Superintendencia de Notariado y Registro

ANEXO No. 1 - ESPECIFICACIONES TÉCNICAS - LOTE UNO

SUPERINTENDENCIA DE NOTARIADO Y REGISTRO
OFICINA DE TECNOLOGIAS DE LA INFORMACION - OTI

Objeto:

ADQUISICIÓN Y RENOVACIÓN DE EQUIPOS DE NETWORKING Y SEGURIDAD PERIMETRAL, INCLUYENDO LICENCIAMIENTO, SOPORTE Y GARANTÍA.
.

JULIO, 2025

Tabla de contenido

INTRODUCCIÓN 3
1. IDENTIFICACIÓN DEL CLASIFICADOR DE BIENES Y SERVICIOS 4
2. ALCANCE OBJETO DEL LOTE 1 4
3. CONTEXTO Y CARACTERISTICAS DE LA PLATAFORMA DE NETWORKING Y SEGURIDAD DE LA PLATAFORMA JUNIPER 4
3.1. ADQUISICIÓN DE EQUIPOS DE NETWORKING JUNIPER 4
4. ESPECIFICACIONES TÉCNICAS MÍNIMAS: 6
4.1. ESPECIFICACIONES TÉCNICAS MÍNIMAS – ADQUISICION DE EQUIPOS DE NETWORKING Y SEGURIDAD PERIMETRAL POR OBSOLESCENCIA Y/O FIN DE VIDA ÚTIL: 6
ADQUISICIÓN DE TECNOLÓGICA POR OBSOLESCENCIA Y FIN DE VIDA UTIL DE SWITCHES DE CORE DE 48 PUERTOS. 7
ADQUISICIÓN DE TECNOLÓGICA POR OBSOLESCENCIA Y FIN DE VIDA UTIL DE SWITCHES DE CORE DE 48 PUERTOS 8
ADQUISICIÓN DE TECNOLÓGICA POR OBSOLESCENCIA Y FIN DE VIDA UTIL DE SWITCHES DE OFICINA DE 48 PUERTOS 10
AQUISICIÓN DE TECNOLÓGIA POR OBSOLESCENCIA Y FIN DE VIDA UTIL DE SWITCHES DE OFICINA DE 24 PUERTOS 12
ADQUISICIÓN TECNOLÓGICA DE DDI 16
4.2. ESPECIFICACIONES TÉCNICAS MÍNIMAS – RENOVACIÓN DE SOPORTE TÉCNICO; LICENCIAMIENTO Y GARANTÍA DE EQUIPOS DE NETWORKING Y SEGURIDAD PERIMETRAL: 25

INTRODUCCIÓN

La Superintendencia de Notariado y Registro (SNR) juega un papel crucial en el fortalecimiento de la confianza ciudadana hacia el Estado, actuando como garante de la tradición de los derechos de la propiedad y la validez de ciertos actos civiles. Esta confianza se basa en la certeza de que las actuaciones del Registro de Instrumentos Públicos se alinean con el orden jurídico y reflejan fielmente la voluntad de las partes involucradas. Para lograr esto, es imperativo que la superintendencia y las oficinas de registro empleen herramientas eficientes y seguras que faciliten el acceso a los servicios registrales.

En este contexto, el Decreto 2723 de 2014 encarga a la SNR la asesoría al Gobierno Nacional en la formulación de políticas públicas y el desarrollo de programas y planes en el ámbito de los servicios públicos registral y notarial. Además, la ley 1579 de 2012, en su artículo 6, subraya la importancia de unificar los sistemas de registro de la propiedad inmueble a nivel nacional mediante el uso de tecnologías digitales y procedimientos técnicos avanzados, para asegurar un proceso de registro seguro, rápido y eficaz.

La SNR ha emprendido un proceso de modernización de sus procesos misionales, apoyándose en tecnologías de la información y comunicaciones (TIC), esto incluye infraestructura de Seguridad que permite proteger tanto los sistemas de información, como los datos que se crean, transmiten, procesas o almacenan en los mismos.

Este esfuerzo de modernización se alinea con las directrices del Manual de implementación de la Política de Gobierno Digital y la ley 2294 de 2023 (PND), que buscan mejorar la relación Ciudadano-Estado y hacer interoperable la información a través del Sistema de Administración de Tierras (SAT), el repositorio de datos maestros (RDM) y la consolidación del Catastro Multipropósito.

Finalmente, la entidad se ha propuesto como objetivo estratégico convertirse en un modelo de excelencia en la prestación de servicios públicos registral y notarial, liderando los procesos de protección, restitución y formalización de la recuperación de tierras. Este objetivo se apoya en una plataforma tecnológica moderna y un talento humano fortalecido, para satisfacer la demanda cambiante de los servicios asociados y garantizar el acceso oportuno a la información de propiedad inmobiliaria en todo el territorio nacional, independientemente de la ubicación geográfica de las Oficinas de Registro.

1. IDENTIFICACIÓN DEL CLASIFICADOR DE BIENES Y SERVICIOS

El presente proceso está codificado en el clasificador de bienes y servicios UNSPSC como se indica en la siguiente Tabla.

Código	Segmento	Familia	Clase
43222600	Difusión de tecnologías de información y Comunicaciones.	Equipos o plataformas y accesorios de redes multimedia o de voz o de datos.	Equipos de servicio de red.
43223300	Difusión de tecnologías de información y comunicaciones.	Equipos o plataformas y accesorios de redes multimedia o de voz o de datos.	Dispositivos y equipos para instalación de conectividad de redes y datacom.
43222500	Difusión de tecnologías de información y Comunicaciones.	Equipos o plataformas y accesorios de redes multimedia o de voz o De datos.	Equipo de seguridad de red.
81161700	Servicios basados en ingeniería, investigación y Tecnología	Entrega de servicios de tecnología de información.	Servicios de telecomunicaciones.

2. ALCANCE OBJETO DEL LOTE 1

ADQUISICIÓN Y RENOVACIÓN DE EQUIPOS DE NETWORKING Y SEGURIDAD PERIMETRAL, INCLUYENDO LICENCIAMIENTO, SOPORTE Y GARANTÍA**.**

3. CONTEXTO Y CARACTERISTICAS DE LA PLATAFORMA DE NETWORKING Y SEGURIDAD DE LA PLATAFORMA JUNIPER

3.1. ADQUISICIÓN DE EQUIPOS DE NETWORKING JUNIPER

Es fundamental mantener una solución de red robusta que garantice la conectividad, productividad y seguridad de la SNR en el entorno digital actual. Por esta razón, es necesaria la renovación tecnológica de los equipos de la marca Juniper, que constituyen la base de la infraestructura de red activa de la entidad. Cambiar de marca implicaría riesgos significativos para la estabilidad, compatibilidad y continuidad operativa de la red, lo que podría afectar la eficiencia en la prestación del servicio público registral. La actualización

tecnológica no solo refuerza la integridad del sistema, sino que también mejora el rendimiento y la seguridad, alineándose con los estándares más avanzados del mercado.

La adquisición de nuevos equipos Juniper con el correspondiente licenciamiento, soporte y garantía es una medida estratégica clave para asegurar la disponibilidad y seguridad de los servicios críticos de la entidad. Esta renovación tecnológica es especialmente relevante debido a que hay equipos que se encuentran en estado de obsolescencia, lo que compromete tanto la eficiencia como la seguridad de los servicios misionales de la SNR.

Es imprescindible adquirir y/o actualizar estos equipos, dado que han alcanzado el final de su ciclo de vida útil, lo que ha generado limitaciones tecnológicas que impiden una protección y optimización adecuada de la red. La plataforma Juniper, con sus avanzadas funcionalidades en seguridad y rendimiento, garantiza una transición fluida hacia nuevas capacidades tecnológicas. Esto es crucial para enfrentar eficazmente las amenazas emergentes y atender las crecientes demandas de tráfico de red, asegurando la estabilidad y continuidad operativa de los servicios esenciales.

SEGURIDAD PERIMETRAL DE LOS EQUIPOS JUNIPER SRX4200 Y SRX4100

Prevención de Intrusiones (IPS): Detecta y bloquea amenazas en tiempo real, crucial para proteger la red contra ataques conocidos y desconocidos, incluidos los exploits de día cero.

Protección contra Amenazas Avanzadas (ATP): Emplea inteligencia artificial y análisis de comportamiento para identificar y mitigar amenazas sofisticadas, incluyendo malware y ransomware.

