LICITACIÓN POR CONCURSO DE OFERTAS LCO Nº 15/2015 "ADQUISICIÓN DE EQUIPOS DE SEGURIDAD DE RED DE FIREWELL – AD REFERENDUM"

ID Nº 301.842

ADENDA Nº 03

Se modifica parcialmente el Pliego de Bases y Condiciones del presente llamado, de la siguiente manera:

QUEDA REDACTADA DE LA SIGUIENTE MANERA:

Sección I Datos de la Licitación (DDL)

IAO 10.1

, anexos técnicos, folletos y otros

textos complementarios en idioma diferente al castellano: SI La convocante aceptará catálogos, anexos técnicos, folletos y otros textos complementarios en idioma ingles

En forma solo enunciativa y no limitativa, se podrán presentar los siguientes documentos en el idioma de origen del documento: NO SE APLICA

Sección III. Suministros Requeridos

1.9 Equipo de Seguridad Perimetral

Donde Dice:

1.9 Equipo de Seguridad Perimetral				
Marca:			**El bien ofertado cumple con los requerimientos**	
Modelo:				
Procedencia:				
Cantidad:	**1 (Una) Unidad**			
Características	**Requerimientos**	**Carácter**	**Si**	**No**

La Solución propuesta deberá incorporar en un solo equipo las siguientes funcionalidades:	• Equipo de seguridad tipo Statefulinspection • VPN IPSec • VPN SSL • Antivirus y Antispyware de perímetro • Sistema de Prevención de intrusos • Sistema de filtrado de navegación Web • Administración de ancho de banda • Funcionalidades de routing • Datos Estadísticos y de registro	Exigido		
	La solución deberá ser tipo appliance, una plataforma específica para hacer labores de NextGeneration de seguridad	Exigido		
	La solución deberá tener sistema operativo propietario, sistemas operativos basados en Linux o Windows Tipo "Endurecido" no serán aceptadas.	Exigido		
	Tecnología de procesamiento multinúcleo.	Exigido		
Consumo máximo de energía	<= 100 W	Exigido		
Calor maximo generado	<= 71 W	Exigido		
Puertos Ethernet 10/100/1000 en cobre	>= 4	Exigido		
Puertos Ethernet 10/100/1000 en SFP	>= 4	Exigido		
Pantalla	Pantalla de información visual (pantalla LCD)	Exigido		
Fuente de Alimentación	Fuentes de poder redundantes (se deberá incluir la fuente redundante)	Exigido		
Tensión de alimentación	100-240 Vac	Exigido		
Frecuencia de alimentación	50/60Hz	Exigido		
Ventiladores	Hotswap Redundantes	Exigido		
Ahorro de Energía	El equipo a deberá cumplir con las normas de EnergyStar o certificación similar (reducción del consumo y el costo de la energía, además de proteger al medio ambiente utilizando productos y practicas especificas)	Exigido		
Administración	Sin límites a nivel lógico de la cantidad	Exigido		

	de usuarios			
Redundancia	El sistema permitirá el uso failover de puertos, es decir si una interface falla automáticamente opere otra	Exigido		
Cantidad de VLANs	≥ 512	Exigido		
Soporte y Capacidades	El sistema soportará enrutamiendo basado en políticas para que el tráfico sea enrutado a las diferentes interfaces basado en el servicio, la direcciónes IP de origen o de destino	Exigido		
	El sistema deberá Permitir enrutamiento: BGP, OSPF, RIPv1/v2, rutas estáticas, Multicast	Exigido		
	El sistema deberá tener capacidad de soportar NAT 1:1, 1:muchos, muchos:1, muchos:muchos, flexible NAT, PAT, y modo transparente	Exigido		
	El sistema deberá soportar Jumbo Frames	Exigido		
	El sistema deberá soportar Port Mirroring	Exigido		
Características de Seguridad				
Implementación	El sistema podrá ser implementado como Router, Layer 2 bridge, Wiremode (Sin hacer bridge capa 2) o como un networktap escuchando el tráfico	Exigido		
Rendimiento de Equipo de seguridad usando la metodología de medición basada en el RFC 2544.	≥ 3 Gbps	Exigido		
Rendimiento de Equipo de seguridad usando la metodología de medición basada en IMIX.	≥ 300 Mbps	Exigido		
Cantidad de conexiones en modo equipo de seguridad	≥ 1.200.000.	Exigido		
Cantidad de conexiones con los módulos de IPS, Antivirus, Antispyware y Control de Aplicaciones activados (DPI)	>= 25.000.	Exigido		
Rendimiento del Equipo de seguridad con VPN,	>= 400 Mbps	Exigido		

AES-128				
Certificación	El producto debe contar con las certificación ICSA Equipo de Seguridad o similar	Exigido		
Características VPN				
Cantidad de túnelesvpnSite to Site soportados	≥ 10.000.-.	Exigido		
Throughput VPN	>= 400 Mbps	Exigido		
Licencias cliente VPN para acceso remoto suministradas	>= 100.	Exigido		
Trafico	Para VPNs, descontaminar el tráfico en tiempo real antes de que llegue a la red corporativa y sin necesidad de que intervenga el usuario. De este modo se neutralizan a tiempo las vulnerabilidades y el código malicioso.	Exigido		
Certificación	El sistema deberá tener certificación VPNc (VPN Consortium)	Exigido		
Ipsec	Deben ser soportadas tanto una CA Interna como una CA externa provista por un tercero.	Exigido		
	Deben ser soportados 3DES y AES-256 para las fases I y II de IKE.	Exigido		
	Debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).	Exigido		
	Debe soportar integridad de datos con md5 y sha1.	Exigido		
	Debe incluir soporte a las topologías VPNs site-to-site: Full Meshed (todos a todos), Star (Oficinas Remotas a Sitio Central) y Hub and Spoke (Sitio remoto a través del sitio central hacia otro sitio remoto)	Exigido		
	Soporte a VPNs client-to-site basadas en IPSEC.	Exigido		
SSL	Debe tener la posibilidad de realizar VPNs SSL sin cliente para acceso remoto, sin necesidad de instalar un cliente.	Exigido		
	Soporte a VPNs tipo L2TP, incluyendo el soporte al cliente L2TP del Iphone.	Exigido		

	El cliente VPNs IPSEC debe soportar roaming (moverse entre diferentes redes/interfaces y cambiar de dirección IP sin presentar desconexión de la VPN) y la funcionalidad de Auto-Connect (detección cuando el endpoint esta afuera de la compañía y una aplicación necesita acceso a la red corporativa y realiza la conexión automática)	Exigido		
	Debe incluir un método simple y central, de crear túneles permanentes entre gateways del mismo fabricante.	Exigido		
	El administrador debe poder aplicar reglas de control de tráfico, al interior de la VPN.	Exigido		
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 50 categorías y debe actualizarse automáticamente.	Exigido		
	Filtrado de contenido basado en categorías 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.	Exigido		
	Configurable directamente desde la interfaz de administración del dispositivo appliance.	Exigido		
	Permitir crear perfiles para filtro de contenido y que sean aplicados a usuarios locales o de LDAP/Active directory, Grupos o Direcciones IP	Exigido		
	Debe cubrir mas de 100 millones de sitios web en al menos 64 categorías preconfiguradas, incluidas las siguientes: Adult, advertisements, arts, chat, computing, criminal, drugs, education, finance, food, gambling, games, glamour & intimate apparel, government, hacking, hate speech,	Exigido		

	health, hobbies, hosting sites, job search, kids sites, lifestyle & culture, motor vehicles, news, personals & dating, photo searches, real estate, reference, religion, remote proxies, search engines, sex education, shopping, sports, streaming media, travel, Usenet news, violence, weapons, web based e-mail.			
	Rastreo por HTTP URL, HTTPS IP, palabra clave y contenido, bloqueo de ActiveX, Java Applet, y cookies, gestión del ancho de banda según categorías de clasificación, listas de admitidos/bloqueados personalizadas	Exigido		
	Debe permitir la creación de excepciones basadas en la definición de objetos de red.	Exigido		
	Debe proveer la opción de modificar la notificación de bloqueo, y redireccionar al usuario a otra página.	Exigido		
	El Filtrado de URL debe poder integrarse a un mecanismo, o bloque de seguridad, que permita controlar aplicaciones web 2.0 y widgets. Dicha integración debe ser dentro del mismo Gateway sin el uso de herramientas de terceros o servidores separados.	Exigido		
	El Gateway de Filtrado URL debe tener la capacidad de bloquear granularmente sitios basado en Web 2.0.	Exigido		
	El Firewall Web debe tener la capacidad de identificar y bloquear herramientas de “proxy bypass” sobre protocolos estándar y no estándar (sin la necesidad de instalar un agente en los hosts o licencias adicionales).	Exigido		
	Debe bloquear Malware sobre sitios Web y Web 2.0.	Exigido		
	Debe incluir un método dinámico en la nube para la categorización de los sitios Web existentes y nuevos sitios emergentes.	Exigido		

