UNP - ANEXO TÉCNICO 3 – LINEA DE SERVICIOS CENTRALES

Abril 2026

Contenido

Contenido

1. DESCRIPCIÓN GENERAL DE LA LINEA 4
   1.1. Línea 4
   1.2. Objetivo 4
   1.3. Caracterización de la línea 4
   1.4. Personal 5
   1.5. Alcance 5
   1.6. Acuerdos de niveles de servicio 6
2. DATACENTER Y DATACENTER ALTERNO 6
   2.1. Objetivo 7
   2.2. Condiciones y necesidades del servicio 7
   2.3. Condiciones generales 9
   2.4. Cobertura 9
   2.5. Horario 10
   2.6. Línea base 10
   2.7. Operación de acuerdo con las prácticas ITIL 4 implementadas 10
   2.8. Colocación en Datacenter Principal 10
      2.8.1. Objetivo 10
      2.8.2. Condiciones y necesidades del servicio 10
   2.9. Colocación del Datacenter Alterno 12
      2.9.1. Objetivo 12
      2.9.2. Condiciones y necesidades del servicio 13
   2.10. Soporte especializado plataformas centrales 15
      2.10.1. Objetivo 15
      2.10.2. Condiciones y necesidades del servicio 15
      2.10.3. Condiciones Generales 16
      2.10.4. Cobertura 16

2.10.5. Horario 17
2.10.6. Línea base 17
2.11. Entregables para Datacenter y Datacenter Alterno/DRP 17
3. CONECTIVIDAD DATA CENTER PRINCIPAL Y ALTERNO 17
3.1. Objetivo 17
3.2. Condiciones y necesidades del servicio 17
3.2.1. Canal de internet ..... **¡Error! Marcador no definido.**
3.3. Condiciones generales 18
3.4. Cobertura 19
3.5. Horario 19
3.6. Entregables de Conectividad 19
4. SEGURIDAD DE LA INFORMACIÓN 19
4.1. Objetivo 19
4.2. Condiciones y necesidades del servicio 19
4.3. Condiciones generales 24
4.3.1. Alcance del servicio (Descripción general de CSOC) 25
4.3.2. Plataformas de Administración del CSOC 25
4.3.3. Respuesta a Incidentes de Seguridad 26
4.3.4. Mejora Continua de Seguridad 26
4.3.5. Administración de Plataformas de Seguridad de Usuarios, Web y BD 27
4.3.6. Gestión y Monitoreo de Dispositivos de Seguridad 27
4.3.7. Disponibilidad del Servicio 27
4.4. Cobertura 28
4.5. Horario 28
4.6. Línea base 28
4.7. Entregables Seguridad de la Información 28
5. LICENCIAMIENTO 29
5.1. Objetivo 29
5.2. Condiciones y necesidades del servicio 29
5.3. Condiciones generales 29

5.4. Cobertura 29
5.5. Horario 30
5.6. Línea base 30
5.7. Entregables de Licenciamiento 30

1. DESCRIPCIÓN GENERAL DE LA LINEA

1.1. Línea

Servicios centrales

1.2. Objetivo

Proveer, mantener y gestionar los servicios que son prestados de manera centralizada, los cuales se encuentran descritos en el presente documento.

1.3. Caracterización de la línea

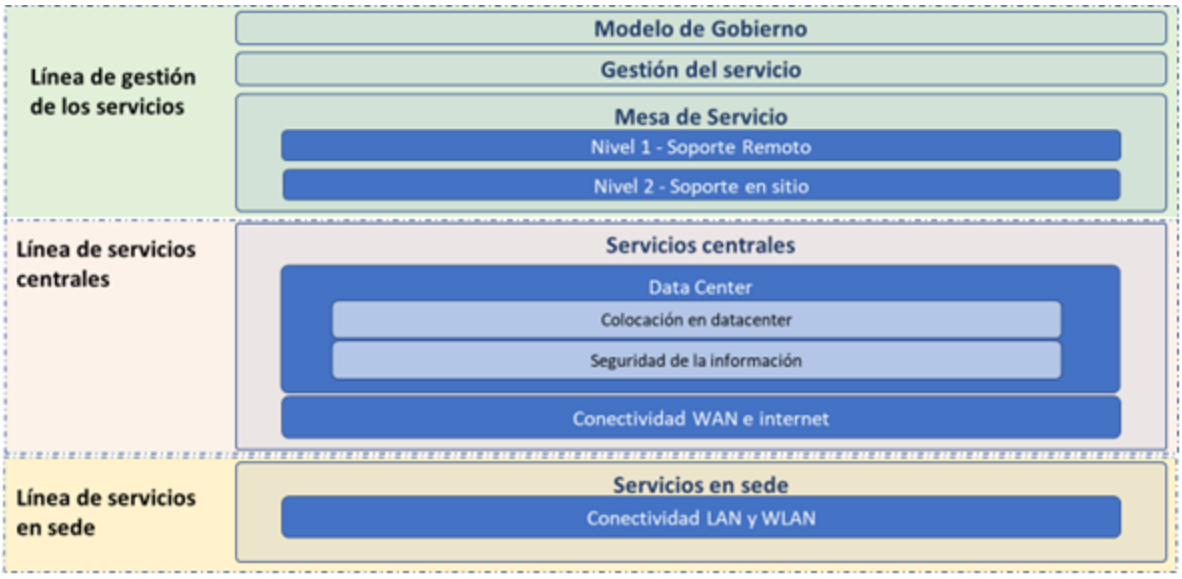


Figura 1. Líneas de servicio

La línea de servicios centrales es la encargada de proveer todos los servicios que deben ser habilitados de manera centralizada (Datacenter, colocación para plataforma central -procesamiento, almacenamiento y respaldo, soporte especializado plataformas centrales, seguridad de la información, licenciamiento de soluciones para Datacenter Alterno y los que permiten acceder a los servicios habilitados de manera centralizada como lo es la conectividad a través de la WAN e internet.

1.4. Personal

El contratista debe dimensionar y disponer los recursos que sean necesarios para implementar, instalar, configurar, operar y gestionar las diferentes tecnologías que son parte del alcance del presente proceso, teniendo en cuenta que como mínimo debe considerar:

- Un (1) líder para la línea de servicios centrales
- Los especialistas o técnicos que sean necesarios para administrar la totalidad de servicios que hacen parte de la presente línea de servicio.

El personal mínimo requerido se encuentra detallado en el documento **UNP - Anexo Personal**.

El oferente debe dimensionar y considerar los recursos adicionales a los establecidos en el documento **UNP - Anexo Personal** que sean necesarios para administrar (Datacenter, colocación para plataforma central -procesamiento, almacenamiento y respaldo-, soporte especializado plataformas centrales, seguridad de la información, licenciamiento de soluciones para Datacenter Alterno y los que permiten acceder a los servicios habilitados de manera centralizada como lo es la conectividad a través de la WAN e internet), según las condiciones establecidas por la entidad en el presente documento

El personal del CONTRATISTA deberá contar con idoneidad, experiencia, herramientas y elementos necesarios para la prestación del servicio.

Lugar y condiciones de prestación del servicio

Todo el personal descrito en este anexo, tanto el mínimo requerido como el adicional que determine el CONTRATISTA, deberá estar ubicado en las instalaciones de la Entidad según sus prioridades y hasta donde su capacidad lo permita.

El CONTRATISTA debe proveer todos los elementos de trabajo que sean necesarios para que los especialistas o responsables de la prestación del servicio puedan desarrollar sus funciones.

