ANEXO "B" ESPECIFICACIONES REQUERIDAS

PLATAFORMA DE SISTEMA CONTABLE

El proveedor deberá ofrecer los componentes de software necesarios para habilitar una Plataforma de un sistema Contable para integrar la funcionalidad de firma electrónica a las aplicaciones que la ASEJ requiera para transacciones y usuarios. Asimismo, se debe proveer los componentes para habilitar una Autoridad de Tiempo confiable interna en la ASEJ para emitir sellos de tiempo ilimitados. La instalación de la Plataforma será en Alta Disponibilidad y contará con Redundancia para ambiente productivo de 750 usuarios web y también en disponibilidad para un entorno de red lan para 400 usuarios.

SERVICIOS PROFESIONALES

SERVICIOS PROFESIONALES PARA LA INSTALACIÓN Y CONFIGURACIÓN (LICENCIAS)

Instalación y puesta a punto de los componentes de software y hardware requeridos dentro del alcance estas bases, y especificados para el Sistema Contable con sus componentes, que deberá incluir las siguientes actividades:

- Instalación y configuración de los componentes de la solución para ambiente productivo en alta disponibilidad y redundancia.
- Pruebas de funcionalidad para su liberación.
- Liberación de ambiente productivo.
- Creación de Memoria Técnica que refleje la configuración de los componentes instalados.

SERVICIO PROFESIONAL DE TRANSFERENCIA DE CONOCIMIENTOS

Instrucción especializada a Operadores, Administradores y Desarrolladores.
Este servicio consistirá en lo siguiente:
Personal Operador y Administrador

- Transferencia de conocimientos para un grupo de hasta 10 personas o los que indique la convocante.
- Transferencia de conocimientos que le permitan al personal capacitado, utilizar los componentes de la solución de Sistema Contable con sus componentes.

Personal Operadores, Administradores y Desarrolladores

- Capacitación para un grupo de hasta 10 personas.
- El plan de capacitación deberá incluir por lo menos los siguientes temas:
  - Administración de los componentes de la solución propuesta por el proveedor.
  - Uso de estándares criptográficos.

La capacitación deberá ser impartida en las instalaciones de la ASEJ.

MANTENIMIENTO Y SOPORTE (PÓLIZA DE SOPORTE 5x8)

El servicio cubierto por la póliza de soporte técnico del licitante ganador, estará enfocado a brindar servicios de información y solución a incidentes y/o problemas, ofreciendo de manera efectiva y oportuna soporte a los productos y servicios que el licitante ganador produzca y que fueran contratados o adquiridos por la convocante.
A continuación la convocante presenta la tabla de tipificación de Prioridad para los incidentes que puedan presentarse con la plataforma.

Prioridad 1 (Crítica)	**Prioridad 2 (Alta)**	**Prioridad 3 (Media)**	**Prioridad 4 (Baja)**
Por interrupción de trabajo			
La falla de la aplicación impide que el usuario realice sus tareas o afecta algún módulo significativo del sistema y su funcionamiento es inestable o nulo.	La falla de la aplicación impide que el usuario realice sus tareas o afecta a una significativa porción de sus trabajos.	La falla de la aplicación causa que el usuario no pueda desarrollar algunas pequeñas porciones de sus trabajos, pero todavía están habilitados para completar la mayoría de otras tareas. Puede además incluir preguntas y requerimientos de información.	La falla de la aplicación causa que el usuario no esté disponible para realizar una mínima porción de sus trabajos, pero todavía están habilitados para completar la mayoría de las tareas.
Número de Clientes Afectados			
La caída de la aplicación afecta a un alto número de usuarios. (Más del 75% de los usuarios)	La caída de la aplicación afecta a un número considerable de usuarios. (Más del 50% de los usuarios)	La caída de la aplicación afecta a un bajo número de usuarios. (Más del 10% de los usuarios)	La caída de la aplicación afecta a menos del 10% de usuarios.
Solución Alternativa			
No es aplicable una solución alternativa para el problema (Ej., el trabajo no puede ser hecho de otra forma)	Hay una solución alternativa aceptable e implementada para el problema (Ej., el trabajo puede realizarse de alguna otra manera).	Puede o no ser aceptable una solución alternativa para el problema.	Es probable que haya una solución alternativa aceptable para el problema incluyendo un sistema en clúster.

A continuación la convocante presenta la tabla de tiempos de respuesta y solución requeridos para los incidentes que puedan presentarse con la plataforma.