	Debe inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL. El Gateway de Filtrado de URL debe hacer dicha inspección como si fuera texto claro, sin la necesidad de utilizar herramientas de terceros, servidores o licencias adicionales.	Exigido		
IPS	El IPS integrado, debe incluir al menos los siguientes mecanismos de defensa: Application control: Previene el uso de aplicaciones específicas del usuario. Engine settings: Protecciones que contienen ajustes que alteran el comportamiento de otras protecciones. Protocol Anomalies: grupo de protecciones que identifican cuando el tráfico no cumple con los estándares del protocolo. Signatures: grupo de protecciones que identifica el tráfico que intenta explotar una vulnerabilidad específica.	Exigido		
	Los módulos de IPS Integrado y de Firewall, deben estar integrados ofreciendo de esta manera, protección multicapa.	Exigido		
	El administrador debe poder configurar la inspección, solo para el tráfico interno.	Exigido		
	El IPS debe proveer al menos dos políticas o perfiles precargados, para ser usados inmediatamente.	Exigido		
	Debe incluir una opción, que permita detener la inspección del IPS en el Gateway bajo condiciones de alta carga, definiendo estos límites basados en % de CPU y Memoria que el administrador decida.	Exigido		
	El IPS integrado, debe incluir la habilidad de detener temporalmente la inspección y bloqueo en el gateway, para efectos de “troubleshooting”.	Exigido		

	El administrador debe poder activar automáticamente nuevas firmas, basados en parámetros de configuración definidos previamente (impacto en el desempeño, severidad de la amenaza, tipo de protección: server o client)	Exigido		
	Debe poder detectar y bloquear las siguientes tipos de amenazas: : Protocol misuse, comunicaciones Outbound con malware, Intentos de Tunneling y ataques genéricos sin contar con firmas predefinidas	Exigido		
	Para cada protección se debe incluir la siguiente información: Tipo de protección (cliente o server), severidad de la amenaza, Impacto en el desempeño, y nivel de confidencia.	Exigido		
	Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en origen, destino, servicio o la combinación de los 3 factores.	Exigido		
	Debe poder realizar captura de paquetes para protecciones específicas.	Exigido		
	Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: Email, DNS, FTP, servicios de Windows (Microsoft Networking) y SNMP.	Exigido		
	Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos. El administrador debe poder definir objetos de red y servicios a excluir.	Exigido		
	Debe proteger contra ataques tipo DNS Cache Poisoning, y de esa manera prevenir a los usuarios el acceso a dominios bloqueados.	Exigido		
	Debe incluir protecciones para los protocolos POP3 e IMAP.	Exigido		
	Debe soportar y proteger protocolos de VoIP (H.323, SIP, MGP y SCCP), asegurando que todos los paquetes de	Exigido		

	VoIP son estructuralmente válidos.			
	Debe detectar y bloquear aplicaciones que realizan control remoto, incluyendo aquellas que son capaces de hacer tunneling en tráfico HTTP.	Exigido		
	El administrador debe poder permitir chat MSN Messenger pero bloquear el Video.	Exigido		
	Debe incluir protección a vulnerabilidades Citrix ICA e implementar cumplimientos de protocolo.	Exigido		
	Debe permitir bloquear tráfico entrante, saliente o ambos correspondiente a determinados paises, sin necesidad de actualizar manualmente los rangos IP correspondientes a cada país.	Exigido		
	Con el fin de incrementar la estabilidad del Gateway de IPS, debe brindar un mecanismo que sea capaz de administrar la capacidad de la tabla de conexiones y el consumo de la memoria del Gateway, esto permitirá al Gateway manejar grandes cantidades de tráfico inesperado, por ejemplo en ataques de denegación de servicio.	Exigido		
	Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound.	Exigido		
Control de Aplicaciones	La solución debe integrar reglas de filtrado de URL y control aplicaciones en la misma licencia.	Exigido		
	La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web.	Exigido		
	La solución debe proveer una librería de aplicaciones que incluya aplicaciones Web 2.0, Widgets y base de datos de URL.	Exigido		
	La solución debe ser capaz de integrar control de aplicaciones y filtrado de URL dentro de la misma plataforma que además proporcione una solución	Exigido		

	de firewall, IPS, etc.			
	La administración debe centralizar las políticas de seguridad del control de aplicaciones y filtrado URL en la misma consola.	Exigido		
	Debe tener la capacidad de hacer un análisis avanzado que incluya, tráfico por sitios, graficas, estadísticas, etc.	Exigido		
	Tiene que crear políticas granulares para sitios Web, Web 2.0 y control de aplicaciones	Exigido		
	Debe ser posible permitir o bloquear aplicaciones o sitios al menos por lo siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales y grupos de usuarios.	Exigido		
	Debe inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL. El Gateway de Filtrado de URL debe hacer dicha inspección como si fuera texto plano.	Exigido		
	Debe contar con un repositorio en línea para identificar URLs y aplicaciones no clasificadas	Exigido		
	Debe tener un servicio de clasificación basando en la nube que permita categorizar dinámicamente el tráfico Web.	Exigido		
	Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.	Exigido		
	Debe ser posible integrar la solución con Directorio Activo u Open LDAP para crear reglas de control de aplicaciones y filtrado URL basadas en: usuarios, grupos de Usuarios, maquinas, dirección IP, redes y todas las opciones combinadas	Exigido		
	Debe ser posible usar al menos las siguientes cuatro acciones en una regla de control de aplicaciones y filtrado de URL: bloquear, monitorear,	Exigido		

	informar al usuario y preguntar al usuario			
	Debe ser posible crear, por regla, un portal adaptable que permita interactuar con el usuario.	Exigido		
	Se debe de poder crear un portal diferente cuando la conexión provenga de dispositivos móviles.	Exigido		
	La solución debe controlar el ancho de banda de las aplicaciones por regla.	Exigido		
	La solución debe permitir la creación de objetos de tiempo por aplicación o grupo de aplicaciones en las reglas, para que una acción definida se cumpla sólo durante tiempos especificados.	Exigido		
Antivirus y Anti-Malware	El gateway antivirus debe realizar scan de virus y bloquearlos en al menos los siguientes protocolos: POP3, FTP, SMTP y HTTP.	Exigido		
	Debe incluir un anti-spyware basado en patrones.	Exigido		
	Debe permitir al administrador elegir la acción (scan, block o pass) para al menos 70 diferentes tipos de archivos. La detección del tipo de archivo no debe ser basada en la extensión del mismo.	Exigido		
	El antivirus debe soportar descargas continuas, de manera que se comience a enviar el archivo escaneado antes de realizar el scan completo del archivo y de esta manera evitar timeouts cuando se realizan scans sobre archivos grandes.	Exigido		
	Debe soportar archivos de al menos 2GB con la opción de configurar un tamaño más pequeño de archivo. El administrador debe poder decidir el límite de tamaño de archivo antes de bloquearlo, o pasarlo sin ningún tipo de scan.	Exigido		
	Debe poder realizar descompresión de archivos, con la opción de poder configurar el máximo nivel de anidación y de compresión para evitar	Exigido		

	ataques DoS.			
	Debe ofrecer al administrador la posibilidad de decidir qué tipos de archivos pueden usar las descargas continuas, y cuáles deben ser escaneados, en su totalidad, antes de iniciar la transferencia al cliente.	Exigido		
	Debe soportar el escaneo por dirección , es decir que el Gateway sea capaz de detectar y escanear archivos que se mueven en una dirección particular, por ejemplo de redes externas o cuando cruza una DMZ.	Exigido		
	El módulo de Antivirus & antimalware debe hacer escaneo en tiempo real tanto de antivirus como de antimalware.	Exigido		
	Se debe poder determinar acciones cuando el escaneo de archivos falle o haya sobre carga en el motor de antivirus.	Exigido		
	Debe hacer inspección sobre tráfico encriptado SSL.	Exigido		
AntiSpam & Seguridad de Email	Debe incluir la posibilidad de bloquear a través de IP reputation, y evitar de esa forma los falsos positivos.	Exigido		
	Debe incluir un mecanismo de protección Zero-hour efectiva contra virus que se propagan por email, sin confiar únicamente en métodos heurísticos o de inspección de contenidos.	Exigido		
	Debe incluir proteccion IPS dentro del email, que permita proteger contra ataques DoS y buffer over-flow.	Exigido		
	Debe bloquear Spam usando deteccion basada en patrones, que permita proteger al menos contra spam basado en imagenes y lenguaje extranjero.	Exigido		
	Debe permitir la creación de listas blancas y negras que pueden ser encontradas también como block list y allow list.	Exigido		

