LICITACION POR CONCURSO DE OFERTAS Nº 01/2011 ADQUISICION DE UN SISTEMA DE SEGURIDAD (CIRCUITO CERRADO) PARA EL REGISTRO DEL ESTADO CIVIL (AD REFERENDUM)

ADENDA Nº 2

PARTE 2 – Suministros Requeridos

SECCION V PROGRAMA DE SUMINISTRO

3. ESPECIFICACIONES TECNICAS

3. Especificaciones técnicas del sistema requerido y sus componentes.

Fue modificado solamente el 3.3, quedando como sigue:

3.3 Switch o Conmutador para Infraestructura IP

El conmutador solicitado debe cumplir como mínimo con lo siguiente:

- 20 Puertos 10/100/1000 BaseT que brinden alimentación PoE.
- 4 Puertos Combo que pueden ser configurados para operar como 10/100/1000BaseT o 1000BaseX
- 2 Puertos 10 Gigabit
- 2 Puertos dedicados para apilamiento
- 1 Puerto Consola
- 1 Puerto USB 2.0
- Memoria Flash 64MB
- Memoria RAM 256MB DRAM
- Capacidad de Forwarding: >65 Mpps
- Capacidad de Switching: >140Gbps
- Soporte de 4000 VLANs configuradas
- Soporte de Jumbo Frames de 9000 bytes
- MBTS > 200.000 hs

El conmutador debe contar con la posibilidad de apilamiento de como mínimo 8 conmutadores administrados como un solo equipo virtual. El conmutador solicitado debe incluir las interfaces SFP (transceiver) para conexión de fibra óptica de tipo multimodo con conector tipo LC

Además debe cumplir con:

Requisitos Generales

La solicitud es para la conmutación de LAN. Con el fin de proteger la inversión, tanto el hardware como el software deben ser resistentes y evolutivos para asegurar una recuperación de inversión y una proposición económicamente viable.

Los conmutadores de agregación serán conmutadores de capa 3 que se puedan actualizar fácilmente para adaptarse a los cambios de demanda de tráfico así como a las fluctuaciones de las necesidades del personal. Entre las opciones que se consideran útiles se incluyen:

- Fuentes de alimentación redundantes e intercambiables en caliente.
- Disponibilidad alimentación CA y/o CD para los conmutadores.

- Funciones de alimentación por Ethernet para admitir teléfonos VoIP, WLAN AP, cámaras de seguridad, etc.
- Disponibilidad de uplink 10 Gigabit

Para ser económicamente viable para el futuro, el conmutador debe ser totalmente compatible con IPv6 con procesamiento basado en hardware para velocidades de cable, clasificación y tunelización. El rendimiento no se debe ver afectado al habilitar el procesamiento de IPv6 ya sea al desplegar IPv4, IPv6 o IPv4/IPv6.

El conmutador debe proporcionar o ser compatible con métodos de autenticación para incluir 802.1x, PKI de autenticación MAC, etc.

Los conmutadores deben cumplir los siguientes requisitos generales:

- Monitorización de la actividad de red
- Configuración y solución de problemas de los dispositivos
- Gestión VLAN
- Configuración de la calidad de servicio
- Seguridad de acceso a los conmutadores
- Posibilidad de cuarentena para los usuarios de visita
- Acceso de seguridad avanzado
- Funciones QoS avanzadas (priorización, filtrador, etc.)
- Compatibilidad flexible con alimentación por Ethernet (PoE)
- Procesamiento a velocidad de cable para IPv4/IPv6
- Total compatibilidad con aplicaciones unicast y multicast, como colaboración de voz-sobre-vídeo
- Cumplir con la directiva sobre restricción de ciertas sustancias peligrosas en equipos eléctricos y electrónicos (RoHS).

Con el fin de cumplir con los requisitos de esta oferta, el Licitante debe poder proporcionar detalles sobre los temas que se enumeran en las secciones a continuación.

