FICHA TÉCNICA SOPORTE DATACENTER

FICHA TECNICA - ESPECIFICACIONES TÉCNICAS MÍNIMAS

LAS SIGUIENTES SON LAS ESPECIFICACIONES TÉCNICAS MÍNIMAS, LAS CUALES SE ENTENDERÁN ACEPTADAS CON LA SUSCRIPCIÓN DEL CONTRATO Y SERÁN DE OBLIGATORIO CUMPLIMIENTO PARA EL CONTRATISTA.

A. ESPECIFICACIONES TÉCNICAS MÍNIMAS

El contratista debe comprometerse a entregar los servicios adquiridos y atender los requerimientos de soporte técnico tal y como se describe en las tablas siguientes, indicando para ello en la oferta que conoce y se obliga con su firma a entregar los servicios y cumplir con las características de los mismos y soporte técnico de la mesa de ayuda del centro de datos según se discrimina a continuación. **Los costos que tengan estas actividades deben estar previstos en la oferta y no generarán costo adicional para la PGN**.

ITEM 1: Balanceador de Carga Baja Capacidad

Este servicio debe contemplar dos (2) appliances virtuales de balanceador de cargas dedicados para la PGN (No se aceptan plataformas compartidas) los cuales permiten distribuir las cargas de trabajo locales en varios recursos diferentes como servidores de procesamiento, unidades de almacenamiento, entre otros alojado en la infraestructura del proveedor. El balanceador de carga tiene como objetivo optimizar el uso de recursos, maximizar el rendimiento, minimizar el tiempo de respuesta y evitar la sobrecarga de cualquier recurso contratado. Finalmente, la infraestructura para los balanceadores será suministrada por la entidad designada por la Corporación designada por la Corporación.

- ✓ Debe llevar a cabo la función de balanceo de carga utilizando mínimo 4 de los siguientes métodos: Random, Round robin, Sticky sessions, Weighted round robin, Fastest, Least connections, Least response time, otros.
- ✓ Balanceo de carga en capa L4 y L7, servicio de sandboxing
- ✓ Debe soportar VMware vSphere ESXi 6,0 y superior
- ✓ Distribución de carga que a través de la capa L4 el equipo puede soportar de 10 Gbps.
- ✓ Diez (10) dominios virtuales
- ✓ Ocho (8) vCPU
- ✓ Memoria RAM de 16 GB
- ✓ Ocho (8) interfaces de red
- ✓ El servicio debe soportar el uso de las versiones IPv4 e IPv6 del protocolo de Internet
- ✓ Debe permitir el filtrado de direcciones IP y permitir/bloquear listas de control de acceso
- ✓ Interfaz de gestión y automatización del balanceador se debe poder integrar nativamente con el FortiManager con que cuenta la entidad designada por la Corporación designada por la Corporación como única herramienta de administración de la arquitectura de seguridad de la entidad designada por la Corporación designada por la Corporación
- ✓ Debe poder integrarse con el reporteador de eventos FortiAnalizer 1000 con que cuenta la entidad designada por la Corporación para la generación de reportes del equipo.

FICHA TÉCNICA SOPORTE DATACENTER

ITEM 2: Firewall Nueva Generación - Media Alta Capacidad

Dos (2) appliances físicos de propósito específico para firewall de nueva generación dedicados para la PGN (No se aceptan plataformas compartidas) que ofrece el rol de protección bloqueando y/o permitiendo el acceso a diferentes recursos de red, ejerciendo así una política de seguridad sobre la red (ejemplo: intrusion, sql injection entre otros).

- ✓ Rendimiento del appliance virtual en rol de Firewall de 158 Gbps
- ✓ Rendimiento Threat Protection Throughput 11 Gbps
- ✓ Soporte hasta 2 TB de almacenamiento
- ✓ Mínimo 10 dominios virtuales
- ✓ Soporte hasta 200.000 políticas
- ✓ Debe contar con funcionalidades de: Firewall, VPN (IPSEC y SSL), Antivirus, IPS/IDS, Filtrado Web, AntiSpyware, Control de aplicaciones, inspección de contenido en SSL.
- ✓ Interfaz de gestión y automatización del NGFW se debe poder integrar nativamente con el FortiManager con que cuenta la entidad designada por la Corporación designada por la Corporación como herramienta de administración de la arquitectura de seguridad de la entidad designada por la Corporación designada por la Corporación. La administración de los equipos será compartida.
- ✓ Debe poder integrarse con el reporteador de eventos FortiAnalizer 1000 con que cuenta la entidad designada por la Corporación designada por la Corporación para la generación de reportes del equipo.

ITEM 3: Monitoreo y Correlación

Debe permitir a la PGN adquirir el servicio de monitoreo de eventos o bitácoras de logs y correlación de eventos de diferentes sistemas de cada entidad designada por la Corporación designada por la Corporación incluyendo soluciones de seguridad, sistemas operativos, aplicaciones, equipos de red, directorios de identidad designada por la Corporación, bases de datos, repositorios de datos y hosts. Dicho servicio debe ser dedicado para la PGN (No se aceptan plataformas compartidas). Cabe resaltar que la correlación se debe realizar a eventos de red, seguridad e infraestructura con una herramienta que soporte hasta 2.000 eventos por segundo que se deben configurar al inicio del contrato y basados en el inventario que suministre la entidad designada por la Corporación designada por la Corporación respecto a equipos de seguridad, de red y máquinas virtuales. Finalmente, dicho servicio será configurado por el proveedor y será insumo para el SOC/NOC de la entidad designada por la Corporación.

- ✓ El proveedor deberá contar con una solución que soporte el servicio de monitoreo con conectores o agentes para la extracción por defecto de dispositivos de red, seguridad, bases de datos, soluciones de nube como Azure u otros, sistemas operativos Windows, Linux, u otros. El servicio debe contar como alcance 2.000 eventos por segundo configurables con la entidad designada por la Corporación designada por la Corporación al inicio del contrato.
- ✓ El equipo debe poder monitorear:
  - Comunicaciones:

FICHA TÉCNICA SOPORTE DATACENTER

- Disponibilidad de las comunicaciones en tiempo real.
- Supervisión del estado del dispositivo.
- Medición del flujo de tráfico.
- Datos de tráfico por puerto.
- Ancho de banda.
- Supervisión de equipos y dispositivos de red.
- Autodescubrimiento de los equipos de red.
- Relaciones y dependencias entre comunicaciones, infraestructura y aplicaciones.