Prioridad del Incidente	**Impacto en el Cliente**	**Respuesta de Servicio al Cliente**
Crítica	Severo	2 horas
Alta	Urgente	4 horas
Media	Importante	7 horas
Baja	Orden de Trabajo/no Crítico	Después de las 8 horas o al día hábil siguiente

El horario de atención que ofrezca el licitante ganador, deberá ser de lunes a viernes en horario de 9:00hrs –18:00 hrs, vía telefónica y/o correo electrónico. El soporte podrá proveerse de manera remota.

PÓLIZA DE MANTENIMIENTO

Se entiende por mantenimiento la actualización a los productos que el licitante proporcione a la convocante, a fin de conservarlos en condiciones óptimas de funcionamiento, de acuerdo a sus propias especificaciones técnicas. El licitante ganador deberá ofertar dentro de su propuesta una póliza de mantenimiento que cubra todo el licenciamiento durante la vigencia del contrato a partir de la firma del contrato que formalizará la adquisición de la presente licitación.
Los servicios se definen en dos categorías.
Nuevas Versiones: Son adecuaciones mayores que consisten en nuevas funcionalidades de los productos y tienen las siguientes características:

- Actualización para cumplir con los estándares de seguridad
- Incorporación de nuevos módulos y protocolos de comunicación.
- Adecuaciones para cubrir con reglamentos y leyes Nacionales e Internacionales.
- Soporte a nuevos sistemas operativos y nuevas versiones de sistemas operativos ya existentes.
- Las nuevas versiones deberán ser enviadas a la convocante, en un plazo no mayor de 30 días hábiles, después de su liberación formal.

Actualizaciones: Son adecuaciones menores y consisten en el arreglo de problemas detectados en versiones anteriores o bien en modificaciones a la interfaz gráfica. Las actualizaciones deberán ser enviadas a la convocante, en plazo no mayor de 15 días hábiles, después de su liberación formal.

1. SUBSISTEMA DE SEGURIDAD INFORMÁTICA Y BALANCEO DE APLICACIONES

Cantidad, 2.

- **Equipo De control de Amenazas Unificado UTM por sus siglas en Ingles**
- **Funcionalidades y Características del Sistema:**
  - **Características del dispositivo**
    - El dispositivo debe ser un "appliance" de propósito específico "Hardware"
    - Basado en tecnología ASIC "Application-Specific Integrated Circuit" y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X o GNU/Linux.
    - Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).
    - Capacidad de re ensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).
    - El equipo deberá poder ser configurado en modo Gateway o en modo transparente en la red.
    - En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.
  - **Características del Sistema operativo incluido**
    - Sistema operativo pre-endurecido específico para seguridad que sea compatible con el "appliance". Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows
    - El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.
  - **Firewall**
    - Las reglas de Firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs
    - Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
    - Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.

- Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando
- Deberán poder definirse reglas de firewall para servicios sobre protocolo SCTP.
- Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación
- Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.
- Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
- Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
- Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.
- Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario)
- La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas
- En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID
- En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.

- **Conectividad y Sistema de ruteo**
  - Funcionalidad integrada de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.
  - Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.
  - Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
  - Soporte a políticas de ruteo (policy routing)
  - El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace.
  - Soporte a ruteo dinámico RIP V1, V2, OSPF, como mínimo
  - Soporte de ECMP (Equal Cost Multi-Path)
  - Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.

- Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.
- Soporte a ruteo de multicast
- La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.

- **VPN IPSec/L2TP/PPTP**
  - Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
  - Soporte para IKEv2 y IKE Configuration Method.
  - Debe soportar la configuración de túneles L2TP.
  - Debe soportar la configuración de túneles PPTP.
  - Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.
  - Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits.
  - Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.
  - Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
  - Posibilidad de crear VPN's entre gateways y clientes con IPSec. esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.
  - La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN).
  - En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.
  - Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.
- **VPN SSL**
  - Capacidad de realizar SSL VPNs.
  - Soporte a certificados PKI X.509 para construcción de VPNs SSL.
  - Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
  - Soporte de renovación de contraseñas para LDAP y RADIUS.
  - Soporte a asignación de aplicaciones permitidas por grupo de usuarios
  - Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.
  - Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.
  - La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS

- Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL
- Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente
- Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.
- Los portales personalizados deberán soportar al menos la definición de:
- Widgets a mostrar.
- Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC.
- Esquema de colores.
- Soporte para Escritorio Virtual.
- Política de verificación de la estación de trabajo.

- **Traffic Shapping / QoS**
  - Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall.
  - Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión.
  - Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.
  - Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo.
  - Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo
  - Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia.
- **Autenticación y Certificación Digital**
  - Capacidad de integrarse con Servidores de Autenticación RADIUS.
  - Capacidad nativa de integrarse con directorios LDAP.
  - Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On".
  - Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet.
  - Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.
  - Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
  - Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.