	La solución debe permitir al menos el envío de traps SNMP, alerta vía email y definición de scripts para las políticas de reputación de IP y para las políticas de contenido.	Exigido		
	Debe ser posible crear excepciones de red para el tráfico de correo específico.	Exigido		
AntiBot	La solución debe proveer una herramienta que haga descubrimiento de bots dentro de la red institucional. Dicha herramienta debe bloquear la comunicación que intenten establecer los bots con los atacantes.	Exigido		
	La solución debe poder detectar host infectados con bots, analizando el tráfico de la red utilizando una tecnología multicapa.	Exigido		
	La herramienta antibot debe analizar al menos 250 millones de direcciones para descubrimiento de bots, que incluyan al menos, direcciones de: IP de Command and Control, URL y DNS.	Exigido		
	Debe incluir al menos 2000 patrones de comunicación de botnets.	Exigido		
	La solución debe incluir al menos los siguientes métodos de identificación: **Identificación de direcciones de Command and control** utilizadas por los criminales para controlar los bots. **Identificación de patrones de comunicación** utilizada por cada familia de bots. **Identificación de comportamiento de bots.**	Exigido		
	La solución debe utilizar tecnología de inspección multicapas.	Exigido		
	La herramienta debe contar con una base de datos en la nube para para la actualización de las firmas.	Exigido		
	Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound.	Exigido		
Acceso Móvil SSL VPN	Se debe incluir el licenciamiento para 5 usuarios concurrentes a SSL VPN en cada equipo.	Exigido		

	La solución debe soportar Secure Sockets Layer (SSL) versión 3, con los siguientes algoritmos de cifrado simétrico y longitud de llaves: RC4 (128 bits), 3DES (128 y 256bits) y AES (128 y 256bits).	Exigido		
	La solución debe tener la opción de reforzar simultáneamente el control de login mediante el bloqueo de sesiones concurrentes desde el mismo usuario.	Exigido		
	La solución debe soportar dispositivos móviles con el uso de un cliente específico de acceso remoto. Dicho cliente debe soportar como mínimo las siguientes plataformas: Windows PocketPC 2003/SE y Windows Mobile 5.0 en PDA y Smartphones.	Exigido		
	Debe soportar aceleración de hardware para SSL/TLS key exchange.	Exigido		
	La solución debe soportar Secure Workspace y SSL Network Extender (Application and Network Modes) en Windows 7 32/64-bit	Exigido		
	La solución debe soportar control de aplicaciones SSL Network Extender por el mismo fabricante del software para que pueda ser de fácil elección el permitir aplicaciones de un fabricante específico.	Exigido		
	La solución debe instalarse sobre iPhone, iPad, y Android	Exigido		
	La solución debe permitir el acceso a aplicaciones Web	Exigido		
	La solución debe permitir el acceso a correo electrónico, calendario y contactos	Exigido		
	La solución debe contar con autenticación de doble factor mediante el certificado del cliente y el usuario/contraseña.	Exigido		
	La solución debe tener soporte para dispositivos móviles con Windows Mobile, iPhone, iPad y Android, permitiendo que todas las aplicaciones nativas tengan acceso por	Exigido		

	los clientes remotos autorizados del dispositivo móvil.			
Funciones Avanzadas de Red y Clustering	Debe soportar al menos los siguientes protocolos de routing: BGP, OSPF, RIPv1 y RIPv2.	Exigido		
	Debe soportar al memos los siguientes protocolos de multicast: IGMP, PIM-DM, PIM-SM	Exigido		
	Weighted Fair Queuing (WFQ) debe soportarse para asignar un mínimo de ancho de banda a un grupo de conexiones o a una conexión específica.	Exigido		
	Debe soportar la asignación de pesos para la definición de prioridades en la asignación de ancho de banda.	Exigido		
	Debe poderse definir limites en el ancho de banda, para restringir aplicaciones no criticas de red.	Exigido		
	Debe soportar Low latency queuing (LLQ) e Integrated Differentiated Services (DiffServ).	Exigido		
	Debe soportar Alta Disponibilidad y Balanceo de Carga de links de al menos 2 ISP, sin depender del uso de enrutamientos dinámicos o equipos externos dedicados.	Exigido		
	La solución debe soportar balanceo a servidores, sin la necesidad de usar software / hardware de terceros, es decir que sea capaz de distribuir tráfico de red a un grupo determinado de servidores.	Exigido		
	El balanceo a servidores debe soportar al menos los siguientes métodos: carga de servidor, round-robin, random, y dominio.	Exigido		
	Dicho balanceo debe permitir configurar persistencia ya sea por servidor o servicio, es decir que la conexión que fue establecida inicialmente entre un cliente y un servidor se mantenga.	Exigido		
	El hardware debe estar basado en una arquitectura abierta, usando	Exigido		

	procesadores Intel o AMD para mantener la flexibilidad y adaptarse a nuevas amenazas, sin disminuir el desempeño.			
	Debe incluir balanceo de carga de Gateways con sincronización de estados, sin necesidad de usar un balanceador externo.	Exigido		
	La solución debe proveer un mecanismo que permita la utilización de todos los procesadores con que cuente el hardware, es decir que pueda dividir la carga de trabajo entre procesadores	Exigido		
	Para una mejor distribución del tráfico, debe poder asociarse el tráfico de una interfaz de red exclusivamente con un procesador	Exigido		
	La solución debe trabajar como un clúster activo/activo con la posibilidad de trabajar como cluster activo/pasivo.	Exigido		
Identificación de usuarios	La identidad de los usuarios se debe poder compartir entre Gateways de Seguridad, de esta forma el usuario sólo se autentificará en un Gateway, y podrá navegar en otros Gateways con esta identidad.	Exigido		
	La solución debe proteger a los clientes de ataques IP-spoofing y Identiity-Spoofing.	Exigido		
	La solución debe proveer una forma de autentificación para los usuarios que no utilicen plataforma de Windows.	Exigido		
	La solución tiene que proveer configuración de acceso basado en tiempo para que los usuarios puedan entrar a los recursos de la red.	Exigido		
	El Gateway de Seguridad debe ser capaz de distinguir entre cuentas de servidores de aplicación y cuentas de usuario.	Exigido		
	Debe soportar el uso de expresiones regulares para la exclusión de usuarios.	Exigido		

	La solución debe proveer tres métodos para obtener las identidades de los usuarios: Sin agente haciendo búsquedas al directorio activo, agente instalado en los equipos del usuario final o portal cautivo.	Exigido		
	Cuando se detecte que los usuarios no se han autenticado, la solución tiene que redireccionarlos a un portal cautivo, a través del protocolo http.	Exigido		
	Dicho portal debe ser completamente adaptable a la imagen corporativa de la organización, es decir que la URL, el título del portal, las imagines utilizadas en el mismo, el lenguaje y la información solicitada al usuario tiene que ser adaptable.	Exigido		
	La solución debe soportar el uso del protocolo WMI (windows managemwnt instrumentation).	Exigido		
	Debe proveer un portal cautivo, para autentificar a los usuarios que no están dentro del directorio activo, los usuarios que no tienen plataforma Windows y los usuarios invitados.	Exigido		
	Los agentes instalados en los equipos, deben proveer un sistema de autentificación SSO (single-sing-on).	Exigido		
	Debe soportar al menos los siguientes métodos de autentificación: nombre de usuario y contraseña, que podrá ser configurado en la base de datos interna del Gateway, servidor de LDAP y servidor de RADIUS.	Exigido		
	Para una implementación sencilla, la solución debe proveer un wizard de configuración.	Exigido		
	Todas las características de la solución deben tener la capacidad de instalarse en un solo Gateway sin la necesidad de usar diferentes servidores o herramientas de terceros para su funcionamiento.	Exigido		
	Debe ser posible desde que zona de la red (Interna, Externa o DMZ) podrá estar disponible el portal cautivo.	Exigido		

	La solución debe retener la identidad de los usuarios aun cuando estos cambien la dirección IP.	Exigido		
	Debe proveer tres tipos de agente para el usuario final: versión completa que provea etiquetación de paquete y protección contra ataques de ip-spoofing, versión ligera que es sólo para autentificación y la versión adaptable.	Exigido		
	Los agentes deben poder descargarse dentro de un portal web, dentro de la misma plataforma, o poderse distribuir a través de software de terceros como archivos MSI.	Exigido		
	El Gateway de Seguridad debe poder implementarse en modo puente o en modo ruteo.	Exigido		
	La solución debe ser capaz de restringir el acceso a la red cuando no se acepte el acuerdo de usuarios (Agreement).	Exigido		
	Debe ser posible solicitar a los usuarios la re autentificación después de un intervalo de tiempo.	Exigido		
	Debe ser posible configurar al Gateway de seguridad en un bosque de dominio	Exigido		
	Debe ser posible verificar el estado de los controladores de dominio vía consola de comandos.	Exigido		
	La solución debe poder integrarse con el directorio activo sin la necesidad de instalar un agente en el servidor de dominio o en los equipos de los usuarios finales.	Exigido		
	Con la finalidad de crear reglas de acceso por usuario, debe poder integrase con otras soluciones como: control de aplicaciones y filtrado de URL.	Exigido		
Administración de la Política de Red Integrada	Debe tener la funcionalidad de Administración de Políticas de Red integrada en el mismo dispositivo de seguridad.	Exigido		