Filtrado de Contenido y Control de Aplicaciones: Implementa políticas de seguridad basadas en la identidad del usuario, dispositivo y ubicación, reduciendo la superficie de ataque.

Actualizaciones de Inteligencia de Amenazas: A través de servicios en la nube, recibe actualizaciones continuas para mantener la red protegida contra las amenazas más recientes.

PLATAFORMA DE NETWORKING JUNIPER:

Licenciamiento y garantía actualizados: Es fundamental para mantener la funcionalidad óptima y la seguridad de los equipos, asegurando su operatividad frente a nuevas amenazas.

Acceso a actualizaciones y parches: Garantiza mejoras en el rendimiento y proporciona protección frente a amenazas emergentes, fortaleciendo la estabilidad de la red.

Protección de hardware: La adquisición de la garantía cubre posibles fallos del equipo, permitiendo reparaciones o reemplazos sin costo adicional, lo que asegura la continuidad operativa.

Compatibilidad con la infraestructura actual: Al mantener la plataforma Juniper, se asegura una integración sin interrupciones con la infraestructura existente, lo que minimiza riesgos de incompatibilidades.

Alta disponibilidad (HA): Los equipos ofrecen redundancia en componentes clave, lo que minimiza el riesgo de fallos y garantiza la continuidad del servicio.

Capacidad de procesamiento escalable: Los equipos están diseñados para soportar el tráfico actual y se encuentran preparados para futuras demandas tecnológicas, como IPv6 y redes definidas por software (SDN).

Funciones de seguridad avanzada: Integran cortafuegos, sistemas de prevención de intrusiones (IDS/IPS) y control de aplicaciones, lo que permite una protección en tiempo real del tráfico y los datos críticos de la entidad.

Eficiencia energética: Los nuevos equipos cumplen con los estándares internacionales de sostenibilidad, optimizando el consumo energético y reduciendo los costos operativos a largo plazo.

Esta adquisición y renovación asegura que la SNR continúe operando de manera eficiente y segura, protegiendo su infraestructura crítica y alineándose con las demandas tecnológicas y de seguridad del entorno digital actual.

4. ESPECIFICACIONES TÉCNICAS MÍNIMAS:

4.1. ESPECIFICACIONES TÉCNICAS MÍNIMAS – ADQUISICION DE EQUIPOS DE NETWORKING Y SEGURIDAD PERIMETRAL POR OBSOLESCENCIA Y/O FIN DE VIDA ÚTIL:

Ítem	Cantidad	Descripción
1	4	Switch de Core que soporten mínimo (48) puertos en cobre 10GbE + 6 uplink (100 GB) Juniper QFX5120-48T-AFO.
2	2	Switch de Core que soporten mínimo (48) puertos en cobre 10GbE + 6 uplink (100 GB) Juniper QFX5120-48Y-AFO2.
3	20	Switch de Oficina de mínimo 48 puertos en cobre 1GbE + 4 uplink SFP/SFP+ (10 GbE) Juniper EX2300-48P POE+

Ítem	Cantidad	Descripción
4	20	Switch de oficina de mínimo 24 puertos en cobre 1GbE + 4 uplink SFP/SFP+ (10 GbE) Juniper EX2300-24P POE+ EX2300-24P
5	3	Adquisición de una solución DDI con redundancia local y geográfica en los Datacenter de la entidad.
6	500	Licenciamiento por 1 año de herramienta para el monitoreo de actividades de 500 estaciones de trabajo de usuarios de la Superintendencia de Notariado y Registro. Se deben incluir servicios profesionales del fabricante para su instalación y configuración.
TOTAL	**549**	

Teniendo en cuenta el cuadro anterior se describe la necesidad:

~~A.~~ ADQUISICIÓN DE TECNOLÓGICA POR OBSOLESCENCIA Y FIN DE VIDA UTIL DE SWITCHES DE CORE DE 48 PUERTOS.

Instalación, configuración y reemplazo de cuatro (4) Switch de Core que soporten mínimo (48) puertos en cobre 10GbE + 6 uplink (100 GB) Juniper QFX5120-48T-AFO.

REQUISITOS TÉCNICOS SWITCH DE OFICINA
ESPECIFICACIONES FÍSICAS PARA LOS SWITCH
• Los equipos ofertados deben soportar el mismo sistema operativo en acceso y Core. • El arreglo de switches debe verse física y lógicamente en el sistema de gestión como unúnico switch • Presentación en tipo chassis o virtualización de chassis (modular) que permita ver al conjunto de equipos modulares como un único equipo lógico y físico. • Capacidad de 48 dual-speed 1GbE/10GbE RJ-45 puertos de cobre. • Capacidad de seis dual-speed 100GbE (QSFP28)/40GbE (QSFP+) uplink puertos
REQUISITOS TÉCNICOS SWITCH
• Soporte de IPv6: El equipo a nivel de hardware y software debe estar listo para implementarIPV6 • Los circuitos encargados de nivel 3 de las controladoras, deben realizar el balanceo de carga,mediante el soporte de protocolo VRRP, para crear defaults gateways virtuales dentro de lared y garantizar que en caso de que ocurra alguna falla en los circuitos de nivel 3 de una tarjeta controladora, otro equipo de nivel 3 pueda tomar el control, sin que la dirección IP deldefault Gateway de los equipos de red cambie, garantizando transparencia y alta disponibilidad para los usuarios/servicios conectados en cada VLAN. • Todas las unidades deben poderse montar en racks de 19 pulgadas los herrajes deben ser incluidos por cada equipo • Indicadores visuales de estado de puertos y sistema • Todos deben incorporar tecnología (EEE) o amigable con el ambiente.

CAPACIDADES DE SWITCHING
Capa 2: ➢ Soporte de tramas estándar y jumbo frames ➢ Soporte de más de 285.000 MAC address ➢ Soporte de 4,091 VLANS ➢ Soporte 802.1Q (vlan Tagging) ➢ Debe estar en propiedad de controlar tormentas de Broadcast, multicast y unicast. ➢ Mapeo ARP estático ➢ Soporte de link aggregation ➢ 802.1D, 802.3X, 802.1w ➢ Mirroring local o remoto para supresión remota de tráfico en el puerto o VLAN
Capa 3: ➢ Soporte de rutas estáticas ➢ Soporte de multicast ➢ Soporte CIDR ➢ Soporte UDP y TCP ➢ DHCP ➢ DNS ➢ Soporte ipv4 e ipv6 ➢ Capacidad de asegurar que los usuarios utilicen únicamente las direcciones previamente asignadas por el servidor DHCP autorizado. ➢ Prevenir el tráfico IP de direcciones IP con direcciones MAC que no correspondan a la tabla de DHCP ➢ Soportar CoS/QoS ➢ Soportar 802.1p ➢ Priorización de tráfico basado en MAC-address, VLAN, port, origen IP, destinoIP, puerto de origen o puerto de destino. ➢ Filtrado de tráfico entrante basado en dirección MAC origen / destino, Ethertype, dirección Origen IP, dirección destino IP, puerto origen / destino TCP puerto origen / destino UDP

B. ADQUISICIÓN DE TECNOLÓGICA POR OBSOLESCENCIA Y FIN DE VIDA UTIL DE SWITCHES DE CORE DE 48 PUERTOS

Instalación, configuración y reemplazo de dos (2) Switch de core que soporten mínimo (48) puertos 25GbE (SFP28)/10GbE (SFP+)/1GbE (SFP) downlink ports + 8 uplink (100 GB) **Juniper QFX5120-48Y-AFO2**.