- Soporte de verificación de validación de certificados digitales mediante el protocolo OSCP (Online Simple Enrrollment Protocol).
- La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.
- Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.
- Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:
- Longitud mínima permitida.
- Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.
- Expiración de contraseña.
- Capacidad de limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.

- **Control de Endpoint**
  - La solución debe tener la capacidad de definir políticas que permitan analizar el estado de las estaciones de trabajo antes de permitir el acceso.
  - Debe poder verificarse al menos los siguientes puntos:
  - Firewall personal instalado y activo
  - Antivirus instalado y con versión de firmas actualizadas
  - La solución debe poder controlar las aplicaciones en la estación de trabajo. Como evaluación de la política deberá ser capaz de determinar si una aplicación debe estar instalada, no instalada, ejecutándose o no ejecutándose.
  - Ante el incumplimiento de políticas la solución debe ofrecer la capacidad de bloquear el tráfico de dicho usuario o sólo alertarlo sobre el mismo.
  - La solución debe brindar la posibilidad de re direccionar el tráfico a un portal de remediación, cuando no se cumpla con alguna política de control de Endpoint
  - La evaluación de políticas podrá aplicarse mediante la instalación de un agente en la estación de trabajo.
  - En caso de requerir un agente en la estación de trabajo, debe poder determinarse la mínima versión aceptada de dicho agente como parte de las políticas de Endpoint
  - Debe permitir la posibilidad de validar el estado de cumplimiento de políticas en el momento de establecer la sesión y forma periódica.
- **Protección contra intrusos (IPS)**
  - El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en SPAN o MIRROR.

- El detector y preventor de intrusos podrá implementarse en línea y fuera de línea en forma simultánea para distintos segmentos.
- Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6.
- Capacidad de detección de más de 4,000 ataques
- Capacidad de actualización automática de firmas IPS mediante tecnología de tipo “Push” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas).
- El Detector y preventor de intrusos deberá de estar orientado para la protección de redes.
- El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o “appliance” externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad “appliance”, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.
- El detector y preventor de intrusos deberá soportar captar ataques por Anomalía (Anomaly detection) además de firmas (signature based / misuse detection).
- Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.
- Tecnología de detección tipo Stateful basada en Firmas (signatures).
- Actualización automática de firmas para el detector de intrusos.
- El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.
- "Mecanismos de detección de ataques:
- Reconocimiento de patrones y Análisis de protocolos.
- Detección de anomalías.
- Detección de ataques de RPC (Remote procedure call).
- Protección contra ataques de Windows o NetBios.
- Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail o POP (Post Office Protocol)
- Protección contra ataques DNS (Domain Name System)
- Protección contra ataques a FTP, SSH , Telnet y Rlogin
- Protección contra ataques de ICMP (Internet Control Message Protocol)."
- "Métodos de notificación:
- Alarmas mostradas en la consola de administración del “appliance”.
- Alertas vía correo electrónico.

- Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.
- La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma “indefinida”, hasta que un administrador tome una acción al respecto."
- Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

- **Prevención de Fuga de Información (DLP)**
  - La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.
  - La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.
  - Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.
  - Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento.
  - En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción.
  - La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo.
  - La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.
- **Control de Aplicaciones**
  - Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
  - La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
  - La solución debe tener un listado de al menos 6,000 aplicaciones ya definidas por el fabricante.
  - El listado de aplicaciones debe actualizarse periódicamente.
  - Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: Permitir, Bloquear, Registrar en logs.
  - Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: Permitir, Bloquear, Registrar en logs.

- Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.
- Preferentemente deben soportar mayor granularidad en las acciones.

- **Inspección de Contenido SSL**
  - La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.
  - La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).
  - La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.
  - Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.
- **Antivirus**
  - Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.
  - El Antivirus deberá poder configurarse en modo Proxy, así como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.
  - Antivirus en tiempo real, integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o “appliance” externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
  - El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.
  - La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo “appliance”, que permita la aplicación de esta protección por política de control de acceso.
  - El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.
  - El “appliance” deberá de manera opcional poder inspeccionar por todos los virus conocidos (Zoo List).
  - El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos Http, FTP, IMAP, POP3, SMTP.
  - El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.

- El Antivirus deberá incluir capacidades de detección y detención de tráfico SPYWARE, ADWARE y otros tipos de MALWARE/GRAYWARE que pudieran circular por la red.
- El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).
- El antivirus deberá ser capaz de filtrar archivos por extensión.
- El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo.
- Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).

