicadas en la presente cláusula, cerciorándose, mediante la adopción de las medidas

22. ANEXOS

- Cotización
- SDP
- Oficio justificación Solicitud de Disponibilidad
- CDP

23. FIRMAS



OCTAVIO ENRIQUE CALDERON JIMENEZ

Profesional de Informática y Tecnología –

Director Nacional de Informática y Tecnología (AF)

Proyecto: Nathalia Becerra Leon- Líder Nvl 3/ Tramites contractuales IT.

Reviso condiciones técnicas- Jorge Armando Garcia – Profesional Experto Nivel III