1.5. Alcance

La línea de servicios centrales está orientada a garantizar la correcta prestación de los servicios que son habilitados de manera centralizada, los cuales en condiciones normales se encuentran alojados en las plataformas de procesamiento y almacenamiento dispuestas al interior del Datacenter, entre los cuales se pueden encontrar bases de datos, sistemas de información, aplicaciones especializadas de orden misional de la entidad, entre otras, las cuales a través pueden ser accedidas o consumidas por los funcionarios de la entidad desde las diferentes sedes a través de la WAN o internet (la Red WAN y el internet son responsabilidad de la entidad).

Como parte de los servicios centrales se encuentran:

- Servicio de Colocación -Collocation- para la plataforma de TI propiedad de la entidad DC Principal. Soporte especializado para plataformas centrales (Datacenter y Datacenter Alterno/DRP) incluyendo Sistemas operativos, bases de datos y Backup.
- Servicios conexos
- Seguridad de la información
- Licenciamiento de soluciones para Datacenter y Datacenter Alterno/DRP
- Administración y soporte para la totalidad de las soluciones de tecnología con las que cuenta la entidad las cuales están descritas en el anexo **UNP - Anexo Inventario - Distribución de Equipos**, la idoneidad técnica será evaluada por la supervisión del contrato en los casos que aplique.

1.6. Acuerdos de niveles de servicio

Los acuerdos de niveles de servicio se encuentran establecidos en el documento **UNP - Anexo acuerdos de niveles de servicio**, dentro del cual se encuentran especificados todos y cada uno de los servicios objeto del presente proceso y asociados a ellos los ANS correspondientes.

2. DATACENTER Y DATACENTER ALTERNO

Datacenter en modalidad de servicio para atender las necesidades de la entidad, a través del cual se habiliten los servicios de procesamiento (servidores), almacenamiento y respaldo para soportar los sistemas de información y aplicaciones especializadas de la entidad.

Datacenter principal - Colocación

La entidad requiere una solución de Datacenter para colocación sobre el cual se hospede la infraestructura tecnológica propiedad de la entidad, permitiendo garantizar la prestación de los servicios de Datacenter para el alojamiento de las aplicaciones misionales y de apoyo a su objeto social, así como los servicios de almacenamiento, licenciamiento, administración de los sistemas operativos y motores de bases de datos, copias de respaldo (backups), herramienta de replicación y seguridad de la plataforma tecnológica y de su información crítica.

La infraestructura de la entidad disponible para el Datacenter Principal se encuentra referenciada en el Anexo de **UNP – Anexo Inventario - Distribución de Equipos**, pestaña DC PRINCIPAL

Datacenter Alterno/DRP

La entidad requiere que como parte del servicio objeto del presente proceso, se habilite por parte del contratista la solución de Datacenter alterno que debe ser concebido bajo el esquema de DRP integral Incluyendo servicio de Collocation, Cross conexiones, administración de SO y BD, Replicación desde datacenter Principal y los elementos de conectividad (Switch y/o Firewall), de acuerdo con el alcance indicado. El servicio de Datacenter alterno debe atender cualquier incidente o falla parcial o total en función del RTO y RPO definido sobre los sistemas a replicar.

La infraestructura de la entidad disponible para el Datacenter Alterno se encuentra referenciada en el **UNP – Anexo Inventario - Distribución de Equipos**, pestaña DC ALTERNO

2.1. Objetivo

Proveer el servicio de Datacenter principal y alterno con funciones y configuraciones de DRP capaces de soportar la infraestructura tecnológica de la entidad.

2.2. Condiciones y necesidades del servicio

Datacenter principal

A continuación, se plantean las condiciones bajo las cuales se debe prestar el servicio por parte del contratista:

- Proporcionar el servicio de Datacenter principal a través de un centro de datos TIER IV o superior certificado por el Uptime Institute o ICREA nivel V certificado por la International Computer Room Experts Association.
- Garantizar la redundancia a todo nivel en el Datacenter principal (suministro eléctrico, aire acondicionado, conectividad interna, etc.) en el Datacenter de acuerdo con los niveles TIER IV o superior del Uptime Institute o nivel V o superior de ICREA
- Interconectar el Datacenter principal con la totalidad de sedes de la entidad
- Interconectar el Datacenter principal con el alterno.
- Suministrar los equipos de red necesarios para garantizar la conectividad al interior del Datacenter para la prestación del servicio.

Consideraciones adicionales para el CONTRATISTA

- El contratista debe aportar la certificación vigente para Datacenter de cualquiera de las siguientes entidades internacionales certificadoras:

  - ICREA (International Computer Room Experts Association), La Entidad que certifica los centros de datos alrededor del mundo. Mínimo Nivel V HS-WCQA.
  - Uptime Institute, The Global Data Center Authority. Mínimo TIER 4 Diseño y Construcción.
- El Datacenter debe estar ubicado en Colombia.
- La ubicación del Datacenter principal ofertado de estar en la ciudad de Bogotá D.C y/o sus alrededores, a una distancia no mayor a 50 kilómetros de la sede principal de la entidad.
- El Datacenter incluido en la propuesta debe demostrar por lo menos ocho (8) años de madurez en prestación en servicios similares desde la construcción del Datacenter. El contratista debe adjuntar carta del representante legal propietario del Datacenter, indicado la madurez de la operación del centro de datos del CONTRATISTA.
- El contratista debe presentar información correspondiente a ubicación detallada del Datacenter principal.
- El contratista o el operador que éste integre para la prestación del servicio de Datacenter debe acreditar la propiedad del predio donde se encuentra ubicado el centro de datos principal presentado en la propuesta, con el fin de asegurar autonomía operacional durante la ejecución del contrato. En caso de que se integre a un operador del servicio de Datacenter, el contratista deberá adjuntar la certificación emitida por el Representante Legal de dicho operador en la que lo autoriza a ofrecer su Datacenter para esta contratación.
- El Datacenter debe contar con controles de acceso, vigilancia, CCTV, sistema de detección y extinción de incendios, sistema de climatización, monitoreo continúo y chapa de seguridad en la puerta de cada rack.
- El propietario del Datacenter debe ser Certificado ISO 27001 vigente con al menos 5 años de madurez en esta certificación.
- El propietario del Datacenter debe ser Certificado ISO 20000 vigente con al menos 3 años de madurez en esta certificación.

Datacenter alterno

A continuación, se plantean las condiciones a nivel de Datacenter que son de obligatorio cumplimiento para la prestación del servicio integral de Datacenter Alterno/DRP por parte del contratista:

- Proporcionar el servicio de Datacenter alterno para garantizar la continuidad del negocio.
- La solución ofertada debe estar alojada en un Datacenter alterno 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.
- La entidad será responsable de suplir los canales de comunicación necesarios para interconectar el Datacenter alterno con la totalidad de sedes de la entidad
- Proporcionar una solución de DRP para garantizar la continuidad de los servicios de Datacenter que soportan la operación de la entidad.

- Las capacidades de Computo, memoria, almacenamiento, licenciamiento y otros que apliquen dependerán de la configuraciones y equipos de la entidad
- Efectuar dos (2) pruebas en la vigencia del contrato, de Failover y Rollback para confirmar el correcto funcionamiento de la solución.
- Ejecutar las pruebas de DRP para las aplicaciones que la entidad defina, dentro del listado de los sistemas que tienen ambientes de contingencia.
- Garantizar un RPO igual o menor a dos (2) horas. El punto de recuperación de la Información en caso de algún evento deberá ser cumpliendo la disponibilidad en un tiempo igual o menor a dos (2) horas.
- Garantizar un RTO igual o menor a dos (2) horas. El tiempo de recuperación de la funcionalidad en caso de algún evento deberá ser igual o menor a dos (2) horas.
- La holgura operacional de los sistemas del DRP de los servicios del Datacenter alterno debe ser mínimo del 50% a nivel funcional de procesamiento y memoria, y del 100% a nivel de almacenamiento.
- Diseñar e implementar 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.
- Suministrar los equipos de red necesarios para garantizar la conectividad al interior del Datacenter para la prestación del servicio.