- **AntiSpam**
  - La capacidad AntiSpam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.
  - La capacidad AntiSpam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address).
  - La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y "checksum" del mensaje, como mecanismos para detección de SPAM.
  - En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.
- **Filtraje de URLs (URL Filtering)**
  - Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.
  - Debe poder categorizar contenido Web requerido mediante IPv6.
  - Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" o dispositivo externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.

- Configurable directamente desde la interfaz de administración del dispositivo "appliance". Con capacidad para permitir esta protección por política de control de acceso.
- Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida.
- Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.
- Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
- La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Navegadores tales como Google, Yahoo! y Bing.
- Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.
- Será posible exceptuar la inspección de HTTPS por categoría.
- Sera posible configurar el equipo para que automáticamente redirija el tráfico de www.youtube.com a http://www.youtube.com/education para que se acceda únicamente a contenido categorizado por el portal como contenido educativo.

- **Cache Web.**
  - La solución debe soportar actuar como un cache web, entendiéndose como la capacidad de almacenar contenido estático que está disponible y puede utilizarse localmente en posteriores requerimientos.
  - Debe poder definirse el tamaño del almacenamiento dedicado para la función de web cache.
  - Debe poder definirse el máximo tiempo en el que un objeto permanecerá en el caché (TTL).
  - El web cache debe configurarse mediante reglas que definirán el contenido que debe ser almacenado al menos con los siguientes parámetros:
  - Dirección IP o grupo de direcciones IP de origen
  - Dirección IP o grupo de direcciones IP de destino
  - Rango de puertos de destino.
  - El Cache Web podrá configurarse en forma transparente. En este modo, no es necesario que el navegador del usuario tenga configurado un Proxy.
  - El Caché Web podrá configurarse como un Proxy HTTP explícito en la red. Esto significa que los navegadores podrán configurar el "appliance" como Proxy para la navegación (A nivel Usuario).
  - Soporte del protocolo WCCPv2. Este protocolo debe soportarse en modo cliente como en modo servidor. En modo servidor, el dispositivo será capaz de re-direccionar el tráfico Web hacia uno o más servidores de

Caché Web en modo transparente para el usuario final. En modo cliente, el dispositivo podrá comportase como un Web Caché al cual se le re direccionará tráfico por un servidor de WCCPv2.

- WCCPv2 deberá soportarse tanto con GRE como Layer 2 forwarding.
- La solución debe soportar la capacidad de aplicar el Caché Web a tráfico encriptado con SSL (HTTPS).
- Cuando la solución se encuentre configurada como un Proxy explícito, éste debe poder habilitarse de forma diferenciada por interfaz de red.
- En Proxy explícito la solución debe soportar los siguientes protocolos: HTTP, HTTPS, FTP y SOCKS.
- En Proxy explícito debe poder configurarse de forma independiente los puertos en los que estarán activos los siguientes protocolos: HTTP, HTTPS, FTP y SOCKS.
- En Proxy explícito la solución debe soportar la configuración automática de los navegadores mediante PAC File (Proxy Auto-Configuration File).

- **Optimización de WAN**
  - La solución deberá soportar la capacidad de disminuir el tráfico transmitido por un determinado enlace mediante diferentes técnicas.
  - El Optimización de WAN debe configurarse mediante reglas que definirán el tráfico a optimizar al menos con los siguientes parámetros:
  - Dirección IP o grupo de direcciones IP de origen.
  - Dirección IP o grupo de direcciones IP de destino.
  - Rango de puertos de destino.
  - Deberán utilizarse al menos las siguientes técnicas para Optimización WAN: Compresión, Byte Caching, Object Caching.
  - En caso de requerirse un dispositivo en ambos extremos del enlace de comunicaciones, debe ser posible autenticar las partes antes de establecer la optimización.
  - La solución debe tener la capacidad de encriptar el tráfico cuando se esté optimizando.
  - Deberán soportarse optimización adicional de protocolos al menos para HTTP, CIFS, MAPI y FTP.
- **Alta Disponibilidad**
  - Posibilidad en Firewall Soporte a Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.
  - Alta Disponibilidad en modo Activo-Pasivo.
  - Alta Disponibilidad en modo Activo-Activo.
  - Posibilidad de definir al menos dos interfaces para sincronía.
  - El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red.
  - Será posible definir interfaces de gestión independientes para cada miembro en un Cluster.
- **Características de Administración**

- Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS).
- La interfaz gráfica de usuario (GUI) vía Web deberá estar en español y en inglés, configurable por el usuario.
- Interfaz basada en línea de comando (CLI) para administración de la solución.
- Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.
- Comunicación cifrada y autenticada con username y password, tanto como para la interfaz gráfica de usuario como la consola de administración de línea de comandos (SSH o TELNET).
- El administrador del sistema podrá tener las opciones incluidas de autenticarse vía password y vía certificados digitales.
- Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden Administrar y realizar cambios de configuración.
- El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, TELNET, HTTP o HTTPS.
- El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
- Soporte de SNMP versión 2 y Soporte de SNMP versión 3.
- Soporte de al menos 3 servidores SYSLOG para poder enviar bitácoras a servidores de SYSLOG remotos.
- Soporte para almacenamiento de eventos en un repositorio que pueda consultarse utilizando SQL.
- Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.
- Monitoreo de comportamiento del "appliance" mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.
- Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.
- La interfaz gráfica de usuario (GUI) deberá de contar con la funcionalidad de autentificarse con un TOKEN (Autentificación de segundo factor) sin necesidad de integrar un equipo adicional o solución de otro fabricante.

- **Virtualización**

- El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains".
- La instancia virtual debe soportar por lo menos funcionalidades de Firewall, VPN, URL Filtering, IPS y Antivirus.
- Se debe incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer.
- Cada instancia virtual debe poder tener un administrador independiente.
- La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.
- Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red.
- Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.
- Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.
- Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.

- **Capacidades de Desempeño:**
  - El equipo debe contar con un Throughput Firewall de al menos 8 Gbps para paquetes de 1518, 512 y 64 bytes UDP en IPv4 e IPv6.
  - El equipo debe contar con un Throughput VPN de por lo menos 7 Gbps.
  - El equipo debe contar con un Throughput IPS de al menos 2.8 Gbps.
  - El equipo debe contar con un Throughput AntiVirus en modo Proxy de al menos 1.4 Gbps.
  - El equipo debe contar con al menos 6 millones de Sesiones concurrentes.
  - El equipo debe soportar 200,000 Nuevas sesiones por segundo.
  - El equipo debe de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 600 usuarios de VPN SSL.
  - El equipo debe poder soportar túneles de al menos 10,000 VPN's IPSec Client to Gateway.
  - El equipo debe poder soportar túneles de al menos 2,000 VPN's IPSec Gateway to Gateway
- **2 Características de Hardware:**
  - El equipo debe contar con al menos 10 Interfaces GigaEthernet .
  - El equipo debe contar con al menos 4 puertos SFP
  - El equipo Deberá de contar con capacidad de fuente de poder redundante (interna o externa).
  - El equipo debe de contar con un disco de almacenamiento de mínimo 100 GB.
- **Soporte y garantías.**
  - La garantía de los equipos deberá de ser por 3 años.
  - El soporte y atención a fallas 8x5.
  - La actualización de versiones, parches, y servicios de protección completo por 3 años.

Balanceador de aplicaciones.

Cantidad, 2.

Operación general

- Contar con una solución de balanceo de servidores y de enlaces que permita mejorar el desempeño de las mismas y al mismo tiempo generar un esquema de alta disponibilidad.
- Funcionalidades
- La solución debe estar diseñada para proveer aceleración en Layer-4 y Layer-7
- La solución debe ser desarrollada por el fabricante y no debe incluir desarrollos de terceros
- La solución debe ser capaz de balancear trafico ICMP,UDP,TCP y poseer entendimiento de protocolos como HTTP/s, FTP y RADIUS.
- La solución debe ser capaz de balancear carga de manera transparente o utilizando NAT basándose en información obtenida de Layer-7 como URL, Cookie, SSL ID, etc.
- La solución debe poseer distintos métodos de balance como round robin, weighted round robin, least connection y shortest response
- La solución debe ser capaz de hacer routing/switching inteligente de contenido en Layer-7 basándose en la información enviada por el cliente (URL, HTTP header, cookie, URL, etc)
- La solución debe proveer persistencia en Layer-4 basándose en la dirección IP de origen y puerto. Adicionalmente la persistencia en Layer-7 debe poder ser configurada basándose en la información del cliente como URI, HTTP headers, hostname, SSL session ID y Cookies.
- La solución debe ser capaz de hacer SSL Offloading.
- La solución debe ser capaz de realizar balance entre datacenters (GSLB).