- Infraestructura:
  - Disponibilidad y rendimiento de equipos (Almacenamiento, procesamiento y memoria).
  - Disponibilidad y rendimiento de sistemas operativos.
  - Autodescubrimiento de los equipos (comunicaciones (redes), procesamiento y almacenamiento).
  - Relaciones y dependencias entre comunicaciones, infraestructura y aplicaciones.
  - File Integreting Monitoring (FIM)
  - Otras que no estén al alcance del software de monitoreo de la entidad designada por la Corporación designada por la Corporación.

- Aplicaciones:
  - Rendimiento de las aplicaciones.
  - Relaciones y dependencias entre comunicaciones, infraestructura y aplicaciones.
  - Disponibilidad para los usuarios en cualquier ubicación.
  - Estado de la sesión.
  - Estado de las transacciones de aplicaciones en entornos tradicionales, virtualizados y de nube.
  - Simulación de transacciones para predicción de mediciones (emula la experiencia del usuario final para evaluar el rendimiento de las aplicaciones desde diferentes perspectivas de clientes).
  - Transacciones sintéticas.
  - Otras que no estén al alcance del software de monitoreo de la entidad designada por la Corporación designada por la Corporación.

✓ Finalmente, la entidad designada por la Corporación designada por la Corporación a través de su SOC/NOC requiere tener visibilidad en línea del monitoreo de eventos de seguridad, infraestructura y red.

✓ La solución que soporte el servicio deberá contar con una base de datos, tienda online o repositorio de casos de uso, reglas de correlación, casos de ataque o comportamiento de amenazas predefinidos, que permitan al proponente asignar estos casos a los equipos de cada entidad designada por la Corporación designada por la Corporación al inicio de cada servicio, de esta forma contar con identificación temprana de incidentes, sin requerir configurar de forma manual cada caso de uso.

FICHA TÉCNICA SOPORTE DATACENTER

- ✓ Estos casos de uso deben ser actualizados periódicamente por el fabricante de la solución SIEM y ser aplicados al servicio por el proveedor.

- ✓ El proveedor debe garantizar la habilitación de todo lo necesario para permitir el monitoreo detallado de todos los servicios solicitados por la entidad designada por la Corporación designada por la Corporación.

- ✓ El proveedor debe asegurar que estén iniciados los servicios que se requieran de acuerdo con el sistema operativo que se vaya a monitorear.

- ✓ El proveedor debe tener habilitado el agente SNMP v3.

- ✓ El proveedor debe asegurar la apertura bidireccional para los puertos necesarios entre los servicios a monitorear y los servidores de monitoreo.

- ✓ Los agentes habilitados NO deben degradar el funcionamiento de los equipos, aplicaciones y redes a monitorear.

- ✓ La instalación de los agentes será realizada por el proveedor del servicio de colocation.

- ✓ El servicio deberá alertar los incidentes de seguridad, red e infraestructura a la entidad designada por la Corporación designada por la Corporación cuando se presenten amenazas de alta criticidad, ataques detectados, comportamientos sospechosos críticos de acuerdo con lo establecido en las condiciones transversales al SOC/NOC de la entidad designada por la Corporación designada por la Corporación.

- ✓ Frecuencia de medición del servicio en tiempo real.

- ✓ El servicio debe estar basado en una herramienta de SIEM (Security Information and Event Management) empresarial de 2.000 eventos por segundo, licenciada no open source que no permita la modificación o eliminación del contenido de los eventos en reposo, esto con el objetivo de garantizar la integridad de los eventos en procesos forenses. esta herramienta deberá permitir realizar como mínimo los siguientes numerales:

    - Extracción de eventos y/o Logs
    - Parseo y normalización de eventos permitiendo contar con los eventos en un formato estructurado y constante que permita a los analistas rápida identificación información crítica.
    - Monitoreo en tiempo real de alertas de seguridad.
    - Correlación de eventos basado en casos de uso o reglas de correlación de ataques y amenazas conocidas y no conocidas.
    - Plataforma de análisis de eventos en tiempo real para investigación de incidentes.
    - Presentación de dahsboards de monitoreo consultables por las entidad designada por la Corporaciónes.
    - Retención de eventos de mínimo 3 meses

FICHA TÉCNICA SOPORTE DATACENTER

- ✓ El equipo debe estar en la capacidad de generar un reporte mensual incluyendo como mínimo los siguientes reportes:
    - Top de dispositivos con incidentes de seguridad (4 agentes por sistema operativo).
    - Top de ataques detectados en el ambiente it de la entidad designada por la Corporación designada por la Corporación
    - Top de usuarios con autenticaciones fallidas.
    - Informe de navegación sospechosa por usuario.
    - Reporte de riesgo e incidentes por entidad designada por la Corporación designada por la Corporación.
    - Reporte de alertas e incidentes recurrentes o de alta criticidad.
    - Debe contar con CMDB, Monitoreo de Transacciones sintéticas y agentes para Windows y Linux de FIM

- ✓ El proveedor de los servicios de colocation hará una presentación y entrega de informe relacionado.

- ✓ Debe poder integrarse nativamente con el reporteador de eventos FortiAnalizer 1000 con que cuenta la entidad designada por la Corporación para la generación de reportes del equipo.

- ✓ La entidad designada por la Corporación cuenta con su propia herramienta de monitoreo de infraestructura y de aplicaciones, la cual se debe seguir usando en las plataformas ubicadas en los rack que hacen parte del alcance. Igualmente cuenta con un servicio de SOC/NOC que debe utilizar los eventos generados que realiza el SIEM a nivel de File Integreting Monitoring (FIM) y transacciones sintéticas a nivel de aplicaciones.
- ✓ La entidad designada por la Corporación debe contar con el equipo correlacionador de eventos que sirva de insumo con los parámetros FIM y transacciones sintéticas para el NOC/SOC de la entidad designada por la Corporación, quienes a su vez utilizan el software de monitoreo con que cuenta la entidad designada por la Corporación y que seguirá instalado en la infraestructura.