REQUISITOS TÉCNICOS SWITCH
ESPECIFICACIONES FÍSICAS PARA LOS SWITCH
• Los equipos ofertados deben soportar el mismo sistema operativo en acceso y Core. • El arreglo de switches debe verse física y lógicamente en el sistema de gestión como un único switch • Presentación en tipo chassis o virtualización de chassis (modular) que permita ver al conjunto de equipos modulares como un único equipo lógico y físico. • Capacidad de 48 25GbE (SFP28)/10GbE (SFP+)/1GbE (SFP) downlink ports. • Capacidad de ocho dual-speed 100GbE (QSFP28)/40GbE (QSFP+) uplink puertos.
REQUISITOS TÉCNICOS SWITCH
• Soporte de IPv6: El equipo a nivel de hardware y software debe estar listo para implementar IPV6 • Los circuitos encargados de nivel 3 de las controladoras, deben realizar el balanceo de carga, mediante el soporte de protocolo VRRP, para crear defaults gateways virtuales dentro de la red y garantizar que en caso de que ocurra alguna falla en los circuitos de nivel 3 de una tarjeta controladora, otro equipo de nivel 3 pueda tomar el control, sin que la dirección IP del default Gateway de los equipos de red cambie, garantizando transparencia y alta disponibilidad para los usuarios/servicios conectados en cada VLAN. • Todas las unidades deben poderse montar en racks de 19 pulgadas los herrajes deben ser incluidos por cada equipo • Indicadores visuales de estado de puertos y sistema • Todos deben incorporar tecnología (EEE) o amigable con el ambiente
CAPACIDADES DE SWITCHING
Capa 2: ➢ Soporte de tramas estándar y jumbo frames ➢ Soporte de más de 285.000 MAC address ➢ Soporte de 4,091 VLANS ➢ Soporte 802.1Q (vlan Tagging) ➢ Debe estar en propiedad de controlar tormentas de Broadcast, multicast y unicast. ➢ Mapeo ARP estático ➢ Soporte de link agregation ➢ 802.1D, 802.3X, 802.1w ➢ Mirroring local o remoto para supresión remota de tráfico en el puerto o VLAN **Capa 3:** ➢ Soporte de rutas estáticas ➢ Soporte de multicast ➢ Soporte CIDR ➢ Soporte UDP y TCP ➢ DHCP ➢ DNS ➢ Soporte ipv4 e ipv6

➢ Capacidad de asegurar que los usuarios utilicen únicamente las direcciones previamente asignadas por el servidor DHCP autorizado. ➢ Capacidad de revisar que los paquetes ARP vienen de direcciones IP válidas (Dynamic ARP Inspection) ➢ Prevenir el tráfico IP de direcciones IP con direcciones MAC que no correspondan a la tabla de DHCP ➢ Soportar CoS/QoS ➢ Soportar 802.1p ➢ Priorización de tráfico basado en MAC-address, VLAN, port, origen IP, destinoIP, puerto de origen o puerto de destino. ➢ Filtrado de tráfico entrante basado en dirección MAC origen / destino, Ethertype, dirección Origen IP, dirección destino IP, puerto origen / destino TCP puerto origen / destino UDP

C. ADQUISICIÓN DE TECNOLÓGICA POR OBSOLESCENCIA Y FIN DE VIDA UTIL DE SWITCHES DE OFICINA DE 48 PUERTOS

Instalación, configuración y reemplazo de cinco (5) Switch de oficina de mínimo 48 puertos en cobre 1GbE + 4 uplink SFP/SFP+ (10 GbE) Juniper EX2300-48P POE+

REQUISITOS TÉCNICOS SWITCH
ESPECIFICACIONES FÍSICAS PARA LOS SWITCH
• Los equipos ofertados deben soportar el mismo sistema operativo en acceso y Core. • El arreglo de switches debe verse física y lógicamente en el sistema de gestión como unúnico switch. • Presentación en tipo chassis o virtualización de chassis (modular) que permita ver al conjunto de equipos modulares como un único equipo lógico y físico. • Los switches deben interconectarse entre sí mediante puertos de fibra independientes a los48 puertos de acceso, ofreciendo un backplane mínimo 80Gbps • La capacidad de conmutación mínima de cada uno de los switches que compongan el arreglodebe ser de 176Gbps.
REQUISITOS TÉCNICOS SWITCH
• Garantizar la existencia física de cómo mínimo 2 switches que actúen uno como Routing Engine (RE) Principal y el otro como Backup • Debe contar con una funcionalidad Graceful Route Engine Switch over (GRES) que permitaal arreglo de switches continuar enrutando paquetes en el evento de falla del switch que actúa como Routing Engine (RE) Principal • Debe permitir que si falla uno de los switches del arreglo, se pueda extraer el switch que falla,sin afectar la conmutación de paquetes del resto de switches y sin necesidad de intervención humana para reconfigurar tablas de enrutamiento. • Debe permitir que al ingresar un switch al arreglo para reemplazar algún otro que esté fallando, el arreglo se encargue de actualizar el sistema operativo del nuevo switch de formaautomática y sin detener el enrutamiento de paquetes del arreglo de switch. • Soporte de puertos de 10/100/1000 autosense para acceso en todos los puertos • Soporte de 4 puertos 1/10Gbps para fibras MM y SM

- Detección automática de puertos DCE o DTE (MDI-MDIX)
- Soporte de IPv6: El equipo a nivel de hardware y software debe estar listo para implementarIPV6
- Los circuitos encargados de nivel 3 de las controladoras, deben realizar el balanceo de carga,mediante el soporte de protocolo VRRP, para crear defaults gateways virtuales dentro de lared y garantizar que en caso de que ocurra alguna falla en los circuitos de nivel 3 de una tarjeta controladora, otro equipo de nivel 3 pueda tomar el control, sin que la dirección IP deldefault Gateway de los equipos de red cambie, garantizando transparencia y alta disponibilidad para los usuarios/servicios conectados en cada VLAN.
- Todas las unidades deben poderse montar en racks de 19 pulgadas los herrajes deben ser incluidos por cada equipo
- Indicadores visuales de estado de puertos y sistema
- Todos deben incorporar tecnología (EEE) o amigable con el ambiente.

CAPACIDADES DE SWITCHING

Capa 2:

- Soporte de tramas estándar y jumbo frames
- Soporte de más de 16.000 MAC address
- Listas de acceso de nivel 2
- Soporte de 4,093 VLANS (más de 2000 Vlans activas)
- Soporte 802.1Q (vlan Tagging)
- Debe estar en propiedad de controlar tormentas de Broadcast, multicast y unicast.
- Mapeo ARP estático
- Soporte de link agregation
- 802.1D, 802.3X, 802.1w
- Mirroring local o remoto para supresión remota de tráfico en el puerto o VLAN
- Procesamiento distribuido que garantice wirespeed

Capa 3:

- Soporte de rutas estáticas
- Soporte de multicast
- Soporte CIDR
- Soporte UDP y TCP
- DHCP
- DNS
- Listas de acceso basadas en IP origen y destino, y puerto origen destino.
- Soporte ipv4 e ipv6
- Capacidad de asegurar que los usuarios utilicen únicamente las direcciones previamente asignadas por el servidor DHCP autorizado.
- Capacidad de revisar que los paquetes ARP vienen de direcciones IP válidas (Dynamic ARP Inspection)
- Prevenir el tráfico IP de direcciones IP con direcciones MAC que no correspondan a la tabla de DHCP
- Soporte de IEEE 802.1AK (MVRP) para el manejo de VLANs DINAMICAS, simplificando la administración de la red.
- Soportar CoS/QoS
- Soportar 802.1p

➢ Soportar DSCP ➢ Asignación de VLAN y QoS basados en perfiles en la autenticación de red RADIUS 802.1x ➢ Priorización de tráfico basado en MAC-address, VLAN, port, origen IP, destinoIP, puerto de origen o puerto de destino. ➢ Filtrado de tráfico entrante basado en dirección MAC origen / destino, Ethertype, dirección Origen IP, dirección destino IP, puerto origen / destino TCP puerto origen / destino UDP

D. AQUISICIÓN DE TECNOLÓGIA POR OBSOLESCENCIA Y FIN DE VIDA UTIL DE SWITCHES DE OFICINA DE 24 PUERTOS

Instalación, configuración y reemplazo de cinco (5) Switch de oficina de mínimo 24 puertos en cobre 1GbE + 4 uplink SFP/SFP+ (10 GbE) Juniper EX2300-24P POE+.