- La solución debe poseer la capacidad de proteger aplicaciones y servidores de ataques SYN-Flood y cantidad de conexiones. Además debe ser capaz de integrar tabla de conexiones statefull para IPv4 e IPv6.
- La solución debe poder ser administrada vía interfaz gráfica (GUI) e interfaz de línea de comandos (CLI) .
- La Solución propuesta deberá proveer alta disponibilidad, failover transparente y escalabilidad para las aplicaciones.
- La solución propuesta deberá contar con un servicio de protocolo virtual de para los siguientes protocolos HTTP, HTTPS, TCP, TCPS, FTP, FTPS, UDP, DNS, SIP UDP, SIP TCP, RTSP, RDP, IP, L2IP, este servicio virtual también deberá funcionar en modo proxy reverso, proxy transparente.
- La solución propuesta deberá reenviar los paquetes IP a diferentes destinos MAC para distribuir la carga a nivel de capa 2 puerto físico, a nivel de capa 3 dirección IP y rango de puertos TCP/UDP.

- La solución propuesta deberá ofrecer un sistema de almacenamiento de contenido Web completamente integrado con funcionalidades de HTTP/HTTPS, compresión y funciones de administración de tráfico para almacenar y enviar objetos validando las peticiones de los clientes sin tener que consultar a los servidores reales acelerando la respuesta de las aplicaciones, reduciendo el ancho de banda y la carga de los servidores. Deberá proveer estadísticas detalladas del acceso al cache basándose en IP o en http hosts como mínimo, las coincidencias de los objetos almacenados podrán estar basadas en URL parciales. Deberá tener reglas configurables para tamaño máximo de objetos, TTL y la forma de acceso, soporte del set de caracteres extendidos.
- La solución propuesta deberá tener un sistema de compresión dinámico en línea , en donde de forma automática deberá comprimir archivos de texto, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT y XLS, también deberá contemplar reglas para no comprimir URL seleccionados que contengan RegEx y objetos web seleccionados para el servicio virtual seleccionado y proporcionar estadísticas detalladas de la compresión.
- La solución propuesta deberá tener un sistema de aceleración de SSL basado en hardware soportando HTTPS, NNTPS, SMTPS, POPS, IMAPS y LDAPS. Soporte de SSLv3 y TLSv1 y soportar cifrado de 2048-bits, redirección automática de HTTP a HTTPS, deberá poder actuar como servidor de SSL o como cliente de SSL al mismo tiempo, hasta 64 servicios virtuales podrán utilizar el mismo certificado. La única limitante para el almacenamiento de certificados digitales será el espacio en disco de la unidad. Autogeneración de peticiones de firma de certificados (Certificate Signing Request. CSR) para un host específico. Los certificados y llaves privadas podrán ser importados a través de TFTP soportando los formatos OpenSSL/Apache, *.PEM", "MS IIS, *.PFX", y "Netscape, *.DB por lo menos
- El licitante deberá entregar documento donde especifique el performance que entregara la solución.

2. SUBSISTEMA DE PROCESAMIENTO, ALMACENAMIENTO Y COMUNICACIONES

Servidores Tecnología X_86

Se requieren de 3 Servidores x86 con las siguientes características:

Tipo 1: Cantidad, 2.

- Debe incluir 2 CPUs Intel Xeón E5-2670 v3
- Debe incluir al menos 12 cores por procesador 2.3 GHz.
- Debe incluir al menos 192 GB de memoria RAM.
- Capacidad de crecimiento de Memoria RAM de al menos 768 GB.
- Debe incluir almacenamiento interno redundante para hypervisor de al menos 15krpm o SSD.
- Con soporte de al menos 8 discos internos de 2.5".
- Debe soportar de discos SSD
- Debe incluir 1 unidad de DVD writer.
- Debe de incluir fuentes de poder con soporte de reemplazo en caliente, configuradas de manera redundante.
- Debe incluir 4 puertos RJ-45 integrados en el chasis del servidor que soporte las velocidades 100/1000/10000 Mb/seg.
- Debe incluir dos HBA de 2 puertos cada una de 8Gb FC compatibles con el sistema de almacenamiento mencionado en la presente licitación.
- Debe incluir 4 puertos USB en el mismo chasis.
- Debe incluir 1 puertos VGA HD15 en el mismo chasis.
- Debe incluir 1 puerto de administración RJ45 en el mismo chasis.
- Debe de incluir un puerto de administración Ethernet 10/100/1000 RJ-45.
- Debe incluir el software de virtualización en su última versión y sin límite en el número de procesadores y memoria que pueda tener configurado el equipo.
- El hardware debe estar soportado por el software de virtualización propuesto.
- Los equipos deben tener soporte 3 años con atención 7 x 24 ofrecido por el fabricante.
- Todo el Software y SO de los equipos ofertados que se incluya debe tener soporte 3 años con atención 7 x 24 ofrecido por el fabricante.
- Todos los componentes del subsistema deben ser del mismo fabricante.
- Deberá incluir 2 licencias de Microsoft SQL Ent última versión a la fecha de fallo
- Deberá incluir todo lo necesario para interoperar con la red y servicios que entrega la licitante a sus usuarios.
- EL LICITANTE GANADOR será responsable de toda la interconexión del equipo, software, hardware, cableado, instalación, migración, configuración y puesta a punto.
- Debe incluir Licenciamiento de Windows Datacenter 2012 R2 Gov OLP dos licencias, así como una licencias de Windows server estándar gov OLP para administración, así mismo considerar las licencias de dispositivo o usuario de la red para necesarias para cumplir con la legislación de propiedad intelectual.