ITEM 4: Servicios SASE (Secure Access Service Edge)

Funcionalidades Generales:

Se requiere de una solución (SaaS) del tipo Secure Service Edge (SSE) que proporcione visibilidad, cumplimiento, seguridad de datos y protección contra amenazas para servicios basados en la nube, con el objetivo de:

- ➢ Proveer capacidades de Secure Web Gateway y Firewall as a Service (FWaaS) para dispositivos con o sin agente.
- ➢ Permitir acceso granular por aplicación pudiéndose realizar dinámicamente un cambio critico de confianza implícita a explicita con el uso de ZTNA (Zero Trust Network Access).
- ➢ Brindar capacidades de Inspección SSL para el análisis de tráfico encriptado.

FICHA TÉCNICA SOPORTE DATACENTER

- Analizar el comportamiento de los usuarios para detectar comportamientos sospechosos o irregulares y generar alertas por comportamiento malicioso.
- Realizar análisis activo de detección de virus y malware.

Funcionalidades Especificas

- La solución debe estar licenciada para 5500 usuarios de la entidad designada por la Corporación.
- La solución debe permitir el uso de al menos dos dispositivos con o sin agente por usuario licenciado.
- Debe permitir la inspección de tráfico encriptado TLS v1.3
- La solución debe estar en capacidad de integrarse de manera nativa con los dispositivos de SD-WAN con los que cuenta la entidad designada por la Corporación para la implementación de una arquitectura single vendor SASE, de acuerdo con la definición de Gartner
- La solución debe estar en capacidad de proporcionar capacidades completas de seguridad en cada uno de sus puntos de presencia (PoPs), para hacer inspección completa del tráfico en línea de los usuarios sin tener que redirigirlo a otros sitios para su aseguramiento. Esto con el fin de ofrecer una experiencia óptima a los usuarios de la entidad designada por la Corporación.
- La solución debe soportar ser utilizada con agente o agentless.
- Debe brindar reconocimiento de al menos 200 aplicaciones.
- Debe poseer la capacidad de antivirus/antimalware en línea con soporte de sandbox cloud u on premise con integración nativa (teniendo en cuenta que la entidad designada por la Corporación cuenta con una plataforma en premisas para este fin).
- La solución debe proveer control de navegación a través del uso de categorización de sitios web, patrones específicos de URL y filtrado de contenido.
- Debe brindar protección de DNS a través del uso de categorías, así de patrones personalizados, también debe reconocer y bloquear conexiones a sitios de Bonet y C&C
- Debe proporcionar capacidades de Intrusion Prevention (IPS) para la detección y mitigación de ataques de red.
- Los servicios de seguridad suministrados por la plataforma deben ser de sus propios laboratorios de inteligencia de amenazas (no vía OEM), y validados por analistas independientes.
- Debe proveer capacidades de filtrado de archivos basados en el tipo
- Debe permitir la autenticación de usuarios de locales, así como remotos de Active Directory/LDAP, RADIUS y Azure AD

FICHA TÉCNICA SOPORTE DATACENTER

- La solución debe estar en capacidad de brindar protección antimalware directamente en el punto final, teniendo la capacidad de contener tráfico localmente, mejorando el consumo de ancho de banda.
- Debe brindar capacidades de escaneo de vulnerabilidades sobre los dispositivos finales, mediante el uso del agente de la solución.
- Debe soportar conectividad a través de túneles seguros automáticos, así como de navegador web.
- La solución debe integrarse de manera nativa con los Firewalls de Nueva Generación de la entidad designada por la Corporación, con el fin de dirigir de manera automática el tráfico hacia las aplicaciones residentes en los datacenters, mediante túneles automatizados directos sin pasar por el PoP de SSE, disminuyendo la latencia y retardo de procesamiento, al tiempo que se aplican las funcionalidades de seguridad y ZTNA en estos dispositivos. Esto al menos para tráfico basado en protocolos TCP.
- La solución debe proveer la capacidad de monitorear los siguientes parámetros de uso:

    - Orígenes de conexión
    - Destinos de conexión
    - Aplicaciones
    - Aplicaciones de nube
    - Sitios web
    - Uso de políticas
    - Sesiones
    - Amenazas

- La solución debe proveer la capacidad de generar reportes bajo demanda o programados tales como:

    - Reporte de amenazas
    - Reporte de uso Web
    - Eventos e incidentes de seguridad
    - Uso de ancho de banda de aplicaciones
    - Nivel de riesgo de aplicaciones

- Debe contar con integración nativa de la con la plataforma de logs de seguridad con la que cuenta la entidad designada por la Corporación (FortiAnalyzer) y la plataforma de SIEM de la entidad designada por la Corporación (FortiSIEM), plataformas actualmente en producción.
- Se debe contar con soporte del fabricante durante su implementación y por un año contado a partir de su entrega en producción.

Transferencia de Conocimiento

FICHA TÉCNICA SOPORTE DATACENTER

- El contratista debe ofrecer transferencia de conocimiento técnica, para diez (10) funcionarios de la entidad designada por la Corporación con una intensidad horaria de mínimo doce (12) horas, sobre la operación, administración y resolución de problemas de los servicios ofertados. Toda la transferencia de conocimiento debe estar soportada por su respectiva documentación.

Uso y apropiación

- El contratista deberá liderar y acompañar la campaña de uso y apropiación de la solución para así lograr una socialización que permita la usabilidad y concientización respecto al cambio de la tecnología.