REQUISITOS TÉCNICOS SWITCH
ESPECIFICACIONES FÍSICAS PARA LOS SWITCH
• Los equipos ofertados deben soportar el mismo sistema operativo en acceso y Core. • El arreglo de switches debe verse física y lógicamente en el sistema de gestión como unúnico switch • Presentación en tipo chassis o virtualización de chassis (modular) que permita ver al conjuntode equipos modulares como un único equipo lógico y físico. • Los switches deben interconectarse entre sí mediante puertos de fibra independientes a los24 puertos de acceso, ofreciendo un backplane mínimo 80Gbps • La capacidad de conmutación mínima de cada uno de los switches que compongan el arreglodebe ser de 128Gbps.
REQUISITOS TÉCNICOS SWITCH
• Garantizar la existencia física de cómo mínimo 2 switches que actúen uno como Routing Engine (RE) Principal y el otro como Backup • Debe contar con una funcionalidad Graceful Route Engine Switch over (GRES) que permita al arreglo de switches continuar enrutando paquetes en el evento de falla del switch que actúa como Routing Engine (RE) Principal • Debe permitir que si falla uno de los switches del arreglo, se pueda extraer el switch que falla,sin afectar la conmutación de paquetes del resto de switches y sin necesidad de intervención humana para reconfigurar tablas de enrutamiento. • Debe permitir que al ingresar un switch al arreglo para reemplazar algún otro que esté fallando, el arreglo se encargue de actualizar el sistema operativo del nuevo switch de formaautomática y sin detener el enrutamiento de paquetes del arreglo de switch. • Soporte de puertos de 10/100/1000 autosense para acceso en todos los puertos • Soporte de 4 puertos 1/10Gbps para fibras MM y SM • Detección automática de puertos DCE o DTE (MDI-MDIX) • Soporte de IPv6: El equipo a nivel de hardware y software debe estar listo para implementarIPV6 • Los circuitos encargados de nivel 3 de las controladoras, deben realizar el balanceo de carga,mediante el soporte de protocolo VRRP, para crear defaults gateways virtuales dentro de lared y garantizar que

en caso de que ocurra alguna falla en los circuitos de nivel 3 de una tarjeta controladora, otro equipo de nivel 3 pueda tomar el control, sin que la dirección IP deldefault Gateway de los equipos de red cambie, garantizando transparencia y alta disponibilidad para los usuarios/servicios conectados en cada VLAN.

- Todas las unidades deben poderse montar en racks de 19 pulgadas los herrajes deben ser incluidos por cada equipo
- Indicadores visuales de estado de puertos y sistema
- Todos deben incorporar tecnología (EEE) o amigable con el ambiente.

CAPACIDADES DE SWITCHING

Capa 2:

- Soporte de tramas estándar y jumbo frames
- Soporte de más de 16.000 MAC address
- Listas de acceso de nivel 2
- Soporte de 4,093 VLANS (más de 2000 Vlans activas)
- Soporte 802.1Q (vlan Tagging)
- Debe estar en propiedad de controlar tormentas de Broadcast, multicast y unicast.
- Mapeo ARP estático
- Soporte de link agregation
- 802.1D, 802.3X, 802.1w
- Mirroring local o remoto para supresión remota de tráfico en el puerto o VLAN
- Procesamiento distribuido que garantice wirespeed

Capa 3:

- Soporte de rutas estáticas
- Soporte de multicast
- Soporte CIDR
- Soporte UDP y TCP
- DHCP
- DNS
- Listas de acceso basadas en IP origen y destino, y puerto origen destino.
- Soporte ipv4 e ipv6
- Capacidad de asegurar que los usuarios utilicen únicamente las direcciones previamente asignadas por el servidor DHCP autorizado.
- Capacidad de revisar que los paquetes ARP vienen de direcciones IP válidas (Dynamic ARP Inspection)
- Prevenir el tráfico IP de direcciones IP con direcciones MAC que no correspondan a la tabla de DHCP
- Soporte de IEEE 802.1AK (MVRP) para el manejo de VLANs DINAMICAS, simplificando la administración de la red.
- Soportar CoS/QoS
- Soportar 802.1p
- Soportar DSCP
- Asignación de VLAN y QoS basados en perfiles en la autenticación de red RADIUS 802.1x
- Priorización de tráfico basado en MAC-address, VLAN, port, origen IP, destinoIP,

puerto de origen o puerto de destino.
- Filtrado de tráfico entrante basado en dirección MAC origen / destino, Ethertype, dirección Origen IP, dirección destino IP, puerto origen / destino TCP puerto origen / destino UDP.

Requerimientos técnicos adicionales para los ítems A, B, C y D, del presente documento:

Producto	Requerimiento	Unidad de medida
REQUISITOS TÉCNICOS SWITCHES	**Compatibilidad con Estándares:** IEEE 802.1D (STP) IEEE 802.1p (CoS) IEEE 802.1Q (VLANs) IEEE 802.1w (RSTP) IEEE 802.1X (Seguridad) IEEE 802.3 (Ethernet) IEEE 802.3ad (Agregación de enlaces) IEEE 802.3ab (100Base-T) IEEE 802.3u (Fast Ethernet) IEEE 802.3x (Control de Flujo) IEEE 802.3z (Gigabit Ethernet) **Gestión de Red y Elementos de Red:** Permitir la administración a través de interfaz gráfica y de comandos (CLI). Poseer puerto de consola local y cables necesarios para conexión al puerto decomunicaciones del PC (DB9) Soportar 4 grupos de RMON (statistics, history, alarm y events) Soportar MIB II Soportar RIPv2- MIB Capacidad de lmacenamiento y restauración de imágenes de software y deconfiguración del equipo (Backup y Restore), TFTP, FTP. Los equipos deben ser 100% compatibles con el software de administración que se pueda adquirir con la marca.	

Producto	Requerimiento	Unidad de medida
MÓDULOS TRANSCEPTORES SFP	módulos transceptores SFP modelo EX-SFP-10GE-SR, con el fin de interconectar varios Switches 10 GB	30 módulos SFP
REEMPLAZO DE EQUIPOS	El oferente deberá realizar el reemplazo de los equipos obsoletos en cada sede de la SNR a nivel nacional, así mismo, deberá realizar la instalación y parametrización de los mismos, remitirse al documento "**ANEXO EQUIPOS JUNIPER**". **Nota: La Superintendencia se encargará de realizar el envío de los dispositivos a cada sede.**	
SOFTWARE DE ADMINISTRACIÓN Y MONITOREO	Plataforma de monitoreo y gestión centralizada para la plataforma Juniper con el fin de aplicar políticas de red, gestión desde un solo panel para los equipos, actualizaciones automáticas de software y monitoreo de su disponibilidad, por un año.	Licenciamiento por 1 año
GARANTIA	• Contrato de servicios por un (1) año que asegure el remplazo de partes al siguiente día hábil en sitio, garantizando el correcto funcionamiento de los equipos activos, actualizaciones ilimitadas de software durante la vigencia de la garantía y soporte 7x24 remoto y/o telefónico a través de Technical Assistance del fabricante. Adicional se debe asegurar que la SNR tenga acceso directo al portal del fabricante con cuentas de la SNR y autorizadas por el fabricante para descargar versiones de software, acceso a la base de conocimiento y permitir la creación de casos de soporte o requerimientos RMA. Durante el tiempo de garantía el contratista deberá para los equipos de switch de oficina: • Soporte telefónico y/o remoto a través de una mesa de ayuda o centro de soporte en modalidad 7x24 por un periodo de un (1) año, provisto directamente por el fabricante. • Derecho a actualizaciones ilimitadas (UPDATE y UPGRADE) de las versiones de software entregadas durante un (1) año, provisto directamente por el fabricante a la entidad. • Soporte de hardware: Se deberá garantizar reemplazo de partes o equipos al siguiente día hábil de reportada la falla y autorizado el RMA por parte del fabricante, provisto directamente por el fabricante durante el tiempo de la garantía.	

Producto	Requerimiento	Unidad de medida
	• Tiempo de Respuesta Telefónica inmediato.	
INSTALACION	• Se deben incluir todos los accesorios originales para montaje en rack de la oficina. • El proponente debe adjuntar carta del fabricante que avale la solución presentada cumple con lo solicitado por la Entidad.	
Horas de Soporte Especializado	40 horas de especialista dedicado para nuevas configuraciones de networking (a parte del soporte 7x24 indicado en el ítem anterior) estas horas pueden ser proporcionadas por el proveedor o canal seleccionado. Renovación de dos (02) certificados willcard con Digicert a nombre de la Superintendencia de Notariado y Registro (por un (01) año)	
Certificado Fabricante	Se deberá adjuntar certificación emitida directamente por el fabricante, las cuales acrediten que el proponente es un canal autorizado y que cuenta con personal capacitado y certificado para manejar la solución ofertada. Adicionalmente, el proponente deberá adjuntar certificación expedida por el fabricante correspondiente, donde se autorice al oferente la presentación de oferta para el presente lote y se avale la respectiva propuesta técnica presentada por el mismo, garantizando así, el cumplimiento de los requisitos técnicos solicitados por la Superintendencia de Notariado y Registro (SNR)	

Nota: El contratista debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que su personal asignado al proyecto pueda cumplir con las obligaciones del contrato. Estos valores no incurrirán en costos adicionales para la Superintendencia de Notariado y Registro.