Tipo 2: (Consola de administración y respaldos), Cantidad, 1.

Para la consola de administración se requiere de un software cuya licencia venga incluida se requiere 1 Servidor x86 con las siguientes características como mínimo:

- Debe incluir 2 CPUs Intel Xeón E5-2630 v3
- Debe incluir al menos 8 cores por procesador 2.4 GHz.
- Debe incluir al menos 32 GB de memoria RAM
- Capacidad de crecimiento de Memoria RAM de hasta 768 GB.
- Debe incluir 500GB en almacenamiento usable de 15krpmtolerante a fallas de disco.
- Debe soportar de discos SSD
- Debe incluir 1 unidad de DVD writer
- Debe de incluir fuentes de poder con soporte de reemplazo en caliente, configuradas de manera redundante.
- Debe incluir 4 puertos RJ-45 integrados en el chasis del servidor que soporte las velocidades 100/1000/10000 Mb/seg.
- Debe incluir dos HBA de 2 puertos cada una de 8Gb FC compatibles con el sistema de almacenamiento mencionado en la presente licitación.
- Debe incluir 4 puertos USB en el mismo chasis.
- Debe incluir 1 puertos VGA HD15 en el mismo chasis.
- Debe de incluir un puerto de administración Ethernet 10/100/1000 RJ-45.
- Debe incluir el software de administración de virtualización en su última versión y sin límite en el número de procesadores y memoria que pueda tener configurado el equipo.
- El hardware debe estar soportado por el software de virtualización propuesto.
- Debe contar con todo el licenciamiento necesario para administrar y respaldar el ambiente ofertado, sin límite de capacidad y con capacidad de replicar respaldos a otra ubicación.
- Debe ser interoperable con la red actualmente en producción en la AuditoríaSuperior del Estado de Jalisco
- Los equipos deben tener soporte 3 años con atención 7 x 24 ofrecido por el fabricante.
- Todo el Software y SO de los equipos ofertados que se incluya debe tener soporte 3 años con atención 7 x 24 ofrecido por el fabricante.
- Todos los componentes del subsistema deben ser del mismo fabricante.
- EL LICITANTE GANADOR será responsable de toda la interconexión del equipo, software, hardware, cableado, instalación, migración, configuración y puesta a punto.

Almacenamiento.

Cantidad, 1.

Equipo de almacenamiento para Datos SAN con las siguientes características:

- Debe incluir 2 Controladoras trabajando en cluster activo-activo.
- Debe de incluir fuentes de poder con soporte de reemplazo en caliente, configuradas de manera redundante.
- Debe incluir 4 puertos 8 Gbps de tipo FC por controladora para conectividad SAN.

- La plataforma de almacenamiento en su configuración máxima debe soportar al menos 500 discos físicos pudiendo ser combinado de diferentes tecnologías SAS, NL-SAS o SSD
- Debe tener la capacidad de mover los datos automáticamente de acuerdo a la frecuencia de uso entre diferentes "capas" de tipo de disco, ubicando los datos mas accesados en los discos más rápidos.
- La configuración mínima requerida de los discos en el almacenamiento será la siguiente:
    - 80TB usables para datos en discos 300GB 15k tolerante a fallas
    - 8TB usables en discos de SSD en RAID 10
    - 80TB usables para respaldos en disco tolerante a fallas
- Para los sistemas ofertados con el almacenamiento integrado se deben de soportar los siguientes niveles de protección:
    - Mirror o equivalente
    - RAID5 o equivalente
    - RAID6 o equivalente
- Debe incluir la funcionalidad de duplicación de datos en línea.
- Debe incluir interfaces de administración vía Web y línea de comandos bajo un medio cifrado.
- Debe incluir la funcionalidad de generar reportes de desempeño.
- Debe incluir la funcionalidad de auto reportarse en caso de falla de algún componente del almacenamiento.
- Debe incluir la funcionalidad de realizar réplicas de datos remotas hacia otro equipo con las mismas características
- Los equipos deben tener soporte 3 años con atención 7 x 24 ofrecido por el fabricante.
- Todo el Software y SO de los equipos ofertados que se incluya debe tener soporte 3 años con atención 7 x 24 ofrecido por el fabricante.
- Todos los componentes del subsistema deben ser del mismo fabricante.
- La solución debe tener la opción Call Home, Automatic Service Request o su equivalente para enviar de forma pro-activa y sin intervención del operador mensajes al fabricante sobre fallas potenciales o reales que puedan tener los equipos. El servicio debe ser ofrecido por el fabricante del subsistema.
- La solución de HW y SW de la consola de administración debe ser de la misma marca de todo el subsistema.
- Se debe entregar documento liberado por el fabricante donde especifique la velocidad que entregará el equipo con la configuración ofertada.
- EL LICITANTE GANADOR será responsable de toda la interconexión del equipo, software, hardware, cableado, instalación, migración, licenciamientos necesarios, configuración y puesta a punto.