	Debe soportar diferentes perfiles de administrador, incluyendo al menos los siguientes: read/write y read/only.	Exigido		
	Las comunicaciones entre todos los componentes que pertenezcan a un solo dominio de administración (servidor de administración, gateways), deben establecer comunicaciones seguras a través del uso de certificados para el cifrado.	Exigido		
	Debe incluir una entidad CA (Certificate Authority) interna X.509, que genere certificados al Gateway y a los usuarios para una fácil autenticación en las VPNs.	Exigido		
	Debe incluir la habilidad de confiar en CAs externas, que soporten standards PKCS#12, CAPI o Entrust.	Exigido		
	Debe incluir la opción de crear diferentes perfiles de IPS, que pueden ser aplicados a diferentes gateways.	Exigido		
	Debe incluir la opción de automáticamente habilitar nuevas protecciones de IPS basadas en: Severidad de la amenaza, Impacto de Desempeño y Nivel de Confidencia.	Exigido		
	Debe incluir una manera de marcar las protecciones de IPS para un futuro seguimiento o análisis.	Exigido		
	Debe incluir una herramienta de búsqueda, que permita fácilmente filtrar objetos de red. Debe también incluir la opción de buscar objetos duplicados (con la misma IP) y objetos no usados (en una regla o política) y una lista de las reglas en que un objeto especifico es usado.	Exigido		
	Debe incluir la opción de segmentar las reglas de acceso, usando etiquetas o títulos de sección y de esa forma organizar mejor la política.	Exigido		
	Debe incluir la opción de guardar la política completa o una especifica parte de la política.	Exigido		
	Se debe poder tener la opción de tener alta disponibilidad de	Exigido		

	administración, usando servidores de administración que se sincronizan con el servidor activo, sin necesidad de un dispositivo externo.			
	Debe incluir un comprensivo mapa, que incluya los objetos de red y sus conexiones. Estos mapas pueden ser exportados a una imagen o a Microsoft Visio.	Exigido		
	Debe incluir la habilidad de distribuir y aplicar centralizadamente nuevas versiones de software para el Gateway.	Exigido		
	Debe incluir una herramienta que administre centralizadamente la licencia de todos los gateways, controlados desde la estación de administración.	Exigido		
Administración de Logs Integrada	Debe tener la funcionalidad de Administración de Logs integrada en el mismo dispositivo de seguridad.	Exigido		
	Los logs, deben ser parte del mismo sistema de administración (incluido en el Servidor Administración de la seguridad) y opcionalmente los administradores deben poder instalar servidores de Logs por separado.	Exigido		
	Los logs deben poder estar en el servidor de administración o en un servidor separado.	Exigido		
	Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense.	Exigido		
	Debe poderse diferenciar entre logs de usuarios regulares y los logs propios de la administración.	Exigido		
	Por cada coincidencia de una regla, se debe poder configurar alguna de las siguientes opciones: Log, Alert, Send and SNMP trap, send and email, o ejecutar un user defined script.	Exigido		
	Los logs deben ser transferidos con seguridad entre el Gateway y el servidor de administración o el servidor de logs. De la misma manera	Exigido		

	desde y hacia la consola de administración del servidor.			
	Debe incluir la opción de que dinámicamente bloquee una conexión activa desde la interfase gráfica, sin la requerir la modificación de las reglas de acceso.	Exigido		
	Debe poderse exportar los logs en formato de base de datos.	Exigido		
	Debe poderse realizar un cambio automático de logs, basados en programaciones de tiempo o del tamaño del archivo.	Exigido		
	Debe permitir adicionar excepciones a las protecciones de IPS desde el log.	Exigido		
Garantías	La oferta deberá incluir soporte On-Site del proveedor, por todo el periodo de garantía del equipo.	Exigido		
	por el fabricante	Exigido		
	4 horas	Exigido		
	Las garantías, mantenimientos, entre otros, deben ser presentadas por escrito por el proveedor y al momento de la entrega definitiva de los equipos.	Exigido		
	Todos estos puntos son requerimientos mínimos 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, así como los servicios de post-venta (servicio técnico con mano de obra certificada por el fabricante, piezas originales, laboratorios autorizados por el fabricante).	Exigido		
	La oferta deberá considerar la provisión de todos aquellos materiales, accesorios, componentes o insumos que fuere necesario para la perfecta operatividad y que no esté contemplado en este pliego.	Exigido		

	Garantía escrita de un (1) año como mínimo, incluyendo Soporte de atención aplicada de 8 x 5 x Siguiente día Habil para Hardware, Mano de Obra y Repuestos incluyendo traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del proveedor.	Exigido		
		Exigido		

Debe Decir:

1.9 Equipo de Seguridad Perimetral				
Marca:			**El bien ofertado cumple con los requerimientos**	
Modelo:				
Procedencia:				
Cantidad:	**1 (Una) Unidad**			
Características	**Requerimientos**	**Carácter**	**Si**	**No**
La Solución propuesta deberá incorporar en un solo equipo las siguientes funcionalidades:	• Equipo de seguridad tipo Statefulinspection • VPN IPSec • VPN SSL • Antivirus y Antispyware de perímetro • Sistema de Prevención de intrusos • Sistema de filtrado de navegación Web • Administración de ancho de banda • Funcionalidades de routing • Datos Estadísticos y de registro	Exigido		
	La solución deberá ser tipo appliance, una plataforma específica para hacer labores de NextGeneration de seguridad	Exigido		
	La solución deberá tener sistema operativo propietario, sistemas operativos basados en Linux o Windows Tipo "Endurecido" no serán aceptadas.	Exigido		
	Tecnología de procesamiento multinúcleo.	Exigido		
Consumo máximo de energía	<= 100 W	Opcional		

Calor maximo generado	<= 71 W	Opcional		
Puertos Ethernet 10/100/1000 en cobre	>= 4	Exigido		
Puertos Ethernet 10/100/1000 en SFP	>= 4	Exigido		
Pantalla	Pantalla de información visual (pantalla LCD)	Exigido		
Fuente de Alimentación	Fuentes de poder redundantes (se deberá incluir la fuente redundante)	Exigido		
Tensión de alimentación	100-240 Vac	Exigido		
Frecuencia de alimentación	50/60Hz	Exigido		
Ventiladores	Hotswap Redundantes	Opcional		
Ahorro de Energía	El equipo a deberá cumplir con las normas de EnergyStar o certificación similar (reducción del consumo y el costo de la energía, además de proteger al medio ambiente utilizando productos y practicas especificas)	Exigido		
Administración	Sin límites a nivel lógico de la cantidad de usuarios	Exigido		
Redundancia	El sistema permitirá el uso failover de puertos, es decir si una interface falla automáticamente opere otra	Exigido		
Cantidad de VLANs	>= 500	Exigido		
Soporte y Capacidades	El sistema soportará enrutamiendo basado en políticas para que el tráfico sea enrutado a las diferentes interfaces basado en el servicio, la direcciónes IP de origen o de destino	Exigido		
	El sistema deberá Permitir enrutamiento: BGP, OSPF, RIPv1/v2, rutas estáticas, Multicast	Exigido		
	El sistema deberá tener capacidad de soportar NAT 1:1, 1:muchos, muchos:1, muchos:muchos, flexible NAT, PAT, y modo transparente	Exigido		
	El sistema deberá soportar Jumbo Frames	Exigido		
	El sistema deberá soportar Port Mirroring	Exigido		
Características de Seguridad				
Implementación	El sistema podrá ser implementado como Router, Layer 2 bridge, Wiremode (Sin hacer bridge capa 2) o	Exigido		

	como un networktap escuchando el tráfico			
Rendimiento de Equipo de seguridad usando la metodología de medición basada en el RFC 2544.	≥ 3 Gbps	Exigido		
Rendimiento de Equipo de seguridad usando la metodología de medición basada en IMIX.	≥ 300 Mbps	Exigido		
Cantidad de conexiones con los módulos de IPS, Antivirus, Antispyware y Control de Aplicaciones activados (DPI)	>= 25.000.	Exigido		
Rendimiento del Equipo de seguridad con VPN, AES-128	>= 400 Mbps	Exigido		
Certificación	El producto debe contar con las certificación ICSA Equipo de Seguridad o similar	Exigido		
Características VPN				
Cantidad de túnelesvpnSite to Site soportados	≥ 10.000.-.	Exigido		
Throughput VPN	>= 400 Mbps	Exigido		
Licencias cliente VPN para acceso remoto suministradas	>= 100.	Exigido		
Trafico	Para VPNs, descontaminar el tráfico en tiempo real antes de que llegue a la red corporativa y sin necesidad de que intervenga el usuario. De este modo se neutralizan a tiempo las vulnerabilidades y el código malicioso.	Exigido		
Certificación	El sistema deberá tener certificación VPNc (VPN Consortium)	Exigido		
Ipsec	Deben ser soportadas tanto una CA Interna como una CA externa provista por un tercero.	Exigido		
	Deben ser soportados 3DES y AES-256 para las fases I y II de IKE.	Exigido		
	Debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536	Exigido		