E. ADQUISICIÓN TECNOLÓGICA DE DDI

A continuación, se relacionan las especificaciones técnicas mínimas y su respectiva descripción para la adquisición del fortalecimiento del esquema tecnológico para la solución DDI requerida por la SNR. El alcance se compone de los siguientes elementos:

REQUISITOS TÉCNICOS SWITCH
ESPECIFICACIONES FÍSICAS PARA LA SOLUCION DDI
• Adquirir una solución de red que ofrezca gestión centralizada de los servicios DNS, DHCP e IPAM (IP Address Management), conocida como DDI en configuración HA y con redundancia geográfica; • Soporte técnico especializado (local y fabrica); • Capacitación certificada.
REQUISITOS TÉCNICOS SOLUCION DDI
La plataforma debe contar con dos equipos (appliance) en topología HA y un equipo (appliance) para redundancia geográfica, que soporten cada uno mínimo las siguientes características: • Minimo 67k QPS (peticiones DNS por segundo) • Mínimo 350 LPS (peticiones DHCP) • Fuentes de potencia redundantes “hot-swappable” • Gestión centralizada de la solución desde el mismo cluster, sin requerir un equipo adicional • La solución deberá tener dentro de la arquitectura, software reporteador con maximo 1GB de indexación por día, a ser instalado en servidor virtual de la Entidad. Las características mínimas que debe cumplir son: • La solución debe ser administrable centralizadamente desde una única conexión (HTTPS) al elemento de gestión de la solución DDI. • La solución debe utilizar una base de datos para el manejo de la información de los servicios DDI (IPs, Redes, Zonas, Registros, Rangos DHCP, etc.) embebida en el sistema operativo que no requiere instalación, configuración o mantenimiento manual, • La solución debe estar en capacidad de ofrecer diversos mecanismos de redundancia para la Gestión de la solución, incluyendo redundancia Intra-datacenter y redundancia Geográfica. • La solución deberá estar conformada por dos equipos físicos en configuración HA para el datacenter principal y un equipo físico para redundancia geográfica, desde los cuales se efectuará la gestión centralizada a ser instalado en el sitio principal y a la vez, realizarán los servicios de DNS y DHCP. • La solución debe estar basada en equipos físicos capaz de ejecutar las funciones de DNS, DHCP e IPAM en el mismo servidor/dispositivo (DDI). • Los equipos de la solución deben tener disponible el servicio NTP (stratum 2) para ofrecer el servicio NTP a otros dispositivos en la red • Todos los equipos que conforman la solución deberán soporta IPv4, IPv6 y dual stack a nivel de conectividad y de entrega de servicios. • La solución debe ofrecer una interfaz de tipo API Restful (web API) para integración con productos de terceros • Los equipos de la solución deben poder almacenar log localmente o direccionar log a un servidor syslog externo • La solución debe ofrecer la posibilidad de autenticar los usuarios que acceden el sistema con base en una base de datos de usuarios local, o integrándose a bases de datos de usuarios externas incluyendo Directorio Activo, LDAP, Radius, TACAS+ • La solución debe ofrecer Role Base Access (administración granular basada en Roles)

- La solución debe ofrecer Flujos de trabajo o workflows basados en grupo de usuarios con distintos niveles de permisos.
- La solución debe ofrecer auditoria para cada sesión administrativa de la solución de Automatización de Red.
- La solución debe poder Importar información de DDI desde archivos CSV de manera automática
- Las maquinas de la solución deberán estar asegurados (Hardening) de fábrica y no ofrecer acceso al súper usuario o cuenta root.
- El firmware o S.O. de la solución debe contar con al menos una certificación de seguridad lógica dada por una organización de estandarización de reconocimiento global

Características generales de DNS, DHCP, & IPAM

El oferente deberá demostrar todas las características técnicas requeridas a continuación:

- La solución debe incluir una base de datos autoritativas para la administración de Redes e IPs tanto para IPv4 como IPv6
- La solución de IPAM deberá estar totalmente integrado al funcionamiento de los servicios DNS y DHCP y deberá albergar los registros requeridos para la centralización de la gestión de los datos DNS y DHCP.
- La interface gráfica de la solución de IPAM debe presentar la información en formato de lista de redes, mapas de redes y mapas de IPs
- Los mapas de IPs de la solución IPAM deberán visualizar/incluir los siguientes tipos de información acerca del estatus del direccionamiento IP de una red seleccionada:
    - Direcciones IP no utilizadas.
    - Direcciones IP en Conflicto.
    - Direcciones IP utilizadas.
    - Direcciones IP seleccionadas.
    - Rangos de DHCP dentro de la red.
    - DHCP Ónique Identifier (DUID) en el caso de IPv6.
    - Direcciones IP no administradas o que no dispongan de registros o clasificaciones asignadas (unmanaged).
    - Reservaciones de direcciones fijas.
    - Objetos que son utilizados para configuración DNS.
    - Direcciones IP que no hayan sido configuradas por los servicios de DNS y DHCP.
    - Direcciones IP que tengan Leases Activos DHCP.
    - Rangos de direcciones IP de exclusión de DHCP.
    - Objetos asociados con las distintas direcciones IP, por ejemplo, leases, rangos DHCP ó direcciones fijas.
    - Nombres de los objetivos asociados con las direcciones IP.
    - Direcciones MAC descubiertas del host.
    - Tipo de dispositivo o DHCP “fingerprint”, ó ID del fabricante obtenido mediante la transacción DHCP.
- La solución de IPAM debe ofrecer la capacidad de agrupación de redes IPv4 e IPv6 en grupos o contenedores así como asistir en la gestión de estas redes incluyendo crear redes, unir, redimensionar, dividir, borrar, etc.
- Los appliances ofrecidos deben soportar la implementación de cualquier rol de DNS, incluyendo:

autoritativo (primario o secundario), forwarding, recursivo y caching.

- La solución de DNS debe soportar diversos mecanismos de Alta disponibilidad para DNS, incluyendo redundancia Intra-datacenter y redundancia Geográfica
- La solución de DNS debe soportar Anycast para el servicio de DNS
- La solución debe incluir soporte nativo para advertising de IPs Anycast por OSPF y BGP
- La solución debe poder agrupar varios servidores DNS como un objeto de tipo Grupo al cual se enlazaran diferentes servicios y configuraciones haciendo referencia al grupo directamente.
- La solución debe soportar vistas DNS (o DNS Split) basadas en IPs de clientes (Client Match) y basadas en IPs del servicio DNS (Dest. Match)
- La solución de DNS debe poder Ordenar las respuestas DNS para consultas tipo A y AAAA, dependiendo de la IP o Red desde donde se origina la consulta. De esta manera los clientes podrán utilizar la IP mas adecuada para acceder a un nombre de dominio que tiene mas de una IPv4 o IPv6.
- La solución DNS debe permitir la direccion Link-local IPv6 en un registro tipo Host.
- La solucion DNS debera permitir la asignacion del prefijo IPv6 – Global IPv6 Prefix.
- La solución deberá permitir la configuración de Controles de Acceso DNS, Ya sea ACEs (Access Control Entries) ó utilizar ACL (Access Control List) para determinar cuáles hosts/usuarios pueden acceder a servicios o funciones específicas del DNS.
- La solución de DNS debe soportar zonas directas (forward) autoritativas, zonas reversas autoritativas y delegación de zonas
- La solución debe utilizar plantillas de nombres de host de forma masiva (bulk-host), que permitan aplicar reglas para dichos nombres.
- La solución de DNS deberá poder realizar actualizaciones/transferencias de zonas DNS de manera segura mediante la utilización de TSIG (Transactional Signatures)
- La solución de DNS debe soportar IDNs (Internationalized Domain Names) para las zonas DNS y registros de recursos que permitan proveer de flexibilidad como especificar nombres de dominio en caracteres que no estén en inglés. La solución debe cumplir los siguientes RFC sobre IDN: 3492, 5890, 5891, 5892, 5893, 5894, 5895, 6452
- La solución debe soportar actualizaciones dinámicas de DNS (DDNS), ya sea sin autenticación ó mediante autenticación GSS-TSIG (Generic Security Service-Transaction Signatures)
- Las actualizaciones DDNS pueden ser limitadas por servidor DHCP para controlar todas las actualizaciones DDNS
- La solución debe ofrecer soporte completo para asignar direcciones IPv4 e IPv6 a través de DHCP
- La solución debe soportar redundancia a través de DHCP Failover. esta capacidad deberá permitir que los equipos brinden este servicio en modo Activo -Activo para un mismo pool o scope de Direcciones IP, garantizando la continuidad del servicio a pesar de estar ubicados en distintas zonas geográficas.
- La solución debe mostrar las asignaciones DHCP actuales, y el histórico de asignaciones de DHCP, incluyendo los datos de IPs asignadas, servidor DHCP, MAC o dispositivo, información de tiempos, entre otros.
- La solución debe ofrecer visibilidad del histórico de asignaciones para poder ver las direcciones asignadas en un instante de tiempo especifico
- La solución de DHCP debe ofrecer la capacidad de configurar direcciones DHCP reservadas/fijas
- La solución debe ofrecer la capacidad para convertir fácilmente una dirección DHCP asignada en una dirección DHCP estática o reservada/fija