Disponibilidad

Para garantizar una total disponibilidad en la LAN, la propuesta debe reunir las funciones que se enumeran en esta sección.

- El conmutador debe ser capaz de ofrecer una amplia gama de funciones de disponibilidad como:
- Gestión redundante,
- Fuentes de alimentación redundantes.
- Agregación de enlaces incluyendo 10 Gigabit Ethernet que se pueden configurar en límites de unidades físicas.

Con el fin de eliminar puntos débiles, minimizar la complejidad y el coste operativos e incrementar la disponibilidad de aplicaciones críticas, el conmutador incluirá las siguientes funciones

- CPU redundante (1+1).
- Extracción/inserción en caliente de unidades en una pila.
- Subcomponentes intercambiables en caliente (transceptores SFP/XFP – Fuente de energía de respaldo).
- Carga de software (enrutamiento/seguridad) opcional sin impacto y sin necesidad de reiniciar el sistema
- Rollback de imágenes para volver a cargar automáticamente configuraciones y versiones de software anteriores.

Con el fin de proporcionar una red económica, con alta disponibilidad, escalable y

reconfigurable, sería conveniente ofrecer un chasis basado en módulos que se pueda combinar con otros conmutadores por parte del Licitante.

El Licitante debe ofrecer funciones basadas en estándares como:

- Spanning Tree por VLAN (802.1s) y Spanning Tree de rápida recuperación (802.1w) para proporcionar una mayor resistencia, capacidad de recuperación de fallos rápida mediante enlaces redundantes y carga compartida de capa 2 en enlaces de red no utilizados (capacidad de ancho de banda).
- La agregación dinámica de enlaces (802.3ad) para proporcionar una recuperación inherente a los enlaces existentes restantes en caso de que uno o varios de estos enlaces de la agregación falle, así como proporcionar capacidad multi-Gigabit automáticamente con otros conmutadores.
- Disponibilidad de alimentación auxiliar en caso de que falle una fuente de alimentación

El Licitante debe ofrecer una solución que garantice la solidez de Spanning Tree (opciones de uno o varios STP): IEEE 802.1D (STP) (Spanning Tree 802.1D para topología sin bucles y redundancia de enlaces) y Reconfiguración rápida IEEE 802.1w de Spanning Tree. Debe ofrecer:

- Spanning Tree rápido de anillo optimizado para topología de anillo con un tiempo de convergencia inferior a 100 ms
- IEEE 802.1s Spanning Tree múltiple y Spanning Tree por VLAN (1x1)
- Modo Fast Forwarding en puertos de usuario para evitar el retraso de 30 segundos en Spanning Tree
- Evitar el funcionamiento de los puentes no autorizados vinculados a los Spanning-Tree activos
- Bloqueo BPDU: cierra automáticamente los puertos del conmutador que se usan como puertos de usuario si se detecta un paquete spanning-tree BPDU. Evitar el funcionamiento de los puentes no autorizados vinculados a los Spanning-Tree activos.
- Colas de prioridad: Ocho colas por puerto basadas en hardware

Compatibilidad

La solución debe ser compatible con:

- Agregación de enlaces dinámica IEEE 802.3ad (para admitir la configuración automática de agregaciones de enlaces con otros conmutadores) con funciones sólidas de uplink.

Agregación de enlaces estática (compatible con la configuración automática de agregaciones de enlaces con otros conmutadores). Para garantizar la solidez del hardware, el producto propuesto debe ser resistente a las variaciones de temperatura excesivas y físicas. La solución debe incluir:

- Protección térmica/apagado del chasis
- Monitorización de hardware, monitorización de temperatura y monitorización y gestión de energía
- Tiempos de inicio "en frío" y "en caliente" breves
- Seguridad integrada y consolidación de dispositivos

La resistencia de enlaces y de red es parte importante de la disponibilidad de la red, y el producto propuesto debe admitir el enrutamiento avanzado, la carga compartida y los mecanismos para la reconfiguración rápida de enlaces entre conmutadores, servidores y otros dispositivos de red.