Implementación

- El contratista deberá implementar la herramienta en un período máximo de cuatro (4) meses a partir de la firma del acta de inicio.
- Planeación de cada una de las actividades con el fin de cumplir con los tiempos de personalización del servicio.
- Presentar diseño de seguridad perimetral de acuerdo a buenas prácticas y recomendaciones del fabricante integrando los dispositivos de seguridad con los que actualmente cuenta la entidad designada por la Corporación, este será evaluado y aprobado por el supervisor de contrato.
- Presentar el diseño de Políticas de Seguridad para ser evaluado y aprobado por el líder de infraestructura y el supervisor del contrato.
- Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.
- Implementación de la solución de acuerdo a las mejores prácticas de los fabricantes, teniendo en cuenta una arquitectura de red segura.
- Pruebas de Servicio de la plataforma.
- Puesta en producción de la plataforma.
- Estabilización de la plataforma.
- Entrega a satisfacción a la entidad designada por la Corporación.
- Dentro de los servicios se debe tener en cuenta el diseño, Instalación, configuración y puesta en producción de los dispositivos de seguridad que actualmente cuenta la Entidad designada por la Corporación, así como la entrega a satisfacción de los mismos a la entidad designada por la Corporación, realizando todas las tareas necesarias para cumplir con ello, sin que esto genere gastos o cobros adicionales para el cliente.
- La entidad designada por la Corporación requiere la implementación y puesta en marcha de las plataformas ofertadas, así como la configuración de políticas, objetos y demás configuraciones a que haya lugar para dejar las misma totalmente operativas y a satisfacción de la

entidad designada por la Corporación, así como realizar pruebas de detección de cada una para validar su correcta configuración de acuerdo a las buenas prácticas de implementación del fabricante.

- El contratista debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, Entre otros) requerida para que el personal asignado al proyecto, pueda cumplir sus funciones.

Garantía y Soporte

- El contratista deberá prestar el servicio de soporte para apertura de casos de cualquier criticidad a través de una Mesa de Ayuda, vía telefónica o vía correo electrónico. Por ambos medios la atención de incidentes estará disponible en horario 7x24x365.
- El contratista deberá registrar, gestionar y hacer seguimiento a cualquier incidente reportado por el la Entidad designada por la Corporación, además durante la atención inicial del caso se determinará su criticidad y la metodología para su resolución.
- Niveles de Atención que debe prestar el contratista:
    - Un primer nivel de atención con Agente Nivel I de la Mesa de Ayuda a través de la ejecución de un checklist, en conjunto con la Entidad designada por la Corporación, y la validación del respectivo problema.
    - Si la incidencia no es resuelta se deberá asignar un Ingeniero de Soporte de Nivel II para proceder con la atención remota o en sitio del incidente.
    - Si la incidencia persiste, el Ingeniero de Soporte de Nivel II procederá a gestionar la apertura de un ticket con el TAC del fabricante para dar pronta solución al incidente.
- El soporte requerido para la solución ofertada deberá ser provisto por el contratista durante el tiempo de servicio.
- El contratista deberá atender y resolver cualquier problema técnico de la solución, en un esquema de atención 7x24X365 (telefónico, e-mail, acceso remoto o presencial en caso de que la Entidad designada por la Corporación así lo requiera), este soporte deberá ser suministrado por personal especializado en la herramienta.

Documentación

- El contratista debe adjuntar los folletos, catálogos u hojas de especificaciones técnicas de los productos y servicios ofrecidos.
- El contratista debe entregar una certificación donde se evidencia que se encuentra en el máximo nivel de membrecía con el Fabricante para garantizar que cuenta con la capacidad de ingeniería para soportar la solución de manera óptima.

FICHA TÉCNICA SOPORTE DATACENTER

- El contratista deberá tener una especialización con el fabricante en operaciones seguras o SASE para garantizar que cuente con la experiencia en este tipo de soluciones.
- El contratista debe documentar todos los procedimientos realizados para la instalación, configuración y parametrización de cada una de las funcionalidades implementadas y entregarlos en medio magnético e impreso, una vez revisados y aprobados por el supervisor del contrato.
- Al finalizar la puesta en funcionamiento de la solución contratada, debe entregar en medio magnético e impreso, la documentación que permita la eficiente administración del firewall, como mínimo incluir:
    - Manual de procedimientos de administración y operación de los appliances.
    - Documento de descripción de la configuración de appliance y parámetros de configuración inicial de todo el software instalado.
    - Documentación de la topología de la solución implementada."

ITEM 5: Postura de NAC (Network Access Control)

Generalidades

- La solución debe permitir la visibilidad, control y respuesta automática de todos los dispositivos que se conecten a la red institucional
- Debe proveer protección contra amenazas, extender el control de dispositivos de terceros y orquestar respuestas automáticas a un amplio rango de eventos de red
- Debe proveer el perfil detallado de cualquier dispositivo sin encabezado conectado a la red institucional usando información y fuentes de comportamiento para identificar todo lo que se encuentre en la red
- Debe poder implementar políticas de microsegmentación y cambiar configuraciones en swicthes extreme Networks con que cuenta la entidad designada por la Corporación y así extender el alcance en ambientes heterogéneos.
- Debe reaccionar a eventos en la red institucional en segundos y contener las amenazas antes de que ellas se esparzan.
- Debe estar en capacidad de reaccionar a eventos generados por el Firewall de Nueva generación de la entidad designada por la Corporación, para tomar acciones de contención de amenazas.
- Debe estar en capacidad de reaccionar a eventos generados por la plataforma de logs y reportería de seguridad de la entidad designada por la Corporación, para tomar acciones de contención de amenazas.
- Debe estar en capacidad de aislar dispositivos maliciosos de acuerdo con la detección realizada por la plataforma de decepción y caza de amenazas de la entidad designada por la Corporación, permitiendo por ejemplo, evitar la propagación de Ransomware..