• La solución debe permitir la configuración de rangos de exclusión para DHCP • La solución de DHCP debe mostrar las asignaciones activas dentro de la interface grafica • La solución de DHCP deberá identificar y presentar posibles conflictos de IPs. • La solución debe proveer las estadísticas de utilización DHCP para que los administradores puedan ver fácilmente el nivel de utilización y disponibilidad de un rango de IPs. • La solución debe ofrecer la posibilidad de borrar/liberar las asignaciones DHCP existentes desde la interface grafica • La solución debe ofrecer la habilidad para enviar alertas de notificaciones cuando un rango DHCP alcanza un limite o umbral configurado • La solucion debe permitir la asignacion de varios rangos v6 sobre el mismo servidor • La solución debe mantener registros de auditoria para cada dirección IP de todos los sistemas (ej. direcciones MAC) que han sido asignadas a esas direcciones IP • La solución debe ofrecer una interface grafica que permita configurar las diferentes opciones y espacios DHCP tanto en IPv4 e IPv6, predefinidas y personalizadas para proveer configuraciones e información específica a los clientes DHCP. • La solución debe ofrecer la capacidad para configurar opciones de fabricantes (Vendor Options) para el servicio de DHCP incluyendo opciones específicas para dispositivos de VoIP ó para clientes que no sean Windows.
INSTALACIÓN
• La Entidad entregara la conexión a cero metros para la instalación de los appliances. • El oferente debe realizar la configuración y puesta en funcionamiento de los equipos • El proponente debe adjuntar carta del fabricante que lo acredite como canal.
GARANTIA
• Contrato de servicios por un (1) año garantizando el correcto funcionamiento de los equipos activos, actualizaciones ilimitadas de software durante la vigencia de la garantía y soporte 7x24 remoto y/o telefónico suministrado directamente por el fabricante de los equipos • Derecho a actualizaciones ilimitadas (UPDATE y UPGRADE) de las versiones de software entregadas durante un (1) año, provisto directamente por el fabricante a la entidad. • Tiempo de Respuesta Telefónica inmediato.

F. ESPECIFICACIONES TÉCNICAS MÍNIMAS LICENCIAMIENTO HERRAMIENTA PARA EL MONITOREO DE ACTIVIDADES DE ESTACIONES DE TRABAJO.

REQUISITOS TÉCNICOS
MONITOREO ACTIVIDAD USUARIOS
• El software debe monitorear la actividad de los usuarios en sesiones remotas y/o locales • El software debe estar en capacidad de registrar usuarios con múltiples monitores • La solución debe registrar solo la ventana activa • La solución debería monitorear la actividad del portapapeles. • La solución debería registrar las pulsaciones de teclas introducidas en cualquier aplicación o sitio web

con capacidad de búsqueda futura.
- El software debe admitir grabación de audio.
- El software debe monitorear la carga de archivos.
- La solución debe monitorear el uso del dispositivo USB.
- La solución debe monitorear los sitios web visitados.
- El software debe monitorear las IPs remotas desde las cuales se ha accedido al sistema y filtrar las sesiones por dirección IPs remota.
- La solución debe monitorear las sesiones de visualización en vivo en tiempo real.
- El software debe registrar la actividad del usuario dentro de la salida de la sesión de Linux.
- La solución debe tener la posibilidad de registrar la actividad del usuario en función de las alertas activadas.
- El software debe anonimizar los datos del usuario en las sesiones de usuario.
- La solución debería permitir exportar los resultados del monitoreo para verlos en el futuro como video.
- La solución debe cifrar todos los datos confidenciales, incluidas las pulsaciones de teclas registradas.
- La solución debería permitir deshabilitar la monitorización de pulsaciones de teclas dentro de aplicaciones específicas.
- La solución debe notificar al usuario que la sesión está siendo grabada.
- El software debe admitir la búsqueda de múltiples parámetros en los resultados del monitoreo.
- La solución debe registrar todas las acciones del usuario al administrar el software y trabajar con él y monitorear los resultados, con opciones de filtrado.
- La solución debería registrar la entrada de Linux.
- La solución debería permitir archivar sesiones de usuario.
- El software debería permitir ver las sesiones de usuario desde el archivo.
- El software debería permitir exportar capturas de pantalla separadas.
- La solución debe validar los resultados de las exportaciones para garantizar la integridad de los datos.
- La solución debe validar los resultados del monitoreo para garantizar la integridad de los datos monitoreados.
- El software debería permitir filtrar usuarios durante el monitoreo.
- La solución debería permitir filtrar aplicaciones/sitios web durante la monitorización.
- La solución debe monitorear la actividad del usuario solo durante las horas de trabajo asignadas.
- El software debe detectar desviaciones en el uso de computadoras/inicios de sesión (computadoras/inicios de sesión poco utilizados)
- La solución debe detectar automáticamente los puntos finales monitoreados que se utilizan fuera del horario laboral.
- La solución debe detectar automáticamente los estados inactivos de los puntos finales monitoreados y mostrar el tiempo de inactividad del usuario frente al tiempo activo del usuario en los informes.
- La solución debería permitir archivar o eliminar datos del almacenamiento durante un determinado agente, tiempo o período, dejando intactos los metadatos.
- El software debe enviar notificaciones automáticas por correo electrónico cuando un punto final monitoreado haya estado fuera de línea durante un período de tiempo.

LICENCIAMIENTO

- La solución debería tener licencias de punto final flotantes
- La solución debería permitir licencias separadas para aplicaciones y funciones.
- La solución debe admitir licencias basadas en el usuario.

PLATAFORMAS SOPORTADAS

- El software debe admitir la supervisión de estaciones de trabajo y servidores Windows, Mac, Linux, SELinux y Citrix.
- El software debe admitir la supervisión de Amazon WorkSpaces.
- El software debe ser compatible con entornos VDI con supervisión VDI no persistente y licencias flotantes.
- El software debe soportar la monitorización del sistema de Window X.
- La solución debería monitorear la actividad del usuario y filtrar sitios web en clientes macOS.
- La solución debería monitorear la actividad del usuario en Ubuntu 22.4 con un entorno de escritorio Wayland.
- El software debe ser compatible con el reenvío de Window X.
- La solución debe soportar la monitorización de AIX.
- La solución debe tener la posibilidad de grabar AppStream y Azure VDI/App

DESARROLLO

- El software debe tener una versión local
- La solución debería tener versión SaaS.
- La solución debe tener un panel maestro para monitorear la actividad del usuario desde múltiples implementaciones aisladas en una sola interfaz.
- El software debe ser compatible con el modo multi-tenant
- La solución debe proporcionar una interfaz web para la gestión de software y datos monitoreados.
- El software debe instalar los clientes a través de la interfaz web.
- La solución debe admitir modos de alta disponibilidad y recuperación ante desastres con soporte de balanceador de carga de red.
- La solución debería reducir el uso del ancho de banda ajustando el tamaño de las capturas de pantalla grabadas.
- La solución debe soportar la gestión de problemas del servidor central y el tamaño de la base de datos con notificaciones por correo electrónico para los problemas.
- El software debe admitir la actualización automática de todos los componentes.
- La solución debe admitir Azure SQL como tipo de almacenamiento.
- La solución debe admitir una conexión de base de datos cifrada.
- ¿La solución debería soportar una base de datos SQL como almacenamiento?
- La solución debe soportar el almacenamiento en los almacenamientos de objetos.
- La solución debe soportar el almacenamiento de archivos.
- La solución debe admitir grupos multijerárquicos para proporcionar almacenamiento de claves privadas.
- La solución debería tener una API.
- La solución debería permitir la visualización de sesiones a través de la API.