El Licitante debe ofrecer una solución compatible con:

- VRRP (Protocolo de redundancia de router virtual)
- OSPF
- ECMP (Protocolo de multirruta de mismo coste)

Seguridad

La propuesta debe cumplir las funciones que se enumeran en esta sección.

El oferente debe suministrar aplicaciones integradas o de otro tipo para ofrecer:

- Seguridad proactiva en toda la red, por medio de autenticación auto sensible que evita el acceso no autorizado a ésta.
- Seguridad reactiva, gestionando automáticamente los ataques maliciosos recogiendo la información de intrusión y reconfigurando de forma dinámica la red para resistir el ataque.
- El conmutador debe admitir un enfoque de seguridad distribuida, mejorar las tecnologías de seguridad emergentes y ayudar a la protección del acceso a LAN mediante estrategias proactivas y reactivas.

El oferente debe incluir una solución capaz de implementar la verificación de la integridad del host para garantizar que, antes de permitir la entrada a la red, los dispositivos asociados ejecuten unas credenciales definidas por el administrador como:

- Que el nivel de actualización de sistema operativo.
- Que el firewall local esté activado.
- Que la versión del antivirus está actualizada.

La solución de verificación de integridad del host debe incluir compatibilidad para poder desplazar los hosts que pasan la inspección dinámicamente a la VLAN adecuada según el usuario, o bien moverlos a un entorno protegido donde puedan mantener el acceso limitado a los recursos de red para remediar el problema.

La oferta debe incluir compatibilidad con motor de cuarentena, así como compatibilidad con sistemas de detección de intrusos (IDS), para que la red pueda detectar automáticamente los ataques y llevar a cabo acciones de protección como:

- Limitar el tráfico
- Poner el dispositivo en cuarentena
- Para proteger el acceso a LAN, los conmutadores deben ser compatibles con las listas de control de acceso (ACL) para filtrar y dejar fuera las comunicaciones no deseadas.

El oferente debe ofrecer un conmutador que incluya:

- Una función de VLAN autenticada para ofrecer la capacidad de autenticar al usuario por nombre de usuario y contraseña y, a continuación, ubicarlo en la VLAN adecuada
- IEEE 802.1x, un enfoque de acceso de red que se basa en estándares, es una forma eficaz de solicitar al usuario un nombre de usuario y una contraseña antes de proporcionar acceso a la red
- Seguridad de puerto reconocido (LPS), que permite únicamente a los dispositivos de red previamente autorizados la comunicación entre sí. De esta forma se ofrece protección frente a dispositivos intrusos como puntos de acceso a WLAN, así como portátiles y PC no protegidos y que pueden estar infectados por virus.
- La administración de la solución debe estar protegida con una gestión remota de cifrado con Secure Shell (SSHv2), Secure Socket Layer (SSL) para la gestión basada en Web y SNMPv3 para los sistemas de gestión que abarcan toda la red.

Además, todos los administradores se deben autenticar de forma centralizada por medio de un servidor RADIUS, TACACS+, LDAP o ACE. Se puede suministrar una base de datos local en cada conmutador para la autenticación de los administradores.

El conmutador debe proporcionar seguridad multicapa con una serie de funciones de seguridad. Entre ellas se incluyen las siguientes:

- Autenticación de usuario
- Redes de área local virtuales (VLAN)
- VLAN de cuarentena
- Listas de control de acceso (ACL)
- Restricción de los puertos del usuario para impedir que envíen tráfico de control (BPDU, RIP, OSPF, BGP)
- Prevención frente a la manipulación de dirección IP de origen
- Autenticación de acceso al conmutador
- Cifrado para gestión protegida (SSHv2 / HTTPS / SNMPv3)
- Protección frente a denegación de servicio

Para la protección las funciones de gestión deben estar integradas en la arquitectura, entre ellas:

- Acceso de usuario autenticado, SNMPv3 y SSL para sesiones cifradas, y
- Gestión segmentada para acceso a distintos niveles y administración granular de red.