FICHA TÉCNICA SOPORTE DATACENTER

- Debe contar con un amplio y personalizable set de políticas de automatización que puedan realizar cambios en la configuración de manera instantánea cuando se detecte el comportamiento anómalo.
- Debe permitir escalar de manera efectiva a ubicaciones de múltiples sitios y ser compatible con alta variedad de dispositivos
- Debe interactuar y configurar dispositivos de red de diferentes fabricantes con que cuenta la entidad designada por la Corporación como: Extreme Networks, Aruba y HPE.
- La solución debe soportar el estándar 802.1x pero también estar en capacidad de integrarse con los dispositivos de seguridad y networking usando otros métodos, como SNMP, SSH o API.
- Debe restringir estrictamente el acceso a los activos de red para dispositivos identificados
- Debe poder utilizar como mínimo 15 métodos de perfilamiento de dispositivos
- Debe poder detectar e identificar los dispositivos remotos al conectarse a la red sin agente
- Debe ser un complemento de la solución de NAC sin postura con que cuenta la entidad designada por la Corporación del fabricante Extreme Networks
- Debe proporcionar visibilidad consolidada, clasificación y postura de seguridad.
- Debe permitir tener visibilidad de todos los dispositivos conectados a la red cableada e inalámbrica.
- Debe establecer una política de seguridad basada en reglas que conduzca a la segmentación dinámica y microsegmentación de la red.
- La solución debe estar en capacidad de integrarse con soluciones MDM, ak nmenos Microsoft inTune, Air Watch o Mobile Iron.
- Debe incorporar y gestionar BYOD (Bring your Own Device) con capacidades de gestión de invitados y contratistas.
- Debe poder ver y controlar todos los dispositivos de red (switches, ap, controladora Wireless, firewall de Nueva Generación).
- Debe permitir el acceso menos privilegiado a los recursos de red para dispositivos conectados.
- Debe permitir realizar visibilidad y control de postura sobre dispositivos conectados a través de la VPN SSL del Firewall Perimetral de la entidad designada por la Corporación.
- Debe poder realizar la reautenticación y el monitoreo continuo.
- Debe controlar automáticamente el acceso a la red y responder con flujos de trabajo detallados desde la visibilidad basada en endpoints y los comportamientos en tiempo real.
- Debe identificar y asignar eventos de seguridad a notificaciones. Estos se deben enviar a un administrador, seguido de acciones para mitigar las amenazas de manera dinámica.

FICHA TÉCNICA SOPORTE DATACENTER

- Debe verificar continuamente riesgos para cada endpoint usando inteligencia de amenazas en tiempo real y patrones de comportamiento.
- Debe poder adoptar arquitecturas de Zero Trust para una mejor seguridad de los dispositivos y gestión simplificada.
- Debe enviar datos en tiempo real a la solución de monitoreo y correlación de eventos (SIEM) con que cuenta la entidad designada por la Corporación para así mejorar las respuestas ante incidentes de seguridad.
- Debe contar con portal cautivo que se despliegue al momento del acceso a la red institucional. Este portal cautivo debe personalizarse de acuerdo con las necesidades de la entidad designada por la Corporación.
- Debe poder verificar los dispositivos externos que se conecten a la red (Endpoint Compliance)
- Debe contar con gestión de invitados (Guest Management)
- Debe proveer visibilidad, aplicación de segmentación y ajustes de políticas basado en compatibilidad con las soluciones de seguridad perimetral de la entidad designada por la Corporación.
- Debe integrarse de manera nativa con las soluciones de seguridad perimetral de la entidad designada por la Corporación como Next Generation Firewalls, SIEM, Deceptor, Reporteador de eventos, entre otros.
- Debe ser una solución escalable que se pueda expandir a necesidad de la entidad designada por la Corporación
- La solución se debe proveer en modelo de suscripción por 12 meses contados a partir de su entrega en producción.

Autenticación y Enforcement

- La solución debe permitir conectarse a la red institucional solo a dispositivos autenticados/registrados, desplegando políticas de seguridad que bloqueen y aíslen dispositivos que no cumplan los criterios institucionales, enviándolos a un área de cuarentena sin necesidad de intervención por parte de los administradores de red.
- Debe ser capaz de autorizar los accesos mediante asignación dinámica de VLAN's y/o aplicando ACLs al puerto de acceso.
- Debe ser capaz de controlar escenarios en los que hay más de un equipo conectado a un puerto, asociando a cada equipo la VLAN adecuada, siempre que el equipo de acceso lo permita.
- Debe ser capaz de integrarse con los firewalls para asociar los dispositivos a reglas de seguridad concretas, en función del tipo de dispositivo.
- Debe permitir extender las políticas de seguridad al acceso VPN, ya sea SSL en modo túnel o IPSEC a través de una política de seguridad consistente.
- Debe soportar autenticación de máquina y usuarios, pudiendo autenticar un endpoint sin usar agentes.

FICHA TÉCNICA SOPORTE DATACENTER

- Debe de ser capaz de asociar al dispositivo atributos adicionales, como la ubicación, tipo de dispositivo, fabricante… además de los atributos del usuario conectado.
- Debe soportar opciones de autenticación flexibles, incluyendo 802.1X, autenticación WEB y autenticación MAC.
- Para despliegues 802.1X, debe poder actuar como Radius Proxy y como Radius local (TTLS/PAP, l TTLS/MSCHAPv2, PEAP/MSCHAPv2, TLS)
- Debe soportar integración LDAP y Microsoft Active Directory, sin necesitar ningún componente adicional, para desplegar políticas en función de su pertenencia a ciertos grupos.
- Debe soportar RADIUS Identity store.
- Debe soportar la deteccion y perfilamiento de sistemas operativos chrome
- Integracion de MDM incluida
- Debe soportar enforcement por medio de SSH/SNMP

Requisitos de Endpoint Compliance y Remediación

- La solución debe soportar inspección de los dispositivos tanto basada en agente (persistente y disoluble) como sin agente.
- La solución NAC debe ser capaz de realizar, al menos, las siguientes comprobaciones: service packs, nivel de parcheo, que haya instalado las actualizaciones críticas, Antivirus y AntiSpyware, servicios y procesos, certificados, existencia de archivos y cualquier entrada del registro de Windows.
- Debe contar con un Motor de correlación de eventos.
- La solución debe proporcionar un rol de cuarenta que se interactúe con los Sistemas de parcheo. De esta manera, los dispositivos corporativos que no cumplan los requisitos serán enviados a un portal cautivo de “auto-remediación”: Los equipos que no sean compliant debe de ser enviados a cuarentena dinámicamente, y o bien se le proporcionan instrucciones para la remediación o se ejecuta la remediación automática a través de sistemas como BigFix.

Gestión de Invitados

- El Sistema de control de acceso debe proporcionar una plataforma flexible y eficiente de gestión de usuarios y/o dispositivos no institucionales, que permita manejar el acceso de aquellos usuarios con un acceso transitorio (típicamente invitados) o con un acceso más estable (contratistas externos).
- Debe permitir definir perfiles limitados que solo tengan acceso a la gestión de cuentas de invitados.
- Debe permitir altas masivas (p.e. para conferencias), autoregistros, registros esponsorizados o dados de alta por un administrador.