ACCESO Y MANEJO DE ALERTAS

- La solución debería controlar los dispositivos USB con la posibilidad de bloquear ciertas clases de dispositivos.
- El software debe admitir el acceso multiusuario con permisos personalizados.
- La solución debería bloquear los dispositivos USB automáticamente en caso de violaciones de seguridad o posible pérdida de datos.
- El software debe permitir la detección de parámetros de pulsaciones de teclas para detectar infracciones de seguridad.
- La solución debe proporcionar protección a nivel de kernel contra la detención del proceso de monitoreo y el cambio/borrado de cualquier archivo de registro de sesión, incluso para usuarios con privilegios de administrador.
- La solución debe utilizar la expresión regular para la protección de las reglas de alerta.
- El software debe admitir la autenticación de dos factores para los usuarios que inician sesión en el equipo monitorizado a través de TOTP.
- El software debe admitir la autenticación secundaria para los usuarios que inician sesión en el equipo monitorizado con credenciales adicionales para una protección avanzada del sistema.
- El software debe bloquear a los usuarios manual o automáticamente al detectar acciones prohibidas.
- La solución debe eliminar las aplicaciones no permitidas detectadas que utiliza un usuario.
- El software debe permitir/prohibir el acceso de los usuarios al sistema monitorizado en función de una lista negra.
- La solución debería requerir que los usuarios proporcionen un comentario antes de acceder al sistema monitoreado.
- La solución debe integrarse con el directorio activo.
- El software debe integrarse con SIEM.
- La solución debe registrar eventos cuando un cliente se conecta o desconecta para la integración con el sistema SIEM.
- La solución debe integrarse con los sistemas WebLogin.
- El software debe integrarse con SAML.
- La solución debe integrarse con onelogin a través de SAML.
- El software debe integrarse con Okta a través de SAML
- La solución debe restringir el acceso del usuario al entorno corporativo según el horario laboral.
- La solución debe integrarse con el Servidor de Certificados para solicitar acceso con aprobación de seguridad.
- El software debe proporcionar una vista de página única para todas las solicitudes de acceso, como solicitudes de contraseñas de un solo uso, acceso a puntos finales y solicitudes de acceso a almacenamiento masivo.
- La solución debe proporcionar detección en tiempo real basada en reglas de comportamientos anormales del usuario.
- El software debe proteger el registro de auditoría interna de modificaciones.

REPORTES

- El software debe exportar datos de monitorización estadística en formatos xlsx o xls.
- La solución debe tener paneles de productividad.
- La solución debe tener un motor de informes integrado para la generación de informes con múltiples

parámetros. • El software debe crear informes a través del programador. • El software debe integrarse con Power BI. • El software debe proporcionar plantillas de exportación para Microsoft Power BI. • La solución debería poder analizar la frecuencia de uso de la aplicación y la frecuencia de las visitas al sitio. • El software debería admitir la gestión de incidencias del servidor central y el tamaño de la base de datos con notificaciones por correo electrónico para problemas. • El software debería permitir la personalización de los informes.
MANEJOS DE CONTRASEÑAS
• La solución debería gestionar las contraseñas para acceder a Windows Server, servidores Linux, sistemas basados en web, MS SQL Server Management Studio y Active Directory. • La solución debería permitir el registro selectivo de la actividad solo para usuarios privilegiados. • El software debería tener la posibilidad de crear una lista de puntos finales permitidos para el uso de secretos. • La solución debería detectar y incorporar cuentas privilegiadas locales de Windows. • La solución debería detectar e incorporar cuentas privilegiadas de Active Directory. • La solución debería admitir la incorporación de cuentas detectadas en secretos mediante acciones masivas. • La solución debería permitir configurar las reglas de detección para la detección automatizada de cuentas privilegiadas. • La solución debería admitir la rotación remota de contraseñas. • La solución debe proporcionar una navegación rápida a un secreto y permitir una navegación sencilla a las sesiones de usuario donde se utilizó un secreto específico. • La solución debe admitir solicitudes de acceso a secretos en PAM con opciones para elegir el tipo de acceso. • La solución debería tener una credencial de aplicación rota para el módulo PAM. • El software debe utilizarse para administrar contraseñas personales. • El software debe permitir procedimientos de transferencia de archivos mediante la gestión de contraseñas.
INSTALACIÓN
• El oferente debe realizar la configuración del software en un mínimo de 50 estaciones de trabajo a través de servicios profesionales del fabricante. • El proponente debe adjuntar carta del fabricante que lo acredite como canal, avale la solución presentada a la Entidad y se comprometa a realizar la instalación requerida con personal propio
GARANTIA
• Contrato de licenciamiento por un (1) año • Tiempo de Respuesta Telefónica inmediato.

4.2. ESPECIFICACIONES TÉCNICAS MÍNIMAS – RENOVACIÓN DE SOPORTE TÉCNICO; LICENCIAMIENTO Y GARANTÍA DE EQUIPOS DE NETWORKING Y SEGURIDAD PERIMETRAL:

Ítem	Cantidad	Descripción
1	2	Renovación Soporte y garantía Firewall Juniper SRX4200-SYS-JB-AC por un (1) año.
2	2	Renovación Soporte y garantía Firewall Juniper SRX4100-SYS-JB-AC por un (1) año.
3	1	Renovación Soporte y garantía Firewall Juniper SRX300 por un (1) año.
4	4	Renovación Soporte y garantía switch EX4600-40F-AFO por un (1) año.
5	2	Renovación Soporte y garantía switch EX3400-48P por un (1) año.
6	112	Renovación Soporte y garantía switch EX2300-24P por un (1) año.
7	79	Renovación Soporte y garantía switch EX2300-48P por un (1) año.
8	2	Renovación Licenciamiento IPS, AppSecure, URL Filtering, Cloud AV and AS, SKYATP, Sec Intel, with SW Support para SRX4200 por un (1) año.
9	2	Renovación Licenciamiento IPS, AppSecure, URL Filtering, Cloud AV and AS, SKYATP, Sec Intel, with SW Support para SRX4100 por un (1) año.
10	6	Renovación Soporte y garantía Switch QFX5120-48T-AFO por un (1) año.
11	41	Renovación Soporte y garantía Switches EX2300-48MP por un (1) año.
TOTAL	**253**	

Teniendo en cuenta el cuadro anterior se describe la necesidad:

DESCRIPCIÓN DE EQUIPOS A RENOVAR					
Support Coverage	**Product Name**	**Quantity**	**Start Date**	**End Date**	**Serial Number**
SVC-ND-EX23-48MV	EX2300-48MP	40	16-Dec-2025	15-Dec-2026	XP3122290034 XP3122290040 XP3122290043 XP3122290048 XP3122290049 XP3122290060 XP3122290064 XP3122290065 XP3122290071

					XP3122290073
					XP3122290076
					XP3122290077
					XP3122290079
					XP3122290083
					XP3122290087
					XP3122290088
					XP3122290162
					XP3122290164
					XP3122290168
					XP3122290171
					XP3122290026
					XP3122290024
					XP3122290022
					XP3122290020
					XP3122290019
					XP3122290017
					XP3122290015
					XP3122160055
					XP3122290032
					XP3122290197
					XP3122290196
					XP3122290195
					XP3122290194
					XP3122290192
					XP3122290189
					XP3122290187
					XP3122290186
					XP3122290182
					XP3122290181
					XP3122290178
SVC-ND-QFX51-48T	QFX5120-48T-AFO	6	16-Dec-2025	15-Dec-2026	WJ4924470335
					WJ4924470173
					WJ4924470123
					WJ4924470117
					WJ4924470071
					WJ4924470424