	bit), Grupo 14 (2048 bit).			
	Debe soportar integridad de datos con md5 y sha1.	Exigido		
	Debe incluir soporte a las topologías VPNs site-to-site: Full Meshed (todos a todos), Star (Oficinas Remotas a Sitio Central) y Hub and Spoke (Sitio remoto a través del sitio central hacia otro sitio remoto)	Exigido		
	Soporte a VPNs client-to-site basadas en IPSEC.	Exigido		
SSL	Debe tener la posibilidad de realizar VPNs SSL sin cliente para acceso remoto, sin necesidad de instalar un cliente.	Exigido		
	Soporte a VPNs tipo L2TP, incluyendo el soporte al cliente L2TP del Iphone.	Exigido		
	El cliente VPNs IPSEC debe soportar roaming (moverse entre diferentes redes/interfaces y cambiar de dirección IP sin presentar desconexión de la VPN) y la funcionalidad de Auto-Connect (detección cuando el endpoint esta afuera de la compañía y una aplicación necesita acceso a la red corporativa y realiza la conexión automática)	Exigido		
	Debe incluir un método simple y central, de crear túneles permanentes entre gateways del mismo fabricante.	Exigido		
	El administrador debe poder aplicar reglas de control de tráfico, al interior de la VPN.	Exigido		
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 60 categorías y debe actualizarse automáticamente.	Exigido		
	Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo	Exigido		

	o software adicional para realizar la categorización del contenido.			
	Configurable directamente desde la interfaz de administración del dispositivo appliance.	Exigido		
	Permitir crear perfiles para filtro de contenido y que sean aplicados a usuarios locales o de LDAP/Active directory, Grupos o Direcciones IP	Exigido		
	Debe cubrir mas de 100 millones de sitios web en al menos 60 categorías preconfiguradas, incluidas las siguientes: Adult, advertisements, arts, chat, computing, criminal, drugs, education, finance, food, gambling, games, glamour & intimate apparel, government, hacking, hate speech, health, hobbies, hosting sites, job search, kids sites, lifestyle & culture, motor vehicles, news, personals & dating, photo searches, real estate, reference, religion, remote proxies, search engines, sex education, shopping, sports, streaming media, travel, Usenet news, violence, weapons, web based e-mail.	Exigido		
	Rastreo por HTTP URL, HTTPS IP, palabra clave y contenido, bloqueo de ActiveX, Java Applet, y cookies, gestión del ancho de banda según categorías de clasificación, listas de admitidos/bloqueados personalizadas	Exigido		
	Debe permitir la creación de excepciones basadas en la definición de objetos de red.	Exigido		
	Debe proveer la opción de modificar la notificación de bloqueo, y redireccionar al usuario a otra página.	Exigido		
	El Filtrado de URL debe poder integrarse a un mecanismo, o bloque de seguridad, que permita controlar aplicaciones web 2.0 y widgets. Dicha integración debe ser dentro del mismo Gateway sin el uso de herramientas de terceros o servidores separados.	Exigido		

	El Gateway de Filtrado URL debe tener la capacidad de bloquear granularmente sitios basado en Web 2.0.	Exigido		
	El Firewall Web debe tener la capacidad de identificar y bloquear herramientas de “proxy bypass” sobre protocolos estándar y no estándar (sin la necesidad de instalar un agente en los hosts o licencias adicionales).	Exigido		
	Debe bloquear Malware sobre sitios Web y Web 2.0.	Exigido		
	Debe incluir un método dinámico en la nube para la categorización de los sitios Web existentes y nuevos sitios emergentes.	Exigido		
	Debe inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL. El Gateway de Filtrado de URL debe hacer dicha inspección como si fuera texto claro, sin la necesidad de utilizar herramientas de terceros, servidores o licencias adicionales.	Exigido		
IPS	El IPS integrado, debe incluir al menos los siguientes mecanismos de defensa: Application control: Previene el uso de aplicaciones específicas del usuario. Engine settings: Protecciones que contienen ajustes que alteran el comportamiento de otras protecciones. Protocol Anomalies: grupo de protecciones que identifican cuando el tráfico no cumple con los estándares del protocolo. Signatures: grupo de protecciones que identifica el tráfico que intenta explotar una vulnerabilidad específica.	Exigido		
	Los módulos de IPS Integrado y de Firewall, deben estar integrados ofreciendo de esta manera, protección multicapa.	Exigido		
	El administrador debe poder configurar la inspección, solo para el	Exigido		

	tráfico interno.			
	El IPS debe proveer al menos dos políticas o perfiles precargados, para ser usados inmediatamente.	Exigido		
	El IPS integrado, debe incluir la habilidad de detener temporalmente la inspección y bloqueo en el gateway, para efectos de “troubleshooting”.	Exigido		
	El administrador debe poder activar automáticamente nuevas firmas, basados en parámetros de configuración definidos previamente (impacto en el desempeño, severidad de la amenaza, tipo de protección: server o client)	Exigido		
	Debe poder detectar y bloquear las siguientes tipos de amenazas: : Protocol misuse, comunicaciones Outbound con malware, Intentos de Tunneling y ataques genéricos sin contar con firmas predefinidas	Exigido		
	Para cada protección se debe incluir la siguiente información: Tipo de protección (cliente o server), severidad de la amenaza, Impacto en el desempeño, y nivel de confidencia.	Exigido		
	Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en origen, destino, servicio o la combinación de los 3 factores.	Exigido		
	Debe poder realizar captura de paquetes para protecciones específicas.	Exigido		
	Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: Email, DNS, FTP, servicios de Windows (Microsoft Networking) y SNMP.	Exigido		
	Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos. El administrador debe poder definir objetos de red y servicios a excluir.	Exigido		

	Debe proteger contra ataques tipo DNS Cache Poisoning, y de esa manera prevenir a los usuarios el acceso a dominios bloqueados.	Exigido		
	Debe incluir protecciones para los protocolos POP3 e IMAP.	Exigido		
	Debe soportar y proteger protocolos de VoIP (H.323, SIP, MGP y SCCP), asegurando que todos los paquetes de VoIP son estructuralmente válidos.	Exigido		
	Debe detectar y bloquear aplicaciones que realizan control remoto, incluyendo aquellas que son capaces de hacer tunneling en tráfico HTTP.	Exigido		
	El administrador debe poder permitir chat MSN Messenger pero bloquear el Video.	Exigido		
	Debe incluir protección a vulnerabilidades Citrix ICA e implementar cumplimientos de protocolo.	Exigido		
	Debe permitir bloquear tráfico entrante, saliente o ambos correspondiente a determinados paises, sin necesidad de actualizar manualmente los rangos IP correspondientes a cada país.	Exigido		
	Con el fin de incrementar la estabilidad del Gateway de IPS, debe brindar un mecanismo que sea capaz de administrar la capacidad de la tabla de conexiones y el consumo de la memoria del Gateway, esto permitirá al Gateway manejar grandes cantidades de tráfico inesperado, por ejemplo en ataques de denegación de servicio.	Exigido		
	Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound.	Exigido		
Control de Aplicaciones	La solución debe integrar reglas de filtrado de URL y control aplicaciones en la misma licencia.	Exigido		
	La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web.	Exigido		