FICHA TÉCNICA SOPORTE DATACENTER

- Debe permitir autenticaciones por medio de redes Sociales.
- Debe permitir la opción de Aceptar invitados por medio de patrocinadores o Sponsors.
- Debe ser flexible y permitir la definición de diferentes perfiles, como invitados de corta /larga estancia, asistentes a conferencias o auto-registrados.

Actualizaciones de Software

- El contratista debe ofrecer un esquema de acceso a las actualizaciones de software disponibles para la solución durante la vigencia del contrato.
- Se debe realizar la(s) actualización(es) de software durante la vigencia del servicio en la plataforma del fabricante a la última versión disponible y estable relacionada en el objeto del contrato, para mejorar la funcionalidad de la seguridad, cada vez que se requiera.
- El alcance debe cubrir las actualizaciones menores (updates), mayores (upgrades) y prestar el apoyo para su instalación o configuración.

Transferencia de Conocimiento

- El Contratista debe ofrecer transferencia de conocimiento técnica, para diez (10) funcionarios de la entidad designada por la Corporación con una intensidad horaria de mínimo doce (12) horas distribuidas en varias jornadas que se deben coordinar con la entidad designada por la Corporación, sobre la operación, administración y resolución de problemas del servicio ofertado. Toda la transferencia de conocimiento debe estar soportada por su respectiva documentación.

Implementación

- El contratista debe efectuar las instalaciones y configuraciones necesarias de todas las soluciones/servicios de seguridad establecidas en la ficha técnica, incluyendo licenciamientos y el fortalecimiento de las plataformas.
- La actividad de instalación de software deberá comprender los siguientes puntos:
  - Planeación de cada una de las actividades con el fin de disminuir los tiempos de afectación en el servicio.
  - Realizar las actividades planeadas de acuerdo con las mejores prácticas del fabricante.
  - Pruebas de Servicio.
  - Estabilización de la plataforma.
- La entidad designada por la Corporación requiere que se realicen pruebas / muestras de las plataformas/servicios donde se evidencie la correcta configuración de la plataforma implementada.

FICHA TÉCNICA SOPORTE DATACENTER

- El contratista debe garantizar que las licencias de los equipos queden actualizadas a las fechas correspondientes y enviará un informe a la supervisión del contrato donde evidencie este hecho.
- Se debe desplegar con plataformas de gestión, analítica y de reportes con que cuenta la entidad designada por la Corporación.
- Se debe poder desplegar en alta disponibilidad y como virtual appliances (VMware y/o Azure en cada centro de datos)
- Debe poder controlar y gestionar hasta 4.500 dispositivos externos de manera concurrente conectados a la red interna.
- Debe desplegarse de manera centralizada en el centro de datos principal y así controlar el acceso de los dispositivos que se conecten a la red desde cualquiera de las aproximadamente 130 sedes a nivel nacional.

ITEM 6: Servicios de Administración y Soporte de Centro de Datos

Permite a la entidad designada por la Corporación contar con personal profesional para la administración y el soporte de la infraestructura de cómputo, almacenamiento, seguridad, redes, bases de datos y virtualización alojada en el centro de datos del proveedor.

- ✓ Los servicios de administración y soporte deben ser prestados por profesionales certificados y con experiencia en cada una de las tecnologías con que cuenta la entidad designada por la Corporación como sigue:

  i. HPE Simplivity (Hiperconvergencia).
  ii. HPE Synergy (Composable).
  iii. VMware vSphere 6.0 y superior (Virtualización).
  iv. Linux y Windows Server (Sistemas Operativos).
  v. Extreme Networks (Switchs Datacenter).
  vi. SQL Server, Postgress, MySQL, Oracle y Nexus (Bases de Datos).
  vii. Hitachi (Storage).
  viii. Fortinet (FortiAnalyzer, FortiADC, FortiSandBox, Fortiweb, Fortigate).
  ix. Azure Administration.
  x. Backup (Commvault).

- ✓ Las jornadas de administración y soporte deben ser:

  - Fines de semana desde el sábado a las 00:00 y hasta el domingo a las 23:59.
  - Días festivos desde las 00:00 hasta las 23:59.
  - Días vacancia judicial desde las 00:00 hasta las 23:59. Los días de vacancia judicial de la entidad designada por la Corporación por concepto semana santa desde el lunes 14 de abril de 2025 a las 00:00 y hasta el miércoles 16 de abril de 2025 a las 23:59.

    Nota: Dichas jornadas de administración y soporte sólo atenderán incidentes, cambios de emergencia, cambios normales, cambios estándar, actualizaciones de plataformas, ventanas de mantenimiento, documentación

y requerimientos prioritarios que afecten la operación de los servicios en producción de la entidad designada por la Corporación.

- ✓ Cuando se generen incidentes que trasciendan a fin de semana o festivo se generará continuidad de los mismos a través de la integración de las herramientas de gestión de requerimientos e incidentes del proveedor y la entidad designada por la Corporación. Teniendo en cuenta lo anterior, el proveedor debe suministrar una matriz de escalamiento, así como la entidad designada por la Corporación debe suministrar una matriz de contactos autorizados para la creación de requerimientos e incidentes.
- ✓ El personal de operación y soporte debe crear de manera mensual los siguientes insumos por cada una de las plataformas administradas (Seguridad, Redes, Azure, Cómputo, Sistemas Operativos, Virtualización, Respaldo, Almacenamiento): a) Un (1) instructivo relacionado con la operación de cada plataforma administrada.
- ✓ El personal de administración y soporte de la infraestructura de la entidad designada por la Corporación lo hará de manera remota y deben contar con sus propias herramientas para ejecutar sus labores. La asistencia al centro de datos del proveedor sólo se realizará en el caso que el personal de manos remotas no pueda solucionar algún incidente en la infraestructura.
- ✓ El personal de operación y soporte debe entregar al finalizar el primer mes del contrato un (1) esquema con diagramas UML actualizado por cada plataforma administrada.
- ✓ El personal de operación y soporte debe desarrollar durante el primer mes del contrato el inventario con las fechas de vencimiento del soporte de cada una de las plataformas administradas y de las licencias instaladas en cada una de las máquinas físicas.
- ✓ El personal de administración y soporte debe realizar pruebas de failover de las plataformas administradas y que cuenten con un ambiente para su realización de forma mensual en ventanas controladas y el resultado debe hacer parte del informe mensual.
- ✓ El personal de administración y soporte debe entregar un informe consolidado mensual con las evidencias de la gestión (Incidentes, requerimientos, controles de cambios, mantenimientos, ventanas, actualizaciones, recomendaciones, otros) sobre la infraestructura de la entidad designada por la Corporación y la contratada por servicio.
- ✓ El personal de administración y soporte debe incluir dentro de cada informe el listado de actualizaciones recomendado a nivel de versiones de firmware de las plataformas, sistemas operativos, bases de datos, entre otros.