SVC-ND-EX23-48T	EX2300-48T	1	16-Dec-2025	15-Dec-2026	JX3622191373
SVC-ND-SRX300HW	SRX300	1	16-Dec-2025	15-Dec-2026	CV2120AN1597
SVC-ND-SRX4200JB	SRX4200-SYS-JB-AC	1	16-Dec-2025	15-Dec-2026	DK3521AR0231
SVC-ND-SRX4100JB	SRX4100-SYS-JB-AC	1	16-Dec-2025	15-Dec-2026	DJ2418AR0094
SVC-ND-SRX4200JB	SRX4200-SYS-JB-AC	1	16-Dec-2025	15-Dec-2026	DK3521AR0168
SVC-ND-SRX4100JB	SRX4100-SYS-JB-AC	1	16-Dec-2025	15-Dec-2026	DJ2418AR0088
SVC-ND-EX460040F	EX4600-40F-AFO	4	16-Dec-2025	15-Dec-2026	TC4924320159 TC4924320108 TC4924320102 TC4924320096
SVC-ND-EX34-48P	EX3400-48P	2	16-Dec-2025	15-Dec-2026	NY4823361914 NY4823362280
SVC-ND-EX23-24P	EX2300-24P	112	16-Dec-2025	15-Dec-2026	JY4823370853 JY4823370851 JY4823370848 JY4823370837 JY4823370836 JY4823370835 JY4823370829 JY4823370826 JY4823370824 JY4823380504 JY4823370988 JY4823370938 JY4823370934 JY4823370877 JY4823370870 JY4823370868 JY4823370867 JY4823370864 JY4823370862 JY4823370860 JY4823370856

					JY4823371797
					JY4823371795
					JY4823371784
					JY4823371782
					JY4823371764
					JY4823371752
					JY4823371735
					JY4823371220
					JY4823371244
					JY4823371266
					JY4823371301
					JY4823371310
					JY4823371320
					JY4823371321
					JY4823371346
					JY4823371380
					JY4823371402
					JY4823371408
					JY4823371499
					JY4823371601
					JY4823371725
					JY4823371215
					JY4823371206
					JY4823370763
					JY4823370761
					JY4823370700
					JY4823370676
					JY4823370671
					JY4823370628
					JY4823370610
					JY4823370300
					JY4823370812
					JY4823370796
					JY4823370785
					JY4823370773
					JY4823370175
					JY4823370173

					JY4823370172
					JY4823370171
					JY4823370168
					JY4823370161
					JY4823370154
					JY4823370151
					JY4823370144
					JY4823370142
					JY4823370141
					JY4823370139
					JY4823370137
					JY4823370128
					JY4823370124
					JY4823370120
					JY4823370119
					JY4823370114
					JY4823370108
					JY4823370101
					JY4823370097
					JY4823370095
					JY4823370093
					JY4823370076
					JY4823370068
					JY4823370066
					JY4823370059
					JY4823370055
					JY4823370051
					JY4823370046
					JY4823370043
					JY4823370039
					JY4823370022
					JY4823370021
					JY4823370020
					JY4823370014
					JY4823370009
					JY4823370005
					JY4823370292

					JY4823370286
					JY4823370282
					JY4823370269
					JY4823370179
					JY4823370180
					JY4823370181
					JY4823370184
					JY4823370185
					JY4823370187
					JY4823370193
					JY4823370200
					JY4823370219
					JY4823370230
					JY4823370238
					JY4823370246
					JY4823370261
					JY4823370263
					JW4824280226
					JW4824280216
					JW4824280211
					JW4824280200
					JW4824280190
					JW4824280188
					JW4824280182
					JW4824280180
					JW4824280179
					JW4824280176
					JW4824280162
					JW4824280154
					JW4824280148
					JW4824280139
					JW4824280138
					JW4824280136
					JW4824280133
					JW4824280128
					JW4824280126
SVC-ND-EX23-48P	EX2300-48P	79	16-Dec-2025	15-Dec-2026	JW4824280125

					JW4824280119
					JW4824280111
					JW4824280110
					JW4824280108
					JW4824280087
					JW4824280083
					JW4824280064
					JW4824280059
					JW4824280055
					JW4824280051
					JW4824280045
					JW4824280032
					JW4824280027
					JW4824280015
					JW4824280014
					JW4824280005
					JW4824260246
					JW4824260063
					JW4824240801
					JW4824280230
					JW4824280406
					JW4824280418
					JW4824280443
					JW4824280460
					JW4824280475
					JW4824280477
					JW4824280480
					JW4824280486
					JW4824280502
					JW4824280532
					JW4824280533
					JW4824280537
					JW4824280540
					JW4824280549
					JW4824280556
					JW4824280560
					JW4824280587

					JW4824280624
					JW4824280677
					JW4824280390
					JW4824280388
					JW4824280344
					JW4824280342
					JW4824280310
					JW4824280306
					JW4824280301
					JW4824280300
					JW4824280296
					JW4824280295
					JW4824280291
					JW4824280289
					JW4824280288
					JW4824280287
					JW4824280275
					JW4824280271
					JW4824280268
					JW4824280256
					JW4824280250
					JW4824280239

Horas Dedicadas de Soporte Especializado	20 horas de especialista dedicado para nuevas configuraciones en los equipos de SRX4200 y SRX4100 (a parte del soporte 7x24 indicado en el ítem anterior) estas horas pueden ser proporcionadas por el proveedor o canal seleccionado.	Bolsa de horas
Servicios de Soporte y servicios profesionales.	• Servicio de soporte deberá ser proporcionado por el proveedor o canal seleccionado con modalidad 7x24x365 con tiempo de respuesta de solicitudes (primer contacto) no superior a 1 hora. • El servicio de soporte sobre las plataformas debe incluir acompañamiento y consultas sobre funcionamiento o configuraciones de los servicios y requerimientos de soporte por cualquier medio (correo electrónico, sesiones remotas y atención en sitio en caso de requerirse). • Soporte ante cualquier falla presentada sobre las soluciones Juniper indicadas en este anexo técnico. • Apoyo en la actualización y migración a las últimas versiones liberadas por el fabricante de las soluciones de Juniper indicadas en este anexo técnico. • Apoyo en nuevas configuraciones, parametrizaciones sobre las soluciones Juniper indicadas en este anexo técnico.	Servicios de Soporte y servicios profesionales.

	• Afinamientos sobre las soluciones de Juniper indicadas en este anexo técnico. • Creación de nuevos reportes y/o configuración de reglas y alertas para detectar incidentes y/o vulnerabilidades. • Asistencia en la resolución de problemas y análisis de la causa raíz de estos cuando sea necesario sobre las soluciones Juniper. • Apoyo en el escalamiento de casos de soporte con el fabricante Juniper. Cualquier otro requerimiento que se solicite sobre el portafolio de soluciones de Juniper.	
Transferencia de Conocimiento	• Transferencia de conocimiento de mínimo 20 horas, respecto a la administración de las soluciones Juniper indicadas en este anexo técnico en su última versión disponible, que permitan administrar las herramientas con suficiencia, una vez las plataformas sean actualizadas. • La transferencia de conocimiento deberá ser para 4 personas.	20 horas de transferencia de conocimiento

Entregables	• Matriz de Escalamiento de Soporte.
	• Documento con la situación actual de las soluciones (assessment) y mejoras a realizar en la plataforma.
	• Plan de Trabajo que incluya las siguientes actividades:
	  ○ Cronograma de actividades para actualización de las soluciones Juniper indicadas en este anexo técnico.
	  ○ Cronograma para ejecución de mejoras y puesta a punto a realizar en las soluciones Juniper indicadas en este anexo técnico.
	• Registro de asistencia y certificado individual para cada asistente a las transferencias de conocimiento que se dicten
	• Memorias de la transferencia de conocimiento.
	• Grabaciones de la transferencia de conocimiento realizada para la SNR.
		Documentación

Nota: El contratista debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que su personal asignado al proyecto pueda cumplir con las obligaciones del contrato. Estos valores no incurrirán en costos adicionales para la Superintendencia de Notariado y Registro.

Cordialmente,

JOSE RICARDO ACEVEDO SOLARTE
Jefe de la Oficina de Tecnologías de la Información

Elaboro y proyecto: Oscar Fabian Corredor Camargo – Coordinador Grupo servicios tecnológicos
Martha Milena Rueda – funcionaria Grupo servicios tecnológicos
Reviso: Jorge Junior Navarro – Contratista OTI