2.3. Condiciones generales

A continuación, se plantean las condiciones bajo las cuales se debe prestar el servicio por parte del CONTRATISTA:

- Entregar reportes mensuales de la disponibilidad de los servicios y el cumplimiento de ANS asociados.
- El contratista debe garantizar el funcionamiento de hardware, software, entre otros que sean necesarios para garantizar la óptima prestación del servicio.

2.4. Cobertura

La totalidad de la infraestructura que soportan los servicios centrales deben estar habilitados dentro del Datacenter Principal y Alterno, espacio suministrado por el CONTRATISTA, teniendo en cuenta:

- La plataforma central correspondiente a los equipos y componentes asociados a las capas de procesamiento, almacenamiento y respaldo.
- Plataforma de seguridad informática
- Plataforma para aplicaciones especializadas
- Servidores para telefonía IP

Todos los servicios y aplicaciones habilitados en el Datacenter, para gestión o consulta, deben poder ser accedidos por los funcionarios de la entidad a través de la conectividad LAN/WLAN en las sedes y la WAN que interconecta dichas sedes, garantizando la continuidad de la operación de la entidad sobre los aplicativos y plataformas de gestión.

2.5. Horario

Este servicio debe estar disponible y en operación en modalidad 7x24x365, para el Datacenter Principal y Alterno

2.6. Línea base

Las cantidades y distribución de los equipos en las sedes de la entidad se establecen en el documento **UNP – Anexo Inventario - Distribución de Equipos**

2.7. Operación de acuerdo con las prácticas ITIL 4 implementadas

El CONTRATISTA debe efectuar la prestación del servicio de acuerdo con las prácticas de ITIL que dispone la entidad, aplicables a los procesos de Datacenter Principal y Alterno

- Gestión de Catálogo de Servicios.
- Gestión de Incidentes.
- Gestión de Solicitudes.
- Gestión de Problemas
- Gestión de Cambios
- Gestión de Implementación

2.8. Colocación en Datacenter Principal

2.8.1. Objetivo

Proveer las condiciones de Datacenter para habilitar la infraestructura existente propiedad de la entidad, la cual debe ser ubicada en las instalaciones del Datacenter principal provisto por el CONTRATISTA.

2.8.2. Condiciones y necesidades del servicio

A continuación, se plantean las condiciones bajo las cuales se debe prestar el servicio por parte del CONTRATISTA:

- Efectuar el traslado de la infraestructura, teniendo en cuenta todos los costos asociados como lo son transporte, seguros, logística, respaldo de información y todo lo que sea necesario para garantizar la continuidad del servicio.
- Proveer el servicio de colocación en Datacenter para ubicar la infraestructura tecnológica propiedad de la entidad según anexo **UNP – Anexo Inventario - Distribución de Equipos**
- Garantizar la prestación de los servicios de Datacenter para el alojamiento de las aplicaciones misionales y de apoyo del objeto social de La entidad, así como la actualización

de las garantías del hardware propiedad de la entidad que hará parte del servicio base de colocación en Datacenter.

- Prestar a La entidad el servicio de disponibilidad de espacio (colocación), el cual consta de espacio en gabinetes (racks), suministro de conexiones y energía eléctrica y conectividad horizontal y vertical (cobre y fibra óptica), para alojar la infraestructura de TI propiedad de la entidad bajo un ambiente adecuado y seguro de operación de la información.
- Suministrar los racks y disponerlos al interior del Datacenter de forma contigua, los cuales deben ser exclusivos para la entidad.
- Disponer las condiciones de colocación disponibles dentro de máximo un (1) mes a partir de la firma del acta de inicio, en todo caso el contratista deberá garantizar la disponibilidad del servicio durante la ejecución total de la vigencia del contrato
- El Datacenter debe cumplir las condiciones establecidas en el numeral 2. DATACENTER del presente documento.

Especificaciones técnicas para los equipos alojados

- Instalación del rack en el sitio y la disponibilidad de energía.
- Espacio para al menos Cuatro (4) racks completos, de acuerdo con la necesidad del servicio teniendo en cuenta el inventario y futuros crecimientos,
- Incluir al menos cuatro Switch TOR de 48 puertos 1 GB y al menos 2 de 10 Gbps de fibra óptica.
- Incluir los circuitos eléctricos para los Cuatro (4) racks bifásicos y/o trifásicos teniendo en cuenta los equipos a alojar.
- Debe incluir patch cords UTP categoría 6A por rack, tanto para los racks de servidores como para los racks de cableado LAN. En igual número de puertos de acuerdo al swtich TOR con longitud que satisfaga la interconexión a equipos entre racks.
- Enlaces de fibra horizontal multimodo con patch panel por rack si aplica.
- Patch cords de fibra LC-LC por rack, para los racks de servidores y para los racks de cableado SAN. Para cubrir la conectividad necesaria con una longitud mínima de 5 metros.
- Instalación física del rack anclaje y aterrizaje de cada uno de los racks.
- Etiquetado de los racks.
- Marquillado del cableado
- Energía para Rack, 3 de los cuatro requeridos se encuentran en un consumo mensual de 5 KVAs y uno se encuentra con un consumo de 7KVAs

Otros servicios

- Paquete de servicio de 15 horas de manos remotas por mes acumulable por lo menos un año 7x24x365.
- Servicio de cintoteca para alojamiento de cintas y medios magnéticos mínimo para seiscientas (600) Cintas dentro del Datacenter.

- Dos (2) puestos de trabajo compartidos disponibles para ser utilizados por la entidad en el momento que sea requerido de acuerdo con el protocolo indicado por el contratista, los cuales deben tener conectividad hacia los racks de La Entidad.

Condiciones de prestación del servicio

- La operación del Datacenter debe ser 7x24x365
- La disponibilidad comprometida para equipos con doble fuente debe ser de 99,982% o en una configuración de tipo HA
- La disponibilidad comprometida para equipos con una fuente debe ser de 99,6 %.
- Los operadores de Datacenter deben reportar a quien designe la entidad cualquier alarma que observen en los equipos alojados en el Datacenter
- Los operadores deben tramitar los requerimientos solicitados y/o autorizadas por el contacto principal de la entidad, para ingreso de repuestos, retiro de elementos, ingreso de elementos, para los equipos de la entidad que ingresaron con los procedimientos definidos por el Datacenter, y con un tiempo de respuesta no mayor a cuatro (4) horas.
- Para el caso de equipos de reemplazo, repuestos o partes que se requieran para dar continuidad a la operación, la autorización de ingreso deberá ser tramitada a cualquier hora del día, en un plazo máximo de una (1) hora.
- Los operadores deben tramitar los requerimientos solicitados y/o autorizadas por el contacto principal de La Entidad del servicio de ojos y manos remotas, para los equipos de la entidad que ingresaron con los procedimientos definidos por el Datacenter.
- Los operadores deben tramitar los accesos de autorización de entrada de personas solicitadas y/o autorizadas por el contacto principal de La Entidad 7x24x365, y con un tiempo de respuesta no mayor a una (1) hora.

Bodega de tránsito

El CONTRATISTA debe contar con una bodega transitoria para gestión de cambio infraestructura en el Datacenter por un tiempo mínimo de 30 días durante la ejecución del presente contrato.

2.9. Colocación del Datacenter Alterno

2.9.1. Objetivo

Proveer la colocación para la infraestructura de la Entidad que hará parte de la solución de Datacenter Alterno.