1. Condiciones Transversales para la prestación de los servicios

Con respecto a los servicios a desarrollar se deben establecer las siguientes condiciones transversales:

- ✓ El proveedor seleccionado debe realizar la administración de toda la tecnología dispuesta y realizar el levantamiento y/o desarrollo manuales y procedimientos de operación y gestión de la tecnología entregada, así como

crear y mantener el repositorio de arquitectura actualizado acorde a los cambios gestionados.

- ✓ En el plan de operación debe quedar contemplada la estrategia de monitoreo, backup y gestión de la solución, donde se incluye la integración de todo el ecosistema de monitoreo, los temas de cumplimiento de las políticas de backup y retención, pruebas de restauración y el modelo de gestión de TI que incluya el soporte, mantenimiento y administración de la tecnología dispuesta por la Entidad designada por la Corporación.

- ✓ El proveedor debe contar con licenciamiento actualizado, soporte y mantenimiento vigente directamente prestado por el fabricante de toda la infraestructura que preste como servicio.

- ✓ Se debe realizar la configuración y administración de la infraestructura en servicio mientras dure el colocation, y entregar al final del proceso backup de las reglas implementadas y configuraciones desarrolladas.

- ✓ Con respecto a la infraestructura de perímetro y demás infraestructura prestada como servicio, durante la operación y al final de servicio prestado debe entregar backup de configuración y reporte de operación periódico y de eventos mitigados y/o gestionados.

- ✓ El proveedor debe realizar pruebas de restauración de backups incluyendo el resultado en los informes mensuales.

- ✓ Deberá entregar la arquitectura de infraestructura actual y objetivo, en el repositorio de arquitectura de la Entidad designada por la Corporación - Utilizando diagramas UML de despliegue y componentes, nombrando todos los ítems acordes a inventario y cargando sus características y especificaciones.

1. EQUIPO DE TRABAJO

Gerente del proyecto

Será el responsable de la definición del proyecto y de la asignación de recursos (personas, actividades y tiempo) al mismo. Dando soporte a las tareas de estimación y definición de las actividades contenidas en los planes y en realizar la revisión y aprobación de los mismos.

Formación	Profesional en ingeniería de sistemas, industrial, telemática, electrónica o afines. Título de especialización o maestría en Gerencia de Proyectos o Gerente de Proyectos en proyectos informáticos o ingeniería

FICHA TÉCNICA SOPORTE DATACENTER

	de software o áreas afines con conocimientos certificados en Dirección de Proyectos Certificación vigente Project Management Professional (PMP) del PMI
Experiencia General	Mínimo con seis (6) años de experiencia profesional
Experiencia Especifica	Mínimo con tres (3) años de experiencia específica en coordinación y/o dirección de proyectos de análisis y/o diseño y/o desarrollo y/o implementación de soluciones de software.

Responsabilidades y actividades:

- Liderará los equipos de trabajo en función de alcanzar los objetivos del proyecto.
- Preparar y mantener un cronograma detallado de las actividades a realizar durante el proyecto
- Proporcionar las estimaciones de esfuerzo en el desarrollo de los artefactos o módulos requeridos por la PGN para la aprobación por parte del supervisor técnico.
- Priorizar actividades, recursos y tiempos.
- Gestionar el presupuesto del proyecto.
- Actuar como el interlocutor entre la firma consultora y la PGN.
- Realizar informes de los avances y estados del proyecto.
- Gestionar los riesgos del proyecto.
- Ejecutar acciones correctivas en el caso de ser necesario.

ADMINISTRADORES TÉCNICOS DE LA INFRAESTRUCTURA

El contratista deberá proporcionar evidencia documentada que demuestre que cuenta con personal idóneo para la prestación de los servicios.

Para demostrar lo anterior, deberá presentar los currículos (Experiencia, certificaciones y académicos) que garanticen la correcta administración, operación y soporte de las siguientes plataformas:

- Microsoft Azure.
- Extreme Networks.
- Seguridad Fortinet (Fortigate, FortiSandbox, FortiAnalizer, FortiADC, FortiWeb).
- Almacenamiento Hitachi Vantara.
- Cómputo HPE Synergy.
- Hiperconvergencia HPE Simplivity.
- Sistemas Operativos Windows Server y Linux.
- Virtualización VMware (vSphere, vRealize).
- Bases de Datos Oracle, SQL Server, Postgress, Nexus y MySQL
- Respaldo (Commvault).

FICHA TÉCNICA SOPORTE DATACENTER

NOTA 1: Los servicios de administración y soporte de las plataformas descritas se pueden cumplir con uno o varios perfiles que se deben presentar en la oferta especificando cuales operarán y darán soporte a cada plataforma.

NOTA 2: Será responsabilidad del proveedor suministrar el personal adicional que se requiera para la ejecución de este proyecto.