Inteligencia

Para que se le considere inteligente, el producto debe ser compatible con las siguientes funciones:

- El oferente debe ofrecer un conmutador basado en un diseño que pueda distribuir los procesos en las interfaces de red y no confiar en una arquitectura de nivel de control centralizada en la que el módulo de gestión es responsable de todo el procesamiento. El diseño distribuido permitirá a procesos clave, como Spanning Tree, mantener un estado completamente operativo.
- Las aplicaciones críticas siempre deben estar disponibles, admitiendo las funciones avanzadas de Calidad de servicio (QoS).

El conmutador debe poder gestionar las colas de hardware, la inteligencia y la granularidad necesarias para:

- Identificar correctamente (la identificación se basa en funciones basadas en políticas que van desde la capa 1 a la 4)
- Marcar y priorizar flujos de datos

El oferente debe proporcionar conmutadores que ofrezcan compatibilidad con IPv6 para rapidez, clasificación y túneles a velocidad de cable. El rendimiento del conmutador no se puede ver afectado con independencia de si se despliega IPv4, IPv6 o IPv4/IPv6.

La oferta del oferente debe ser compatible con la clasificación basada en hardware (listas de control de acceso [ACL] y calidad de servicio [QoS], desvío y gestión para IPv6).

El producto debe contar con estándares de clasificación del sector, incluyendo 802.1Q/p, TOS y DiffServ, mejorados con funciones complementarias, como las asignaciones exhaustivas de QoS y el reetiquetado de la priorización:

El producto propuesto debe ser compatible con:

- Compatibilidad completa de alimentación a través de Ethernet (PoE) IEEE 802.3af
- Funciones de puente residencial: DHCP option-82, DHCP-Snooping y asignación de puertos

- Protocolos de enrutamiento: IPv4 y IPv6, RIPng, RIPv1/v2 y OSPFv2&v3 y OSPF-ECMP y BGPv4

Gestionabilidad

El oferente debe ofrecer funciones de gestión que puedan utilizar información de los dispositivos, el tráfico de datos y la identidad del usuario mantener de forma automática y dinámica al usuario conectado a los recursos sin problemas con independencia de su ubicación en el campus. Por ejemplo, los departamentos de marketing, finanzas, operaciones y ventas podrían coincidir en la misma reunión en una ubicación física común pero tener acceso protegido y dinámico a sus respectivos recursos de red.

El conmutador debe ofrecer todas las ventajas de gestionar un conmutador auténticamente basado en chasis, entre ellas:

- Actualizaciones de software sencillas y rápidas
- Cambios de configuración de conmutador
- El conmutador debe incluir una interfaz de línea de comandos (CLI) estándar en el sector para simplificar la configuración de cara al personal técnico.

Para gestionar las funciones de alimentación por Ethernet de forma eficaz y evitar errores de configuración en el conmutador, los puertos del conmutador deben incluir funciones de configuración automática con el fin de determinar:

- Si el cable conectado es directo o cruzado
- La naturaleza del dispositivo de red (PC, conmutador, router) para crear automáticamente una condición de enlace.
- El conmutador debe poder gestionar los requisitos de energía de los dispositivos y equilibrarlos con las energías disponibles para evitar pérdidas de alimentación o sobrecargas.
- El conmutador debe proporcionar flexibilidad, siendo compatible con conectividad mediante enlaces de cobre o de fibra y a la vez que reduciendo los costes al eliminar la necesidad de contar con módulos uplink Gigabit independientes.