2.9.2. Condiciones y necesidades del servicio

Servicios de la entidad que deben ser respaldados a través de la solución de Replicas en Datacenter Alterno provista por el CONTRATISTA

- Proveer el servicio de colocación en Datacenter Alterno para ubicar la infraestructura tecnológica propiedad de la entidad descrita en los anexos **UNP – Anexo Inventario - Distribución de Equipos** y **UNP – Anexo de Licenciamiento**
- La entidad requiere replicar Máquinas virtuales de las que se tienen en el Datacenter principal (300 Vcpus y 1500 GB de Memoria) en un hosting en el datacenter alterno.
- Las Máquinas virtuales a replicar en el hosting deben contar con su respectivo antivirus.
- La entidad actualmente en las máquinas virtuales a replicar tiene una capacidad de 30 TB, las cuales deben tener un rendimiento mínimo de 5000 IOPS.
- La cantidad de Máquinas virtuales a Replicar en el hosting será de acuerdo con el anexo **UNP – inventario- distribución de equipos**.
- El CONTRATISTA es responsable del licenciamiento de Sistema operativo Windows y Linux en el esquema de servicio solicitado para el hosting del Datacenter Alterno, cuando aplique. Los licenciamientos que no se puedan actualizar quedaran como MAQUINAS NO SOPORTADAS
- Se requiere como mínimo 25 Vcore con licenciamiento SQL Standard y 25 Vcore con licenciamiento SQL Standard.
- El CONTRATISTA es responsable de la administración, monitoreo y gestión de la Hiperconvergencia del datacenter alterno
- El CONTRATISTA es responsable de la administración, monitoreo y gestión de Base de datos MS SQL/POSTGRES cantidad 15 y My SQL cantidad 10.
- El CONTRATISTA es responsable del licenciamiento de la herramienta de replicación como servicio, que garantice la cantidad de máquinas y data a replicar, garantizando el RPO y RTO solicitado por la entidad.
- El CONTRATISTA es responsable de entregar la conectividad para replicación, necesaria hacia el Datacenter Alterno.
- El CONTRATISTA es responsable de la documentación y de los procesos a realizar para las pruebas de DRP/Failover y escenarios reales, donde se debe entregar con detalle el plan de contingencia y regreso hacia el Datacenter Principal, los cuales deben ser aprobados por la supervisión del contrato
- El contratista debe administrar la antivirus propiedad de la entidad dentro del servicio de Datacenter Alterno
- El Datacenter Alterno debe contar con espacio y disponibilidad energética para instalar 3 Servidores DELL para una Hiperconvergencia propia de la entidad.
- El contratista debe administrar los servicios de Colocation, hiperconvergencia y el clúster de servidores DELL que la entidad disponga para el Datacenter Alterno.

El CONTRATISTA es responsable funcional de la administración de aplicaciones en el Datacenter Alterno, en los casos que aplique.

Especificaciones técnicas para los equipos alojados

- Instalación del rack en el sitio y la disponibilidad de energía.
- Espacio para Rack, de acuerdo con el inventario de La Entidad.
- Incluir al menos un Switch TOR de 48 puertos 1 GB y al menos 1 Switch de 10 Gbps de fibra óptica por cada Rack.
- Incluir los circuitos eléctricos el medio Rack bifásicos y/o trifásicos teniendo en cuenta los equipos a alojar.
- Energía para Rack, la cual esta medida en un consumo mensual de 5 KVAs
- El Rack debe incluir patch cords UTP categoría 6A, con longitud que satisfaga la interconexión a equipos dentro del rack.
- Enlaces de fibra horizontal multimodo con patch panel por rack si aplica.
- Patch cords de fibra LC-LC por rack, para los servidores y dispositivos que la entidad disponga.
- Instalación física del rack anclaje y aterrizaje.
- Etiquetado de Rack
- Marquillado del cableado

Condiciones de prestación del servicio

- La operación del Datacenter Alterno debe ser 7x24x365
- La disponibilidad comprometida para equipos con doble fuente debe ser de 99,982% o en una configuración de tipo HA
- La disponibilidad comprometida para equipos con una fuente debe ser de 99,6 %.
- Los operadores de Datacenter Alterno deben reportar a quien designe la entidad cualquier alarma que observen en los equipos alojados en el Datacenter Alterno
- Los operadores deben tramitar los requerimientos solicitados y/o autorizadas por el contacto principal de la entidad, para ingreso de repuestos, retiro de elementos, ingreso de elementos, para los equipos de la entidad que ingresaron con los procedimientos definidos por el Datacenter Alterno, y con un tiempo de respuesta no mayor a cuatro (4) horas.
- Para el caso de equipos de reemplazo, repuestos o partes que se requieran para dar continuidad a la operación, la autorización de ingreso deberá ser tramitada a cualquier hora del día, en un plazo máximo de una (1) hora.
- Los operadores deben tramitar los requerimientos solicitados y/o autorizadas por el contacto principal de La Entidad del servicio de ojos y manos remotas, para los equipos de la entidad que ingresaron con los procedimientos definidos por el Datacenter Alterno.
- Los operadores deben tramitar los accesos de autorización de entrada de personas solicitadas y/o autorizadas por el contacto principal de La Entidad 7x24x365, y con un tiempo de respuesta no mayor a una (1) hora.

2.10. Soporte especializado plataformas centrales

2.10.1. Objetivo

Proveer como parte de los servicios de gestión de las plataformas centrales de la entidad, a fin de garantizar la correcta prestación de los servicios centrales a los funcionarios de la entidad.

2.10.2. Condiciones y necesidades del servicio

A continuación, se plantean las condiciones bajo las cuales se debe prestar el servicio por parte del CONTRATISTA:

Asegurar la correcta operación de los servicios de acceso teniendo en cuenta:

Servicios Base Directorio Activo

- **Servicios de acceso**
  - DNS
  - DHCP
- **Sistemas operativos**
  - Linux
  - Windows
  - AOS
- **Ambientes virtuales**
  - Nutanix
  - HyperV
- **Base de datos**
  - SQL(Server – Standard)
  - MY SQL
  - PostgresSQL
- **Respaldos**
  - Veeam BackUp
  - DellNetworker

- De acuerdo con el inventario suministrado por la entidad, el CONTRATISTA será responsable, durante la ejecución del contrato, de las renovaciones de licenciamiento y del soporte de hardware de los elementos incluidos en la colocatión, según lo estipulado en el Anexo **UNP - Anexo de Licenciamiento**
- El CONTRATISTA es responsable del soporte y garantía de Software hipervisor y solución de veeam Backup , según el anexo **UNP - Anexo de Licenciamiento**
- El CONTRATISTA es responsable del monitoreo, gestión y administración de los Sistemas Operativos Windows Server y los sistemas operativos Linux en el Datacenter principal, y a su vez es responsable de la administración de los sistemas a replicar en el Datacenter alterno que están definidos en el capítulo de recuperación de desastres del presente documento.

- El CONTRATISTA es responsable del monitoreo, gestión y administración de 20 Bases de Datos MS SQL y 15 Bases de datos My SQL en el Datacenter principal, y a su vez es responsable de la administración de las bases de datos a replicar en el Datacenter alterno del presente documento.
- El CONTRATISTA es responsable del monitoreo, gestión y administración de la solución de respaldo de datos actual de la entidad la cual es VEEAM BackUp, así mismo es responsable de la actualización, soporte y garantía de este licenciamiento, según el anexo **UNP - Anexo de Licenciamiento y UNP-Anexo de inventario-Distribución de equipos.**
  El CONTRATISTA es responsable de la renovación del soporte y garantía de licenciamiento de acuerdo con el anexo de inventario en caso de que aplique, revisar el anexo **UNP - Anexo de Licenciamiento**
- La entidad es responsable del licenciamiento funcional de los sistemas de información que hacen parte del **UNP - Anexo de Licenciamiento**, de la pestaña de sistemas de información tanto para el Datacenter principal y alterno.
- El CONTRATISTA es responsable de licenciamiento, administración y soporte de las herramientas de réplica de datos entre el Datacenter principal y alterno, cumpliendo el RTO y RPO solicitado por la entidad.