Acuerdos De Nivel de Servicio para plataformas administradas

Plataforma	Descripción	Evento	Alcance	Tipo de caso	SLA
ALMACENAMIENTO	**Red SAN**	INDISPONIBILIDAD FALLA	Soporte a las plataformas de virtualización, y almacenamiento	INCIDENTE	3 Horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	6 Horas
		GESTIÓN ALMACENAMIENTO APROVISIONAMIENTO CONFIGURACIÓN ACTUALIZACIÓN		REQUERIMIENTO	2 días
	Storage Primario	INDISPONIBILIDAD FALLA		INCIDENTE	3 Horas

FICHA TÉCNICA SOPORTE DATACENTER

		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	6 Horas
		GESTIÓN ALMACENAMIENTO APROVISIONAMIENTO CONFIGURACIÓN ACTUALIZACIÓN		REQUERIMIENTO	2 días
	NAS	INDISPONIBILIDAD FALLA		INCIDENTE	3 Horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	6 Horas
		GESTIÓN ALMACENAMIENTO APROVISIONAMIENTO CONFIGURACIÓN ACTUALIZACIÓN		REQUERIMIENTO	2 días
	HCP	INDISPONIBILIDAD FALLA		INCIDENTE	3 Horas

FICHA TÉCNICA SOPORTE DATACENTER

		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	6 Horas
		GESTIÓN ALMACENAMIENTO APROVISIONAMIENTO CONFIGURACIÓN ACTUALIZACIÓN		REQUERIMIENTO	2 días
COMPUTO	**Synergy**	INDISPONIBILIDAD FALLA	Soporte a las plataformas de virtualización, y almacenamiento	INCIDENTE	3 Horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	6 Horas
		GESTIÓN ALMACENAMIENTO		REQUERIMIENTO	5 Días
		APROVISIONAMIENTO CONFIGURACIÓN ACTUALIZACIÓN		REQUERIMIENTO	2 días
	Simplivity	INDISPONIBILIDAD FALLA		INCIDENTE	3 Horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	6 Horas
		GESTIÓN ALMACENAMIENTO		REQUERIMIENTO	5 Días

FICHA TÉCNICA SOPORTE DATACENTER

		APROVISIONAMIENTO CONFIGURACIÓN ACTUALIZACIÓN		REQUERIMIENTO	2 días
	Azure	INDISPONIBILIDAD FALLA		INCIDENTE	3 Horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	4 Horas
		GESTIÓN ALMACENAMIENTO		REQUERIMIENTO	5 Días
		APROVISIONAMIENTO CONFIGURACIÓN ACTUALIZACIÓN		REQUERIMIENTO	2 días
SEGURIDAD INFORMATICA	**Firewall**	FALLA INDISPONIBILIDAD	Soporte a los dispositivos de seguridad perimetral	INCIDENTE	3 Horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	4 Horas
		GESTIÓN VULNERABILIDADES FILTRADO CONTENIDO WEB GESTION DE ACCESO		REQUERIMIENTO	1 día
		GESTIÓN DE POLÍTICAS CONFIGURACIÓN		REQUERIMIENTO	2 días
	Balanceador	FALLA INDISPONIBILIDAD		INCIDENTE	3 Horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	4 Horas
		GESTIÓN VULNERABILIDADES FILTRADO CONTENIDO WEB GESTION DE ACCESO		REQUERIMIENTO	1 día
		GESTIÓN DE POLÍTICAS CONFIGURACIÓN		REQUERIMIENTO	2 días
	ANTISPAM	FALLA INDISPONIBILIDAD		INCIDENTE	3 Horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	6 Horas

FICHA TÉCNICA SOPORTE DATACENTER

		GESTIÓN VULNERABILIDADES FILTRADO CONTENIDO WEB GESTION DE ACCESO		REQUERIMIENTO	1 día
		GESTIÓN DE POLÍTICAS CONFIGURACIÓN		REQUERIMIENTO	2 días
	SASE	FALLA INDISPONIBILIDAD		INCIDENTE	3 Horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	6 Horas
		GESTIÓN VULNERABILIDADES FILTRADO CONTENIDO WEB GESTION DE ACCESO		REQUERIMIENTO	1 día
		GESTIÓN DE POLÍTICAS CONFIGURACIÓN		REQUERIMIENTO	2 días
	POSTURA NAC	FALLA INDISPONIBILIDAD		INCIDENTE	3 Horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	6 Horas
		GESTIÓN VULNERABILIDADES FILTRADO CONTENIDO WEB GESTION DE ACCESO		REQUERIMIENTO	1 día
		GESTIÓN DE POLÍTICAS CONFIGURACIÓN		REQUERIMIENTO	2 días
BASES DE DATOS	**SQL Server**	FALLA EN BASE DE DATOS INDISPONIBILIDAD	Soporte a las Bases de Datos que componen los diferentes sistemas de información de la entidad designada por la Corporación	INCIDENTE	5 horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	4 Horas

FICHA TÉCNICA SOPORTE DATACENTER

		LENTITUD		INCIDENTE	8 horas
		CONFIGURACIÓN CREACIÓN DE INSTANCIA CREACIÓN/MODIFICACIÓN/ELEMINACIÓN PERFIL		REQUERIMIENTO	2 días
	Oracle	FALLA EN BASE DE DATOS INDISPONIBILIDAD		INCIDENTE	5 horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	6 Horas

FICHA TÉCNICA SOPORTE DATACENTER

		LENTITUD		INCIDENTE	8 horas
		CONFIGURACIÓN CREACIÓN DE INSTANCIA CREACIÓN/MODIFICACIÓN/ELEMINACIÓN PERFIL		REQUERIMIENTO	2 días
	MySQL	FALLA EN BASE DE DATOS INDISPONIBILIDAD		INCIDENTE	5 horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	6 Horas

FICHA TÉCNICA SOPORTE DATACENTER

		LENTITUD		INCIDENTE	8 horas
		CONFIGURACIÓN CREACIÓN DE INSTANCIA CREACIÓN/MODIFICACIÓN/ELEMINACIÓN PERFIL		REQUERIMIENTO	2 días
VCENTER		INDISPONIBILIDAD FALLA	Soporte a la plataformas de virtualización,	INCIDENTE	3 Horas
		INDISPONIBILIDAD FALLA ESCALADA A FABRICANTE		INCIDENTE	6 Horas
		CONFIGURACIÓN ACTUALIZACIÓN		REQUERIMIENTO	2 días

Acuerdos de Nivel de Servicio para servicios de balanceadores, firewalls y correlación de eventos (Hardware)

NOTA: Los Acuerdo de Nivel de Servicio para los servicios mencionados, serán los definidos en el acuerdo Marco Nube Privada IV CCENEG-061-01-2022 (Códigos de Servicio: *S1-IT-NP-IS-5-8*, *S1-IT-NP-IS-26-4* e *S1-IT-NP-IP-15-2*) anexos al presente documento.

Las ANS descritos se pueden consultar en el siguiente enlace:

https://colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/acuerdo-marco-para-la-adquisicion-de-servicios-de-0