El oferente debe poder ofrecer interfaces de gestión que:

- Proporcionen a los usuarios comandos e interfaces de usuario que sean ergonómicamente coherentes en toda la red de convergencia.
- Puedan interactuar con otros sistemas de gestión
- Puedan estar basados en Web para una gestión de elementos sencilla
- Puedan utilizar SNMP para sistemas de gestión de redes de terceros

Tabla de cumplimiento mínimo

Marca	**Especificar**	
Modelo	**Especificar**	
Formato apilable en racks de 19"	1RU	
Switching de capa 2 & capa 3	SI	
Arquitectura "Store-and-Forward"	SI	
Interfaces de red 10/100/1000Mbps conectores RJ45 con Alimentación PoE	≥20	
Soporta norma 802.3af para alimentación PoE	SI	
2 puertos de Apilamiento	SI ≥10Gbps por puerto	

2 puertos de Uplinks	SI ≥10Gbps por puerto	
Capacidad adicional de puertos para Fibra óptica	SI ≥4 puertos	
Capacidad de soportar estos módulos de FO (GBICs o SFPs): 100BASE-SX, -BX, -FX: (mono/multimodo) 1000BASE-SX, -LX,-BX (mono/multimodo) 10GBASE-LR Dark fiber SMF/1310 nm hasta10 km 10GBASE-ER Dark fiber SMF/1550 nm hasta 40 km 10GBASE-SR Dark fiber MMF/850 nm hasta 65 meters	SI	
Puertos 1000BaseSX-LC habilitados	1 puerto	
"Auto-negotiating" & "Auto-sensing" en cada puerto	SI	
Capacidad mínima de expedición de ancho de banda (Switching)	≥140Gbps (agregado)	
Capacidad mínima de expedición (Forwarding)	≥65Mpps	
Tamaño de tabla (MAC-Address) en capa 2	≥16000	
Tamaño de tabla (IP-Address) en capa 3	≥48000	
Capacidad MTU (incluyendo tramas Jumbo)	9000bytes	
Tamaño de Memoria DRAM	≥256MB	
Tamaño de Memoria Flash	≥64MB	
Administración por interfaz serial, SSH, HTTPS. Capacidad para no optar por protocolos no seguros.	SI	
Capacidad de Autenticación usando hasta 2 servidores RADIUS (RFC 2138)	SI	
Capacidad para guardar y cargar Configuración por FTP seguro, TFTP.	SI	
Soporta administración por SNMPv1, SNMPv2, and SNMPv3 inclusive con Autenticación Codificada	SI	
Soporta DHCP forwarding (RFC 2131)	≥ 8 servidores DHCP	
Soporta DHCP snooping	SI	
Soporta RMON (RFC 2819)	SI	
Soporta OSPF (RFC 2328) inclusive con Autenticación Codificada	SI	
Soporta VRRP (RFC 2338) inclusive con Autenticación Codificada	SI	
Soporta VRRP (Virtual Router Redundancy Protocol - RFC 3768)	SI ≥255 grupos VRRP / VLAN	
Soporta CIDR (RFC 1519)	SI	
Soporta IGMPv1 (RFC 1112), IGMPv2 (RFC 2236), IGMPv3 (RFC 3376)	SI	
Soporta Actualización de Software sin necesidad de realizar un "shutdown"	SI	
Soporta "Port Mirroring"	SI	
Capacidad de desactivación automática de puertos por superar configurable capacidad de broadcasts por segundo	SI	
Capacidad de filtrar (permitir) solo paquetes de protocolo IP	SI	
Soporta IPv6	SI	
Soporta Filtramiento por IGMP	SI	