2.10.3. Condiciones Generales

- El servicio debe garantizar la disponibilidad de las diferentes plataformas y sistemas de información de la entidad, las cuales deben estar disponibles cuando sean requeridas por los funcionarios para efectos de apoyar el desarrollo de sus funciones.

Consideraciones adicionales

- El personal que disponga el CONTRATISTA para el cumplimiento de las condiciones, deberá contar con el conocimiento y experiencia necesaria para administrar y soportar la plataforma de TI de la entidad.

A continuación, se plantean las condiciones bajo las cuales se debe prestar el servicio por parte del CONTRATISTA:

2.10.4. Cobertura

El servicio de soporte especializado está enfocado a administrar y soportar la totalidad de los elementos asociados a la infraestructura central de TI de la entidad que se encuentre alojada en los centros de datos suministrados por el CONTRATISTA.

Todos los servicios y aplicaciones habilitados en el Datacenter, para gestión o consulta, deben poder ser accedidos por los funcionarios de la entidad a través de la conectividad LAN/WLAN en las sedes y la WAN que interconecta dichas sedes, garantizando la continuidad de la operación de la entidad sobre los aplicativos y plataformas de gestión.

2.10.5. Horario

Este servicio debe estar disponible y en operación en modalidad 7x24x365, para el Datacenter Principal y Alterno

2.10.6. Línea base

Las cantidades y distribución de los equipos en las sedes de la entidad se establecen en el documento **UNP – Anexo Inventario - Distribución de Equipos**

2.11. Entregables para Datacenter y Datacenter Alterno/DRP

- Informe Inicial de cumplimiento de características técnicas del Datacenter Principal y Alterno para la prestación del servicio garantizando el cumplimiento de los requerimientos del presente proceso, el cual debe ser aprobado por la supervisión del contrato.
- Informe de Gestión Mensual del funcionamiento del Servicio de Datacenter Principal, garantizando el cumplimiento de los requerimientos del presente proceso
- Informe de Gestión Mensual del funcionamiento del Servicio de Datacenter Alterno, garantizando el cumplimiento de los requerimientos del presente proceso
- Informe de cumplimiento de ANS

3. CONECTIVIDAD DATA CENTER PRINCIPAL Y ALTERNO.

La entidad requiere contar con el servicio de conectividad de datos que permita la conexión entre el Datacenter principal y alterno para Replicación.

3.1. Objetivo

Proveer los servicios de conectividad de datos que permitan la interconexión entre el Datacenter Principal y el Datacenter Alterno, incluyendo Cross Conexiones y todos los componentes necesarios para el funcionamiento integral de la solución ofertada. Este servicio incluye la administración proactiva y gestión de las plataformas de visibilidad de red y optimización de tráfico con las que cuenta la entidad.

3.2. Condiciones y necesidades del servicio

A continuación, se plantean las condiciones bajo las cuales se debe prestar el servicio por parte del CONTRATISTA:

Conectividad

- La conectividad entre los dos Datacenter (principal y alterno) para la réplica, cuya capacidad debe ser dimensionada por el CONTRATISTA para dar cumplimiento al RTO y RPO exigido en el proceso. De todas formas, el ancho de banda de este canal debe ser mínimo de 1Gbps.
- Bajo el entendido que el Data Center será el punto principal de concentración de las sedes de la entidad, es responsabilidad del CONTRATISTA permitir el ingreso y acceso en los Datacenter del(los) canal(es) de datos de concentración de las sedes del operador de la red actual de la entidad.
- Es responsabilidad del CONTRATISTA la(s) Cross Conexiones con el actual proveedor de la red de datos de la entidad.
- Para el respectivo dimensionamiento, el canal de concentración de la red de datos de la entidad es de 1Gbps.
- Bajo el entendido que el canal de internet de la entidad actualmente se tiene con el actual proveedor, es responsabilidad del CONTRATISTA permitir el ingreso y acceso en los Datacenter de los canales de internet de la entidad.
- Es responsabilidad del CONTRATISTA las Cross Conexiones con el actual proveedor para los canales de internet de la entidad.
- Para el respectivo dimensionamiento, el canal de internet de la entidad es de 1Gbps (en Datacenter principal) y 500Mbps (en Datacenter Alterno).
- Todos los canales de la entidad actualmente cuentan con principal y alterno.
- El CONTRATISTA deberá garantizar la disponibilidad y el correcto funcionamiento de las plataformas de visibilidad y optimización de red. Anexo **UNP – Anexo Inventario - Distribución de Equipos** y **UNP - Anexo de Licenciamiento**
- Es responsabilidad total del CONTRATISTA la actualización de Firmwares, parches de seguridad y versiones de software de las plataformas, previa validación en ambientes de prueba y bajo gestión de cambios.
- El contratista deberá Implementar técnicas de filtrado inteligente en la plataforma de visibilidad para garantizar que las herramientas de análisis reciban únicamente tráfico relevante y optimizado
- Asegurar la correcta integración de las métricas de las plataformas, garantizando que los indicadores más críticos sean visibles de forma permanente.

Consideraciones adicionales

- El CONTRATISTA deberá adjuntar diagrama topológico y certificación del CONTRATISTA o del operador que este integre, suscrita por el respectivo Representante Legal
- El CONTRATISTA deberá suministrar un Sistema de Visualización Crítica y garantizar que los indicadores más críticos sean visibles de forma permanente.

3.3. Condiciones generales

A continuación, se plantean las condiciones bajo las cuales se debe prestar el servicio por parte del CONTRATISTA:

Las características y cantidades de los canales de internet requeridos se deben garantizar para lo descrito en el numeral anterior.

3.4. Cobertura

La totalidad de la conectividad que soporte los servicios centrales deben estar habilitados dentro del Datacenter Principal y Datacenter Alterno suministrado por el CONTRATISTA.

Todos los servicios y aplicaciones habilitados en el Datacenter, para gestión o consulta, deben poder ser accedidos por los funcionarios de la entidad a través de la conectividad LAN/WLAN en las sedes y la WAN que interconecta dichas sedes, garantizando la continuidad de la operación de la entidad sobre los aplicativos y plataformas de gestión.

3.5. Horario

Este servicio debe estar disponible y en operación en modalidad 7x24x365.

3.6. Entregables de Conectividad

- Dentro del informe mensual el contratista adjuntará la evidencia del uso del canal de conectividad.
- Dentro del informe mensual el contratista adjuntará evidencia del software de replicación que valide el uso del canal de conectividad.
- Dentro del informe mensual el contratista adjuntará evidencia del volumen de tráfico procesado y porcentaje de tráfico duplicado (eficiencia de herramientas) de las plataformas de visibilidad de red y optimización de tráfico

4. SEGURIDAD DE LA INFORMACIÓN

4.1. Objetivo

Proveer el servicio de seguridad de la información a fin de anticiparse a situaciones que puedan comprometer los servicios de TI que soportan la operación misional de la entidad.

4.2. Condiciones y necesidades del servicio

A continuación, se plantean las condiciones bajo las cuales se debe prestar el servicio por parte del CONTRATISTA:

- El servicio de Internet dedicado y concentrado en el Datacenter principal de la Entidad deberá contar con una solución centralizada de seguridad perimetral con componentes

como Intrusion Prevention System (IPS), Web Filtering, WAF, Balanceo y anti DDoS como mínimo.