	La solución debe proveer una librería de aplicaciones que incluya aplicaciones Web 2.0, Widgets y base de datos de URL.	Exigido		
	La solución debe ser capaz de integrar control de aplicaciones y filtrado de URL dentro de la misma plataforma que además proporcione una solución de firewall, IPS, etc.	Exigido		
	La administración debe centralizar las políticas de seguridad del control de aplicaciones y filtrado URL en la misma consola.	Exigido		
	Debe tener la capacidad de hacer un análisis avanzado que incluya, tráfico por sitios, graficas, estadísticas, etc.	Exigido		
	Tiene que crear políticas granulares para sitios Web, Web 2.0 y control de aplicaciones	Exigido		
	Debe ser posible permitir o bloquear aplicaciones o sitios al menos por lo siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales y grupos de usuarios.	Exigido		
	Debe inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL. El Gateway de Filtrado de URL debe hacer dicha inspección como si fuera texto plano.	Exigido		
	Debe contar con un repositorio en línea para identificar URLs y aplicaciones no clasificadas	Exigido		
	Debe tener un servicio de clasificación basando en la nube que permita categorizar dinámicamente el tráfico Web.	Exigido		
	Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.	Exigido		
	Debe ser posible integrar la solución con Directorio Activo u Open LDAP para crear reglas de control de aplicaciones y filtrado URL basadas en:	Exigido		

	usuarios, grupos de Usuarios, maquinas, dirección IP, redes y todas las opciones combinadas			
	Debe ser posible usar al menos las siguientes cuatro acciones en una regla de control de aplicaciones y filtrado de URL: bloquear, monitorear, informar al usuario y preguntar al usuario	Exigido		
	Debe ser posible crear, por regla, un portal adaptable que permita interactuar con el usuario.	Exigido		
	Se debe de poder crear un portal diferente cuando la conexión provenga de dispositivos móviles.	Exigido		
	La solución debe controlar el ancho de banda de las aplicaciones por regla.	Exigido		
	La solución debe permitir la creación de objetos de tiempo por aplicación o grupo de aplicaciones en las reglas, para que una acción definida se cumpla sólo durante tiempos especificados.	Exigido		
Antivirus y Anti-Malware	El gateway antivirus debe realizar scan de virus y bloquearlos en al menos los siguientes protocolos: POP3, FTP, SMTP y HTTP.	Exigido		
	Debe incluir un anti-spyware basado en patrones.	Exigido		
	Debe permitir al administrador elegir la acción (scan, block o pass) para al menos 70 diferentes tipos de archivos. La detección del tipo de archivo no debe ser basada en la extensión del mismo.	Exigido		
	El antivirus debe soportar descargas continuas, de manera que se comience a enviar el archivo escaneado antes de realizar el scan completo del archivo y de esta manera evitar timeouts cuando se realizan scans sobre archivos grandes.	Exigido		
	Debe poder realizar descompresión de archivos, con la opción de poder configurar el máximo nivel de anidación y de compresión para evitar	Exigido		

	ataques DoS.			
	Debe ofrecer al administrador la posibilidad de decidir qué tipos de archivos pueden usar las descargas continuas, y cuáles deben ser escaneados, en su totalidad, antes de iniciar la transferencia al cliente.	Exigido		
	Debe soportar el escaneo por dirección , es decir que el Gateway sea capaz de detectar y escanear archivos que se mueven en una dirección particular, por ejemplo de redes externas o cuando cruza una DMZ.	Exigido		
	El módulo de Antivirus & antimalware debe hacer escaneo en tiempo real tanto de antivirus como de antimalware.	Exigido		
	Se debe poder determinar acciones cuando el escaneo de archivos falle o haya sobre carga en el motor de antivirus.	Exigido		
	Debe hacer inspección sobre tráfico encriptado SSL.	Exigido		
AntiSpam & Seguridad de Email	Debe incluir la posibilidad de bloquear a través de IP reputation, y evitar de esa forma los falsos positivos.	Exigido		
	Debe incluir un mecanismo de protección Zero-hour efectiva contra virus que se propagan por email, sin confiar únicamente en métodos heurísticos o de inspección de contenidos.	Exigido		
	Debe incluir proteccion IPS dentro del email, que permita proteger contra ataques DoS y buffer over-flow.	Exigido		
	Debe bloquear Spam usando deteccion basada en patrones, que permita proteger al menos contra spam basado en imagenes y lenguaje extranjero.	Exigido		
	Debe permitir la creación de listas blancas y negras que pueden ser encontradas también como block list y allow list.	Exigido		

	La solución debe permitir al menos el envío de traps SNMP, alerta vía email y definición de scripts para las políticas de reputación de IP y para las políticas de contenido.	Exigido		
	Debe ser posible crear excepciones de red para el tráfico de correo específico.	Exigido		
AntiBot	La solución debe proveer una herramienta que haga descubrimiento de bots dentro de la red institucional. Dicha herramienta debe bloquear la comunicación que intenten establecer los bots con los atacantes.	Exigido		
	La solución debe poder detectar host infectados con bots, analizando el tráfico de la red utilizando una tecnología multicapa.	Exigido		
	La herramienta antibot debe analizar al menos 250 millones de direcciones para descubrimiento de bots, que incluyan al menos, direcciones de: IP de Command and Control, URL y DNS.	Exigido		
	Debe incluir al menos 2000 patrones de comunicación de botnets.	Exigido		
	La solución debe incluir al menos los siguientes métodos de identificación: **Identificación de direcciones de Command and control** utilizadas por los criminales para controlar los bots. **Identificación de patrones de comunicación** utilizada por cada familia de bots. **Identificación de comportamiento de bots.**	Exigido		
	La solución debe utilizar tecnología de inspección multicapas.	Exigido		
	La herramienta debe contar con una base de datos en la nube para para la actualización de las firmas.	Exigido		
	Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound.	Exigido		
Acceso Móvil SSL VPN	Se debe incluir el licenciamiento para 5 usuarios concurrentes a SSL VPN en cada equipo.	Exigido		

	La solución debe soportar Secure Sockets Layer (SSL) versión 3, con los siguientes algoritmos de cifrado simétrico y longitud de llaves: RC4 (128 bits), 3DES (128 y 256bits) y AES (128 y 256bits).	Exigido		
	La solución debe tener la opción de reforzar simultáneamente el control de login mediante el bloqueo de sesiones concurrentes desde el mismo usuario.	Exigido		
	La solución debe soportar dispositivos móviles con el uso de un cliente específico de acceso remoto. Dicho cliente debe soportar como mínimo las siguientes plataformas: Windows PocketPC 2003/SE y Windows Mobile 5.0 en PDA y Smartphones.	Exigido		
	Debe soportar aceleración de hardware para SSL/TLS key exchange.	Exigido		
	La solución debe soportar Secure Workspace y SSL Network Extender (Application and Network Modes) en Windows 7 32/64-bit	Exigido		
	La solución debe soportar control de aplicaciones SSL Network Extender por el mismo fabricante del software para que pueda ser de fácil elección el permitir aplicaciones de un fabricante específico.	Exigido		
	La solución debe instalarse sobre iPhone, iPad, y Android	Exigido		
	La solución debe permitir el acceso a aplicaciones Web	Exigido		
	La solución debe permitir el acceso a correo electrónico, calendario y contactos	Exigido		
	La solución debe contar con autenticación de doble factor mediante el certificado del cliente y el usuario/contraseña.	Exigido		
	La solución debe tener soporte para dispositivos móviles con Windows Mobile, iPhone, iPad y Android, permitiendo que todas las aplicaciones nativas tengan acceso por los clientes	Exigido		

	remotos autorizados del dispositivo móvil.			
Funciones Avanzadas de Red y Clustering	Debe soportar al menos los siguientes protocolos de routing: BGP, OSPF, RIPv1 y RIPv2.	Exigido		
	Debe soportar al memos los siguientes protocolos de multicast: IGMP, PIM-DM, PIM-SM	Exigido		
	Weighted Fair Queuing (WFQ) debe soportarse para asignar un mínimo de ancho de banda a un grupo de conexiones o a una conexión específica.	Exigido		
	Debe soportar la asignación de pesos para la definición de prioridades en la asignación de ancho de banda.	Exigido		
	Debe poderse definir limites en el ancho de banda, para restringir aplicaciones no criticas de red.	Exigido		
	Debe soportar Low latency queuing (LLQ) e Integrated Differentiated Services (DiffServ).	Exigido		
	Debe soportar Alta Disponibilidad y Balanceo de Carga de links de al menos 2 ISP, sin depender del uso de enrutamientos dinámicos o equipos externos dedicados.	Exigido		
	La solución debe soportar balanceo a servidores, sin la necesidad de usar software / hardware de terceros, es decir que sea capaz de distribuir tráfico de red a un grupo determinado de servidores.	Exigido		
	El balanceo a servidores debe soportar al menos los siguientes métodos: carga de servidor, round-robin, random, y dominio.	Exigido		
	Dicho balanceo debe permitir configurar persistencia ya sea por servidor o servicio, es decir que la conexión que fue establecida inicialmente entre un cliente y un servidor se mantenga.	Exigido		
	Debe incluir balanceo de carga de Gateways con sincronización de	Exigido		

	estados, sin necesidad de usar un balanceador externo.			
	La solución debe proveer un mecanismo que permita la utilización de todos los procesadores con que cuente el hardware, es decir que pueda dividir la carga de trabajo entre procesadores	Exigido		
	Para una mejor distribución del tráfico, debe poder asociarse el tráfico de una interfaz de red exclusivamente con un procesador	Exigido		
	La solución debe trabajar como un clúster activo/activo con la posibilidad de trabajar como cluster activo/pasivo.	Exigido		
	La solución debe proteger a los clientes de ataques IP-spoofing y Identiity-Spoofing.	Exigido		
	La solución debe proveer una forma de autentificación para los usuarios que no utilicen plataforma de Windows.	Exigido		
	La solución tiene que proveer configuración de acceso basado en tiempo para que los usuarios puedan entrar a los recursos de la red.	Exigido		
	El Gateway de Seguridad debe ser capaz de distinguir entre cuentas de servidores de aplicación y cuentas de usuario.	Exigido		
	Debe soportar el uso de expresiones regulares para la exclusión de usuarios.	Exigido		
	La solución debe proveer tres métodos para obtener las identidades de los usuarios: Sin agente haciendo búsquedas al directorio activo, agente instalado en los equipos del usuario final o portal cautivo.	Exigido		
	Cuando se detecte que los usuarios no se han autenticado, la solución tiene que redireccionarlos a un portal cautivo, a través del protocolo http.	Exigido		