Switches de comunicación

Cantidad, 2.

Debe incluir al menos con las siguientes características para cada uno:

- Debe incluir 16 puertos activos de 10 GbE Ethernet
- Debe incluir un puerto 1000Base-T para su administración.
- Debe soportar UPLink a 1Gb de al menos 4 puertos en link agregation para interoperar con la red en productivo de la licitante.
- Se requiere que cada uno de los switches sean monitoreados desde la consola central.
- Cada uno de los switches debe incluir al menos un puerto serial de servicio (RJ45) en el mismo chasis.
- Debe incluir la funcionalidad de capa 2 y capa 3
- Debe incluir funcionalidades para capa 2 y capa 3 sin que se requiera licenciamiento adicional para la convocante.
- Cada switch debe soportar los siguientes protocolos de administración CLI, SSH, Interface Web.
- Debe incluir todo el cableado dentro del mismo rack de las comunicaciones ethernet mencionadas en la presente licitación.
- Los equipos deben tener soporte 3 años con atención 7 x 24 ofrecido por el fabricante.
- Todos los componentes del subsistema deben ser del mismo fabricante.
- EL LICITANTE GANADOR, será responsable de toda la interconexión del equipo, software, hardware, cableado, instalación, migración, configuración y puesta a punto.

Sistema de energía no interrumpible (UPS por sus siglas en inglés)

Cantidad, 2.

Debe incluir al menos con las siguientes características para cada uno:

- Soportar la energía de la totalidad de los componentes de la presente durante al menos 20min
- Deberá ser interoperable con la planta de energía actualmente instalada en las instalaciones de la licitante.
- Deberá contemplarse la totalidad de los componentes necesarios para su correcta instalación tales como tableros de control, pastillas térmicas, ductería, cableado, etc
- EL LICITANTE GANADOR, será responsable de toda la interconexión del equipo, software, hardware, cableado, instalación, migración, configuración y puesta a punto.
- Deberá contar con garantía de 3 años en la totalidad de los componentes.
- Deberán ser componentes rackeables en su totalidad.
- Deberá contemplar 2 PDU rackeable con contactos tipo C14 con control por zonas para la totalidad de la solución.

Estantería rack

Cantidad, 1.

Debe incluir al menos con las siguientes características:

- Deberá contar con 42U de altura.

- Deberá contar con medidas estándar en la industria para servidores en general.
- Deberá contar con puertas frontal y trasera con llave.
- Deberá contar con puertas laterales con llave.
- Deberá ser tipo "gabinete".
- Deberá contar con soportes en cada esquina inferior.
- Deberá contar con espacios para PDU estándar en los espacios laterales.

Entregables

El licitante ganador se obliga a entregar la documentación correspondiente a manuales y memorias técnicas en forma electrónica de los siguientes documentos:

- Manual de usuario.
- Memoria Técnica.
- Procedimiento de Escalamiento de Fallas y Problemas en el Servicio.
- Documento técnico donde se especifique com ose cubre cada punto solicitado con referencia del fabricante.
- Licenciamientos necesarios para la solución del Sistema de Contabilidad Gubernamental.

NOTAS:

1) **En virtud de que lo solicitado en bases de esta Licitación Pública requiere una especialización, se autoriza a los participantes para que se asocien con alguien, con el fin de cubrir la totalidad de los requisitos de esta solicitud.**

2) **Interactuar con el personal técnico de la ASEJ para garantizar la compatibilidad de la propuesta.**