- La seguridad perimetral deberá estar configurada en alta disponibilidad (HA) con equipo(s) central(es) en el Datacenter que cumplan con este propósito y un segundo equipo en el Datacenter alterno que se use dentro de la infraestructura que actualmente esta implementada por el cliente y que hace parte de sus activos tecnológicos
- Herramientas adicionales que alimenten las plataformas de ciberseguridad, en este caso el Security Operation System (SOC) podrán ir en dicho Datacenter dependiendo de la funcionalidad que se requiera y/o la ubicación de los equipos (servidores físicos y virtuales), a saber: Sandbox, CASB, Email Seguro, WAF, NAC, EDR/XDR.
- Si bien es cierto el componente de seguridad será en modalidad de servicio, EL CONTRATISTA se compromete a documentar con base en las mejores prácticas cada uno de los eventos e incidente de ciberseguridad a que esté expuesta la Entidad, preferiblemente de manera predictiva (antes de que ocurran), así como realizar la ingeniería forense en caso de un ataque que se presente.
- Definir unos Informes Gerenciales periódicos que deberán ser socializados con la Entidad y unos con Ingeniería de Detalle que el CISO y/o Supervisor de la Entidad pudiese requerir.
- Se deberá tener una base de datos de conocimiento con los eventos que se presenten a diario, basado en las mejores prácticas (NIST, ISO:27001, HIPPA, etc)
- El servicio deberá contar con la anticipación y respuesta de amenazas cibernéticas que contemple los siguientes componentes

Servicio de anticipación y respuestas a amenazas cibernéticas

El CONTRATISTA prestara el servicio técnico especializado orientado principalmente a la anticipación de amenazas cibernéticas en entornos TI y nube, diseñado para reducir de forma continua la probabilidad de compromiso mediante un ciclo integral de visibilidad, análisis y acción preventiva. El servicio integra la identificación temprana de exposición y vulnerabilidades, la producción de inteligencia accionable alineada al contexto de la organización, la detección proactiva de indicios de ataque y la transformación de hallazgos en medidas preventivas trazables, priorizadas por riesgo.

Su valor agregado se fundamenta en convertir la seguridad en una capacidad anticipativa y operable: no se limita a generar reportes aislados, sino que consolida un backlog técnico priorizado, emite alertas oportunas ante campañas o señales relevantes, fortalece la postura defensiva con recomendaciones basadas en evidencia, y retroalimenta continuamente la mejora de controles y procedimientos para disminuir rutas de ataque y reducir la recurrencia de incidentes. opera bajo una metodología oficial registrada, asegurando consistencia técnica, trazabilidad y repetibilidad en la identificación, priorización y tratamiento preventivo del riesgo cibernético.

Capacidades Técnicas

Componente A — Gestión de Exposición y Vulnerabilidades (externo + interno)

- Identificación y mantenimiento del inventario de activos y servicios dentro del alcance, incluyendo exposición relevante en nube.
- Evaluación técnica de exposición y detección de vulnerabilidades en superficie externa e interna.
- Identificación de configuraciones inseguras, componentes desactualizados y condiciones que habiliten rutas de ataque.
- Normalización y priorización de hallazgos por riesgo (severidad técnica, criticidad del activo y probabilidad de explotación).
- Consolidación de backlog único de vulnerabilidades/exposición con trazabilidad de estado.
- Recomendaciones preventivas y correctivas priorizadas para ejecución por la entidad.
- Seguimiento y verificación técnica de mitigaciones aplicadas por la entidad (validación de cierres y métricas).

Componente B — Detección Proactiva, Investigación y Respuesta (Hunting + IR/Forense)

- Investigación proactiva orientada por hipótesis para detección temprana de indicios de ataque o compromiso.
- Recolección y análisis de evidencias disponibles (registros, eventos, artefactos) y correlación de señales.
- Clasificación de casos por severidad operacional (Crítica/Alta/Media/Baja) según evidencia e impacto potencial.
- Reconstrucción técnica de actividad: alcance, vectores, rutas de persistencia o movimiento.
- Emisión de acciones de contención y mitigación recomendadas para ejecución por la entidad.
- Preservación y documentación de evidencia técnica para trazabilidad y análisis posterior.
- Documentación formal de casos y lecciones aprendidas con recomendaciones preventivas.

Componente C — Inteligencia y Análisis de Amenazas (Threat Intel + APT + Malware)

- Recolección y curación de información de amenazas priorizando aplicabilidad al contexto TI y nube de la entidad.
- Análisis y contextualización de amenazas, campañas, tendencias, tácticas y potencial impacto.
- Producción de inteligencia accionable para priorización de exposición, fortalecimiento preventivo y apoyo a detección.
- Emisión de alertas oportunas ante campañas o riesgos relevantes (cuando ocurra), con guía de acción inmediata.
- Análisis técnico especializado de evidencias/artefactos (correos, URLs, muestras o indicadores) para extraer patrones e indicadores.
- Retroalimentación al ciclo de anticipación: insumos para priorización de vulnerabilidades y focos de hunting.

Componente D — Riesgo Digital y Exposición de Datos (filtraciones/credenciales)

- Monitoreo recurrente de señales de exposición de datos y credenciales asociadas a la entidad en fuentes abiertas y entornos de riesgo.
- Triage y validación técnica de exposiciones (autenticidad, vigencia, alcance probable y riesgo).
- Priorización por severidad operacional según impacto potencial y probabilidad de abuso.
- Alertamiento y recomendaciones de contención (por ejemplo: rotación, revisión de accesos, verificación de abuso).
- Seguimiento y trazabilidad de casos, con retroalimentación hacia hunting, vulnerabilidades y mejora continua.

Componente E — Fortalecimiento Continuo (mejora + capacitación bajo demanda)

- Consolidación de hallazgos recurrentes y patrones derivados de vulnerabilidades, exposición, incidentes y causas.
- Priorización de acciones de mejora por riesgo y por impacto preventivo en TI y nube.
- Definición de planes de mejora con recomendaciones y ruta de implementación para ejecución por la entidad.
- Acompañamiento técnico para validación de reducción de riesgo tras acciones implementadas por la entidad.
- Capacitaciones y sensibilización bajo demanda, alineadas a brechas observadas y necesidades del cliente.

Entregables del Servicio

Componente A — Gestión de Exposición y Vulnerabilidades (externo + interno)

- Matriz de priorización y backlog de remediación: listado trazable de hallazgos con criticidad, prioridad, responsable asignable por la entidad y estado.
- Alertas de exposición crítica (cuando ocurra): notificación de hallazgos críticos que requieran atención inmediata, con guía técnica de mitigación recomendada.

Componente B — Detección Proactiva, Investigación y Respuesta (Hunting + IR/Forense)

- Reporte técnico de Hunting e Investigación (cuando aplique): hipótesis, evidencias analizadas, hallazgos, conclusiones y recomendaciones.
- Reporte técnico de Respuesta a Incidentes (cuando aplique): cronología, alcance, evidencias, acciones recomendadas, estado de contención y conclusiones.
- Informe de lecciones aprendidas y medidas preventivas (por caso o consolidado mensual): causas probables, brechas observadas y acciones de prevención priorizadas.

Componente C — Inteligencia y Análisis de Amenazas (Threat Intel + APT + Malware)

- Boletín semanal de inteligencia de amenazas: campañas relevantes, tendencias aplicables, alertas contextualizadas y recomendaciones.

- Informe mensual de inteligencia y tendencias: análisis consolidado, evolución del panorama, riesgos prioritarios y líneas de acción preventivas.
- Alertas de amenazas/campañas relevantes (cuando ocurra): aviso inmediato con indicadores y acciones recomendadas.
- Reporte técnico de análisis de artefactos/evidencias (cuando aplique): conclusiones técnicas, indicadores extraídos y recomendaciones de protección/detección.