Soporta Dynamic Trunking Protocol (DTP)	SI	
Soporta Unidirectional Link Detection Protocol (UDLD)	SI	
Soporta Control de broadcast, multicast, y uni-cast por puerto	SI	
Soporta IEEE 802.1s (Multiple Spanning Tree Protocol)	SI	
Soporta IEEE 802.1Q VLAN y VLAN Trunking	SI ≥255VLANs	
Soporta IEEE 802.1p	SI	
Soporta IEEE 802.1x (seguridad y autenticación de usuario por puerto)	SI	
Soporta IEEE 802.1ad (vMANs)	SI	
Soporta Fast Ethernet (IEEE 802.3u)	SI	
Soporta 802.3ab (1000 Base-T)	SI	
Soporta 802.3ae (10 Gbps)	SI	
Soporta 802.3u (100Mbps)	SI	
Soporta 802.3x (full duplex)	SI	
Soporta 802.3z (1000Base-X)	SI	
Soporta "Link Aggregation" (IEEE 802.3ad)	SI ≥32 grupos	
Soporta IEEE 802.1s (MISTP)	SI	
Soporta IEEE 802.1w (RSTP)	SI	
Soporta IEEE 802.1d (STP)	SI	
Soporta Egress committed rate (ECR)	SI	
Soporta MVR (Multicast VLAN registration)	SI	
Soporta "Rapid Spanning Tree" (IEEE 802.1w)	SI	
Capacidad de limitación de velocidad basado en la dirección IP de fuente y destino	SI	
Capacidad de manejar políticas individuales o agregadas por puerto	Si SI ≥64 políticas	
Soporta ACL basado en puerto	SI	
Soporta Autenticación TACACs	SI	
Soporta BPDU	SI	
Soporta STRG (Spanning-Tree Root Guard)	SI	
Capacidad de VLAN IDs	≥4000	
Soporta monitorización remota SPAN (RSPAN)	SI	
Soporta Network Timing Protocol (NTP)	SI	
Soporta RIPng – (RIP Next Generation)	SI	
Soporta Multicast Listener Discovery (MLD)	SI	
Soporta túneles IPv6	SI	
Soporta Dot1p	SI	
Soporta Precedencia DiffServ (RFC 2474)	SI ≥8 colas/puerto	
Soporta DiffServ (RFC 2598, RFC 2597, RFC 2475)	SI	
Soporta CPU Redundante	SI	
Soporta voltajes de alimentación entre 100 y 240VAC 50Hz	SI	
Capacidad para fuente de alimentación redundante con "Load-Sharing"	SI	
Soporta rango de Temperatura (Celsius)	0° a 45°C	
Capacidad de tramas jumbo	SI ≥9000 bytes	
Capacidad de VLAN por red	SI ≥250	
Dynamic VLANs basado en Direccionamiento MAC,	SI	

Autenticación y VLAN privado		
VLAN exclusivo para voz	SI	
Soporta Detección automatica de teléfonos IP	SI	
Soporta GVRP	SI	
Soporta balanceo de carga por puerto basado en direccionamiento IP y MAC	SI	
Capacidad de detectar Intrusion	SI	
Soporta DoS (Denial of service)	SI	
Soporta mecanismos EAP (MD5, TLS, TTLS)	SI	
Soporta ARP	SI	
ICMP (RFC792, RFC1122)	SI	
Capacidad de configurar tamaño de paquete MTU por interfaz IP	SI	
Soporta IRDP (Internet Router Discovery Protocol - RFC 1256)	SI	
Soporta RIP v1 y RIP v2	SI	
Soporta MPLS (Multiprotocol Label Switching)	SI	
Soporta VPN en Capa 2 y Capa 3	SI	
Capacidad de configuración QoS por cada interfaz virtual o físico	SI	
Soporta CLI (Command Line Interface) vía puerto de consola	SI	
Soporta GUI (Graphical User Interface)	SI	
Capacidad de manejar estadísticas, históricos, alarmas and eventos	SI	
MTBF	>200.000 horas	
Certificaciones necesarias: ISO 9000; FCC CRF Title 47 Subpart B (Class A and Class B* limits); VCCI (Class A and Class B* limits); EN 55022: 2006 (Emission Standard); US UL 60950; UL-AR, Argentina	SI	
Periodo de Garantía mínima	12 meses	
Todos estos puntos son requerimientos mínimos exigibles y no sé aceptarán ofertas que no cumplan con las mismas. Esto a los efectos de garantizar la calidad y compatibilidad de los dispositivos solicitados.	SI	

Nota: Los demás puntos de las especificaciones técnicas quedan sin modificación alguna.