Componente D — Riesgo Digital y Exposición de Datos (filtraciones/credenciales)

- Alertas de exposición de datos/credenciales (cuando ocurra): detalle del caso, criticidad, recomendaciones de contención y verificación.
- Informe mensual de riesgo digital y exposición de datos: casos relevantes, estado de seguimiento, tendencias y acciones recomendadas.
- Registro trazable de casos de exposición: consolidado con estado, fecha de detección, criticidad, acciones recomendadas y cierre.

Componente E — Fortalecimiento Continuo (mejora + capacitación bajo demanda)

- Informe mensual de mejora continua: tendencias de hallazgos, brechas recurrentes, plan de acción priorizado y estado de avance.
- Plan de mejora preventiva (actualizable): recomendaciones estructuradas, prioridades y criterios de verificación (para ejecución por la entidad).
- Acta y material de capacitación (cuando aplique): objetivos, contenidos impartidos, conclusiones y recomendaciones asociadas.

Consideraciones adicionales

- El CONTRATISTA deberá tener personal con la formación, certificaciones y experiencia idónea para prestar los servicios que le escalen desde las plataformas de Mesa de Servicios, NOC, SOC y que por supuesto, comprometan la seguridad informática de la Entidad.
- El CONTRATISTA podrá tener a dichos especialistas en modalidad remota o presencial dependiendo las necesidades de la Entidad, siempre y cuando se cumplan con los ANS de rigor y que no se comprometa la integridad de los flujos de información.

Para el caso de Seguridad de la Información EL CONTRATISTA deberá:

El CONTRATISTA mediante el gestor integral de riesgos SGSI, en el marco de su perfil deberá garantizar que se realicen las actividades de mantenimiento y monitoreo del Sistema de Gestión de Seguridad de la Información según la Norma ISO 27001 y de implementación de los lineamientos de la política de gobierno digital de conformidad con la regulación vigente.

Actividades principales para desarrollar:

- Gestionar mantenimiento y monitoreo del Sistema de Gestión de Seguridad de la Información en articulación con los procesos de la Entidad, conforme a los lineamientos

gubernamentales, Norma ISO 27001, demás normativas legales vigentes y lineamientos institucionales en la materia.

- Identificar, documentar y realizar seguimiento a las acciones correctivas y oportunidades de mejora (ACOM), en el marco de la mejora continua del Sistema de Gestión de Seguridad de la Información.
- Participar colaborativamente en el equipo técnico de apoyo al Sistema de Gestión de Seguridad de la Información.
- Junto con la entidad gestiona la elaboración, revisión, consolidación y presentación del informe de revisión por la dirección en lo relacionado con el Sistema de Gestión de Seguridad de la Información, según los lineamientos institucionales en la materia.
- Acompañar la planeación y ejecución de auditorías internas del Sistema de Gestión de Seguridad de la Información, así como la elaboración de informes y presentación de resultados.
- Realizar y coordinar con los procesos de la Entidad la identificación, análisis, valoración y monitoreo de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías vigentes en la materia, elaborando los informes correspondientes.
- Apoyar a los procesos de la entidad cuando se detecten irregularidades, incidentes o prácticas que atenten contra la seguridad y privacidad de la información de acuerdo con la normativa vigente, con el fin de atender rápidamente este tipo de eventualidades.
- Definir e implementar en coordinación con los procesos de la entidad, las estrategias de sensibilización y divulgación en temas de gobierno digital y seguridad y privacidad de la información para servidores públicos y contratistas, documentando los resultados alcanzados.
- Apoyar la actualización de la Política de Gobierno Digital en consonancia con el (Decreto 767 de 2022), la normativa del Ministerio de Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de la Función Pública.
- Participar en el ejercicio de autodiagnóstico y Medición de Desempeño Institucional (FURAG), en las políticas asociadas al proceso de gestión tecnológica, implementado los procesos de mejora generados en concordancia con los resultados alcanzados.
- En conjunto con la entidad, formular, actualizar, implementar y realizar el seguimiento de los planes e indicadores del proceso de gestión tecnológica en el marco de la seguridad de la información.
- Elaborar el informe de monitoreo de segunda línea de los riesgos de seguridad y privacidad de la Información y demás documentos técnicos relacionados con la materia cuando el supervisor lo requiera.

4.3. Condiciones generales

A continuación, se plantean las condiciones bajo las cuales se debe prestar el servicio por parte del CONTRATISTA:

- Los agentes de SOC podrán operar de manera remota, así como los especialistas siempre y cuando no haya afectaciones a la continuidad del servicio y se cumplan los ANS.
- La Entidad entregara inventario actualizado de los elementos que son de su propiedad y que deben ser administrados de tal manera que EL CONTRATISTA haga uso de ellos en aras de no generar detrimento patrimonial a no ser que dichos elementos (hardware, software, licenciamiento), no puedan o deban ser usados por vencimiento, vetustez, soporte de fabricante, incompatibilidades con lo actual, u obsolescencia tecnológica entre otros.
- El CONTRATISTA en la etapa inicial y en la fase de empalme con los proveedores actuales deberá corroborar la información de inventarios detallados existente en la Entidad.
- Se realizará un entregable a la Entidad con los hallazgos evidenciados en los análisis de vulnerabilidades y Ethical Hacking aplicadas a manera de consultoría según metodología GAP de Seguridad con el fin de poder realizar ajustes a las herramientas de ciberseguridad con que contará la Entidad.
- El CONTRATISTA se compromete a realizar labores de Análisis de Vulnerabilidades y Ethical Hacking de acuerdo con el alcance del componente A y se deberá se entregara un reporte técnico y/o ejecutivo de los hallazgos.

4.3.1. Alcance del servicio (Descripción general de CSOC)

El contratista deberá garantizar la protección integral de los sistemas y datos críticos de la entidad, asegurando el cumplimiento de estándares internacionales de ciberseguridad como ISO/IEC 27001, NIST 800-61, MITRE ATT&CK y CIS Controls, así como el fortalecimiento de las capacidades institucionales para la anticipación y respuesta efectiva ante ciber amenazas.
El contratista deberá garantizar la ejecución de los siguientes procesos fundamentales:

- Monitoreo y administración de la infraestructura de seguridad
- Gestión de eventos e incidentes de ciberseguridad
- Automatización de respuesta con FortiSOAR
- Optimización y mantenimiento de sistemas de seguridad existentes
- Generación de reportes estratégicos y operativos.

4.3.2. Plataformas de Administración del CSOC

El CONTRATISTA será responsable de la administración del CSOC, monitoreo y operación de las tecnologías de seguridad implementadas en la entidad según **UNP - Anexo Inventario - Distribución de Equipos y UNP - Anexo de Licenciamiento:**

Para la Solución integral que recopila, analiza y correlaciona eventos de seguridad de toda la infraestructura de TI (dispositivos, redes, servidores, aplicaciones) para detectar amenazas, automatizar respuestas a incidentes y facilitar el cumplimiento normativo, Se solicita contemplar el siguiente dimensionamiento mínimo:
Número de dispositivos licenciados: 150
Eventos por segundo (EPS): 1000

El CONTRATISTA es responsable de la renovación del soporte y garantía de hardware, software y/o licenciamiento de las herramientas de seguridad con que cuenta la entidad, que se referencian en el anexo **UNP - Anexo de Licenciamiento**

4.3.3. Respuesta a Incidentes de Seguridad

Activación Inmediata de Protocolos de Respuesta a Incidentes

1. Detección y Notificación
2. Contención y Aislamiento
3. Análisis y Evaluación del Impacto
4. Erradicación y Remediación
5. Recuperación y Lecciones Aprendidas

- El contratista deberá contar con un Sistema de Gestión de Incidentes integrado con FortiSIEM para registrar, rastrear y escalar eventos de seguridad en tiempo real.
- El contratista deberá adecuarse a las políticas de incidentes de seguridad de la información que tiene la entidad.

Análisis Forense Detallado

Mitigación de Incidentes con Automatización mediante FortiSOAR

- Bloqueo inmediato de direcciones IP maliciosas
- Desactivación automática de cuentas comprometidas
- Aplicación de reglas de firewall y segmentación de tráfico
- Integración con herramientas de Threat Intelligence

- El contratista deberá diseñar una biblioteca de playbooks automatizados para la contención de amenazas recurrentes, reduciendo la necesidad de intervención manual en incidentes de baja y media criticidad.

Reportes Detallados y Asesoría Post-Incidente

- El contratista deberá generar informes detallados de cada incidente de seguridad gestionado, que incluyan:
  - Descripción del incidente y activos afectados.
  - Línea de tiempo detallada del ataque.
  - Medidas adoptadas para la mitigación.
  - Acciones recomendadas para prevenir incidentes similares en el futuro.

4.3.4. Mejora Continua de Seguridad

El futuro contratista del CSOC de la UNP deberá gestionar un proceso de mejora continua en ciberseguridad, asegurando que la infraestructura y las estrategias de protección evolucionen de manera constante en respuesta a amenazas emergentes y cambios en el entorno tecnológico. Este

proceso incluirá auditorías de seguridad, análisis de brechas, optimización de configuraciones y ajustes estratégicos basados en el análisis de amenazas identificadas.

4.3.5. Administración de Plataformas de Seguridad de Usuarios, Web y BD

El contratista del CSOC de la UNP será responsable de la gestión, monitoreo y mantenimiento continuo de la infraestructura de ciberseguridad implementada en la entidad. Este proceso garantizará la correcta operación, disponibilidad y actualización de los dispositivos y plataformas de seguridad, asegurando una protección efectiva contra amenazas cibernéticas y optimizando el desempeño de los sistemas.

4.3.6. Gestión y Monitoreo de Dispositivos de Seguridad

- El contratante deberá implementar monitoreo continuo 24/7 sobre los dispositivos y plataformas de seguridad, asegurando su disponibilidad y correcta configuración.

Tiempos de Respuesta

El futuro contratista deberá garantizar que el CSOC deberá atender y gestionar incidentes de seguridad dentro de los tiempos de respuesta definidos según su severidad, asegurando una contención y mitigación efectiva de las amenazas.

Severidad	Tiempo de Respuesta
Crítica	30 minutos
Alta	1 hora
Media	4 horas
Baja	8 horas

- Incidentes Críticos: Eventos que comprometen la continuidad operativa de la UNP, como ataques de ransomware, filtraciones de datos o intrusiones activas en la infraestructura.
- Incidentes Altos: Amenazas con impacto significativo en la seguridad, pero que aún no afectan la operatividad total.
- Incidentes Medios: Vulnerabilidades explotables o anomalías que requieren atención para evitar un impacto futuro.
- Incidentes Bajos: Eventos de seguridad con impacto mínimo, pero que deben ser atendidos para prevenir incidentes mayores.

4.3.7. Disponibilidad del Servicio

El CSOC deberá operar bajo un esquema de alta disponibilidad, asegurando la continuidad de los servicios de monitoreo, detección y respuesta ante incidentes.

- Plazo máximo de recuperación de servicios: 8 horas en caso de fallos críticos en la infraestructura del SOC.

4.4. Cobertura

La totalidad de la infraestructura que soporte los servicios centrales deben está habilitados dentro del Datacenter suministrado por el CONTRATISTA, teniendo en cuenta:

- La plataforma de seguridad de la información considerando a los componentes de hardware y software que la integran.

Todos los servicios y aplicaciones habilitados en el Datacenter, para gestión o consulta, deben poder ser accedidos por los funcionarios de la entidad a través de la conectividad LAN/WLAN en las sedes y la WAN que interconecta dichas sedes, garantizando la continuidad de la operación de la entidad sobre los aplicativos y plataformas de gestión.

4.5. Horario

Este servicio debe estar disponible y en operación en modalidad 7x24x365.

4.6. Línea base

Las cantidades y distribución de los equipos en las sedes de la entidad se establecen en el anexo **UNP – Anexo Inventario - Distribución de Equipos**

4.7. Entregables Seguridad de la Información

- Informe de Gestión Mensual de la ejecución de los servicios de seguridad de información, garantizando el cumplimiento de los requerimientos del presente proceso
- Informe de Gestión Mensual de Respuesta a Incidentes
- Informe de Gestión Mensual de Reporte de Análisis Forense (En caso de aplicar)
- Informe de Gestión Mensual de Alertas y Notificaciones de Incidentes en Tiempo Real (En caso de aplicar)
- Informe de Gestión Mensual de Matriz de Automatización de Respuesta
- Informe de Gestión Mensual de Tendencias de Incidentes
- Informe de Gestión Mensual de Simulaciones de Ataques de Phishing y Vishing (En caso de aplicar

5. LICENCIAMIENTO

5.1. Objetivo

El contratista es responsable del licenciamiento de hypervisor, sistemas operativos, bases de datos, aplicaciones y otros en el Datacenter Principal. Para el Datacenter alterno el CONTRATISTA debe Proveer el licenciamiento base de datos MS SQL, sistemas operativos, hypervisor en el caso de virtualización para garantizar el escenario de Datacenter Alterno/DRP solicitado en el numeral correspondiente.

5.2. Condiciones y necesidades del servicio

A continuación, se plantean las condiciones bajo las cuales se debe prestar el servicio por parte del CONTRATISTA:

- Proveer licenciamiento de base de datos MS SQL, Sistemas operativos Windows y Linux que hagan parte del diseño del Datacenter alterno.
- Proveer el licenciamiento de Software de la herramienta de réplica de datos que garanticen el RPO y RTO solicitado por la entidad.
- Proveer el licenciamiento de uso y/o soporte anual de acuerdo al anexo **UNP – Anexo de Licenciamiento** el cual hace parte integral del presente documento:
- Efectuar el entendimiento del alcance asociados a los sistemas de información que se encuentran operando en la entidad, lo anterior que se presten los servicios asociados a mantener operativos dichos sistemas de información, incluyendo costos de licenciamiento (cuando aplique), contratos de soporte y personal que los gestione.

Consideraciones adicionales

- El licenciamiento propuesto para el Datacenter alterno debe contar con la vigencia del contrato.

5.3. Condiciones generales

A continuación, se plantean las condiciones bajo las cuales se debe prestar el servicio por parte del CONTRATISTA:

Las características y cantidades de Licenciamiento (SO-BD) se debe garantizar para lo descrito en el capítulo de Datacenter principal y alterno.

5.4. Cobertura

La totalidad de la infraestructura que soporte los servicios centrales deben está habilitados dentro del Datacenter suministrado por el CONTRATISTA.

Todos los servicios y aplicaciones habilitados en el Datacenter, para gestión o consulta, deben poder ser accedidos por los funcionarios de la entidad a través de la conectividad LAN/WLAN en las sedes y la WAN que interconecta dichas sedes, garantizando la continuidad de la operación de la entidad sobre los aplicativos y plataformas de gestión.

5.5. Horario

Este servicio debe estar disponible y en operación en modalidad 7x24x365.

5.6. Línea base

Las características y cantidades de Licenciamiento (SO-BD) se debe garantizar para lo descrito en el capítulo de Datacenter principal y alterno.

5.7. Entregables de Licenciamiento

- Dentro del informe mensual el contratista presentará el estado de las licencias para ese periodo y adjuntara la evidencia de la entrega del licenciamiento si a ello hubo lugar. Este informe se debe mantener actualizado durante la vigencia del contrato.

OSCAR ANDRES CASAS GOMEZ
Estructurador Técnico
Oficina de tecnologías y sistemas de información