	Dicho portal debe ser completamente adaptable a la imagen corporativa de la organización, es decir que la URL, el título del portal, las imagines utilizadas en el mismo, el lenguaje y la información solicitada al usuario tiene que ser adaptable.	Exigido		
	La solución debe soportar el uso del protocolo WMI (windows managemwnt instrumentation).	Exigido		
	Debe proveer un portal cautivo, para autentificar a los usuarios que no están dentro del directorio activo, los usuarios que no tienen plataforma Windows y los usuarios invitados.	Exigido		
	Los agentes instalados en los equipos, deben proveer un sistema de autentificación SSO (single-sing-on).	Exigido		
	Debe soportar al menos los siguientes métodos de autentificación: nombre de usuario y contraseña, que podrá ser configurado en la base de datos interna del Gateway, servidor de LDAP y servidor de RADIUS.	Exigido		
	Para una implementación sencilla, la solución debe proveer un wizard de configuración.	Exigido		
	Todas las características de la solución deben tener la capacidad de instalarse en un solo Gateway sin la necesidad de usar diferentes servidores o herramientas de terceros para su funcionamiento.	Exigido		
	Debe ser posible desde que zona de la red (Interna, Externa o DMZ) podrá estar disponible el portal cautivo.	Exigido		
	La solución debe retener la identidad de los usuarios aun cuando estos cambien la dirección IP.	Exigido		
	Debe proveer tres tipos de agente para el usuario final: versión completa que provea etiquetación de paquete y protección contra ataques de ip-spoofing, versión ligera que es sólo para autentificación y la versión adaptable.	Exigido		

	Los agentes deben poder descargarse dentro de un portal web, dentro de la misma plataforma, o poderse distribuir a través de software de terceros como archivos MSI.	Exigido		
	El Gateway de Seguridad debe poder implementarse en modo puente o en modo ruteo.	Exigido		
	La solución debe ser capaz de restringir el acceso a la red cuando no se acepte el acuerdo de usuarios (Agreement).	Exigido		
	Debe ser posible solicitar a los usuarios la re autentificación después de un intervalo de tiempo.	Exigido		
	Debe ser posible configurar al Gateway de seguridad en un bosque de dominio	Exigido		
	Debe ser posible verificar el estado de los controladores de dominio vía consola de comandos.	Exigido		
	La solución debe poder integrarse con el directorio activo sin la necesidad de instalar un agente en el servidor de dominio o en los equipos de los usuarios finales.	Exigido		
	Con la finalidad de crear reglas de acceso por usuario, debe poder integrase con otras soluciones como: control de aplicaciones y filtrado de URL.	Exigido		
Administración de la Política de Red Integrada	Debe tener la funcionalidad de Administración de Políticas de Red integrada en el mismo dispositivo de seguridad.	Exigido		
	Debe soportar diferentes perfiles de administrador, incluyendo al menos los siguientes: read/write y read/only.	Exigido		
	Las comunicaciones entre todos los componentes que pertenezcan a un solo dominio de administración (servidor de administración, gateways), deben establecer comunicaciones seguras a través del uso de certificados para el cifrado.	Exigido		

	Debe incluir una entidad CA (Certificate Authority) interna X.509, que genere certificados al Gateway y a los usuarios para una fácil autenticación en las VPNs.	Exigido		
	Debe incluir la habilidad de confiar en CAs externas, que soporten standards PKCS#12, CAPI o Entrust.	Exigido		
	Debe incluir la opción de crear diferentes perfiles de IPS, que pueden ser aplicados a diferentes gateways.	Exigido		
	Debe incluir la opción de automáticamente habilitar nuevas protecciones de IPS basadas en: Severidad de la amenaza, Impacto de Desempeño y Nivel de Confidencia.	Exigido		
	Debe incluir una manera de marcar las protecciones de IPS para un futuro seguimiento o análisis.	Exigido		
	Debe incluir una herramienta de búsqueda, que permita fácilmente filtrar objetos de red. Debe también incluir la opción de buscar objetos duplicados (con la misma IP) y objetos no usados (en una regla o política) y una lista de las reglas en que un objeto especifico es usado.	Exigido		
	Debe incluir la opción de segmentar las reglas de acceso, usando etiquetas o títulos de sección y de esa forma organizar mejor la política.	Exigido		
	Debe incluir la opción de guardar la política completa o una especifica parte de la política.	Exigido		
	Se debe poder tener la opción de tener alta disponibilidad de administración, usando servidores de administración que se sincronizan con el servidor activo, sin necesidad de un dispositivo externo.	Exigido		
	Debe incluir un comprensivo mapa, que incluya los objetos de red y sus conexiones. Estos mapas pueden ser exportados a una imagen o a Microsoft Visio.	Exigido		

	Debe incluir la habilidad de distribuir y aplicar centralizadamente nuevas versiones de software para el Gateway.	Exigido		
	Debe incluir una herramienta que administre centralizadamente la licencia de todos los gateways, controlados desde la estación de administración.	Exigido		
Administración de Logs	Debe tener la funcionalidad de Administración de Logs integrada en el mismo dispositivo de seguridad, o incluir un dispostivo independiente.	Exigido		
	Los logs, deben ser parte del mismo sistema de administración (incluido en el Servidor Administración de la seguridad) y opcionalmente los administradores deben poder instalar servidores de Logs por separado.	Exigido		
	Los logs deben poder estar en el servidor de administración o en un servidor separado.	Exigido		
	Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense.	Exigido		
	Debe poderse diferenciar entre logs de usuarios regulares y los logs propios de la administración.	Exigido		
	Por cada coincidencia de una regla, se debe poder configurar alguna de las siguientes opciones: Log, Alert, Send and SNMP trap, send and email, o ejecutar un user defined script.	Exigido		
	Los logs deben ser transferidos con seguridad entre el Gateway y el servidor de administración o el servidor de logs. De la misma manera desde y hacia la consola de administración del servidor.	Exigido		
	Debe incluir la opción de que dinámicamente bloquee una conexión activa desde la interfase gráfica, sin la requerir la modificación de las reglas de acceso.	Exigido		
	Debe poderse exportar los logs en	Exigido		

	formato de base de datos.			
	Debe poderse realizar un cambio automático de logs, basados en programaciones de tiempo o del tamaño del archivo.	Exigido		
	Debe permitir adicionar excepciones a las protecciones de IPS desde el log.	Exigido		
Garantías	La oferta deberá incluir soporte On-Site del proveedor, por todo el periodo de garantía del equipo.	Exigido		
	por el fabricante	Exigido		
	4 horas	Exigido		
	Las garantías, mantenimientos, entre otros, deben ser presentadas por escrito por el proveedor y al momento de la entrega definitiva de los equipos.	Exigido		
	Todos estos puntos son requerimientos mínimos 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, así como los servicios de post-venta (servicio técnico con mano de obra certificada por el fabricante, piezas originales, laboratorios autorizados por el fabricante).	Exigido		
	La oferta deberá considerar la provisión de todos aquellos materiales, accesorios, componentes o insumos que fuere necesario para la perfecta operatividad y que no esté contemplado en este pliego.	Exigido		
	Garantía escrita de un (1) año como mínimo, incluyendo Soporte de atención aplicada de 8 x 5 x Siguiente día Habil para Hardware, Mano de Obra y Repuestos incluyendo traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del proveedor.	Exigido		
		Exigido		

1.10 Switch de Capa 3 para capa de Distribución.

Donde Dice:

1.10 Switch de Capa 3 para capa de Distribución.				
Marca:			**El bien ofertado cumple con los requerimientos**	
Modelo:				
Procedencia:				
Cantidad:	**1 (Una) Unidad**			
Características	**Requerimientos**	**Carácter**	**Si**	**No**
Descripción	Switch de 12 puertos Gigabit SFP	Exigido		
El equipo	Debe ser rackeables en infraestructuras de 19'' y deben incluir todos los accesorios necesarios para su montaje.	Exigido		
	Doble Fuente de poder 220VAC/50Hz con cable de alimentación con toma tipo americano.	Exigido		
	Deberá soportar un rango de temperatura de operación entre -2° y 40° C y un rango de Humedad no condensada de 10 a 95%.	Exigido		
	Deberá soportar un rango de temperatura de almacenamiento entre -2° y 60° C y un rango de Humedad no condensada de 10 a 95%.	Exigido		
	Deberá permitir operar en stack, el stack no deberá ser menor a 8 equipos	Exigido		
	Deberá tener un tiempo promedio entre fallas (MTBF) >= 300.000 horas.	Exigido		
Cantidad de puertos	Gigabit SFP >= 12	Exigido		
	Como mínimo 4 puertos SFP con velocidad de 1 Gbps o 2 puertos SFP de 10 Gbps (puertos independientes).	Exigido		
	Deberán proveerse con todos los módulo óptico (transceiver) de 1Gbps para Fibra Óptica MM/SM tipo SFP para la interconexión con los switches del ítem 11.	Exigido		
Performance	Capacidad de switching >= 160 Gbps.	Exigido		
	Capacidad de forwarding >= 50 Mpps.	Exigido		
	Deberá soportar al menos 4000 VLANs.	Exigido		
	El equipo deberá soportar frames >= 9000 bytes.	Exigido		
Protocolos y Funcionalidades	IEEE 802.1s	Exigido		
	IEEE 802.1w	Exigido		

	IEEE 802.11	Exigido		
	IEEE 802.1x	Exigido		
	IEEE 802.1x-Rev	Exigido		
	IEEE 802.3ad	Exigido		
	IEEE 802.3af	Exigido		
	IEEE 802.3at	Exigido		
	RMON I and II standards	Exigido		
	SNMPv1, SNMPv2c, and SNMPv3	Exigido		
	IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and	Exigido		
	1000BASE-T ports	Exigido		
	IEEE 802.1D Spanning Tree Protocol	Exigido		
	IEEE 802.1p CoS prioritization	Exigido		
	IEEE 802.1Q VLAN	Exigido		
	IEEE 802.3 10BASE-T specification	Exigido		
	IEEE 802.3u 100BASE-TX specification	Exigido		
	IEEE 802.3ab 1000BASE-T specification	Exigido		
	IEEE 802.3z 1000BASE-X specification	Exigido		
	Soporte de seguridad del puerto mediante filtrado por dirección MAC, limitación de direcciones MAC por puerto.	Exigido		
	Soporte de limitación de tráfico mediante lista de control de acceso (ACL) por direcciones MAC origen o destino y direcciones IP origen o destino.	Exigido		
	Soporte de portmirroring por puerto o por VLAN.	Exigido		
	Deberá soportar PrivateVLANs.	Exigido		
	Implementará políticas de clasificación de tráfico y reasignación (rewrite) de prioridad basadas en protocolo IP (direcciones origen y destino, puertos TCP/UDP origen y destino).	Exigido		
	Deberá soportar IGMP y DHCP snooping.	Exigido		
	Deberá permitir el control de tormentas de broadcast, multicast y unicast en cada puerto.	Exigido		
	Deberá poder realizar la inspección de paquetes ARP.	Exigido		
	Deberá soportar sincronización horaria por medio Network TimingProtocol (NTP).	Exigido		
Administración	Se deberán proveer los bloques de información de management (MIBs) necesarios.	Exigido		
	Deberá tener soporte de AAA utilizando Radius como mínimo.	Exigido		

	Posibilidad de configurar diferentes perfiles de usuarios de administración con diferentes grados de autorización para el acceso y ejecución de las distintas tareas de gestión de la red.	Exigido		
	Soporte de Autenticación de usuarios por puerto de acuerdo al estándar IEEE 802.1x.	Exigido		
	Almacenamiento de sistema operativo y configuración en memoria Flash reescribible con capacidad de actualización por medio de protocolo FTP según RFC 959 ó TFTP.	Exigido		
	Servicio de configuración por medio de puerto de consola.	Exigido		
	Servicio de configuración por medio de consola remota Telnet según RFCs 854/855 sobre transporte TCP/IP según RFCs 793/791.	Exigido		
	Soporte de Gestión Remota segura (SNMPv3 con cifrado, SSL y/o SSH).	Exigido		
	Capacidad de RemoteMonitoring (RMON), deberá soportar al menos 4 grupos (statistics, history, alarm, events).	Exigido		
Layer 3	Enrutamiento estatico	Exigido		
	Protocolos de enrutamiento Dinamico(IPv4): RIPv1; RIPv2; RIPng; OSPF	Exigido		
	Protocolos de enrutamiento Dinamico (IPv6): OSPF	Exigido		
	Policy-based Routing PBR	Exigido		
	PIM-SM	Exigido		
	IPv6	Exigido		

Certificaciones	UL 60950-1 Second Edition CAN/CSA-C22.2 No. 60950-1 Second Edition EN 60950-1 Second Edition IEC 60950-1 Second Edition NOM (obtained by partners and distributors) 47CFR Part 15 (CFR 47) Class A (FCC Part 15 Class A) AS/NZS CISPR22 Class A CISPR22 Class A EN55022 Class A ICES003 Class A VCCI Class A EN61000-3-2 EN61000-3-3 KN22 Class A KCC CNS13438 Class A EN55024 CISPR24 KN24 Reduction of Hazardous Substances (ROHS) 5	Exigido		
Garantías	La oferta deberá incluir soporte On-Site del proveedor, por todo el periodo de garantía del equipo.	Exigido		
	fabricante y ser parte del plantel estable del oferente.	Exigido		
	2 horas	Exigido		
	Las garantías, mantenimientos, entre otros, deben ser presentadas por escrito por el proveedor y al momento de la entrega definitiva de los equipos.	Exigido		
	Todos estos puntos son requerimientos mínimos 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, así como los servicios de post-venta (servicio técnico con mano de obra certificada por el fabricante, piezas originales, laboratorios autorizados por el fabricante).	Exigido		
	La oferta deberá considerar la provisión de todos aquellos materiales, accesorios, componentes o insumos que fuere necesario para la perfecta operatividad y que no esté	Exigido		

	contemplado en este pliego.			
	Garantía escrita de un (1) año como mínimo, incluyendo Soporte de atención aplicada de 8 x 5 x 4 para Hardware, Mano de Obra y Repuestos incluyendo traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del proveedor.	Exigido		
		Exigido		

<u>Debe decir</u>

1.10 Switch de Capa 3 para capa de Distribución.				
Marca:			**El bien ofertado cumple con los requerimientos**	
Modelo:				
Procedencia:				
Cantidad:	**1 (Una) Unidad**			
Características	**Requerimientos**	**Carácter**	**Si**	**No**
Descripción	Switch de 12 puertos Gigabit SFP	Exigido		
El equipo	Debe ser rackeables en infraestructuras de 19'' y deben incluir todos los accesorios necesarios para su montaje.	Exigido		
	Doble Fuente de poder 220VAC/50Hz con cable de alimentación con toma tipo americano.	Exigido		
	Deberá soportar un rango de temperatura de operación entre 0° y 40° C y un rango de Humedad no condensada de 10 a 95%.	Exigido		
	Deberá soportar un rango de temperatura de almacenamiento entre -2° y 60° C y un rango de Humedad no condensada de 10 a 95%.	Exigido		
	Deberá permitir operar en stack, el stack no deberá ser menor a 8 equipos	Exigido		
	Deberá tener un tiempo promedio entre fallas (MTBF) >= 300.000 horas.	Exigido		
Cantidad de puertos	Gigabit SFP >= 12	Exigido		
	Como mínimo 4 puertos SFP con velocidad de 1 Gbps o 2 puertos SFP de 10 Gbps (puertos independientes).	Exigido		
	Deberán proveerse con todos los módulo óptico (transceiver) de 1Gbps para Fibra Óptica MM/SM tipo SFP para la interconexión con los	Exigido		

	switches del ítem 1.11.			
Performance	Capacidad de switching >= 160 Gbps.	Exigido		
	Capacidad de forwarding >= 50 Mpps.	Exigido		
	Deberá soportar al menos 4000 VLANs.	Exigido		
	El equipo deberá soportar frames >= 9000 bytes.	Exigido		
Protocolos y Funcionalidades	IEEE 802.1s	Exigido		
	IEEE 802.1w	Exigido		
	IEEE 802.11	Opcional		
	IEEE 802.1x	Exigido		
	IEEE 802.1x-Rev	Exigido		
	IEEE 802.3ad	Exigido		
	IEEE 802.3af	Exigido		
	IEEE 802.3at	Exigido		
	RMON I and II standards	Exigido		
	SNMPv1, SNMPv2c, and SNMPv3	Exigido		
	IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and	Exigido		
	1000BASE-T ports	Exigido		
	IEEE 802.1D Spanning Tree Protocol	Exigido		
	IEEE 802.1p CoS prioritization	Exigido		
	IEEE 802.1Q VLAN	Exigido		
	IEEE 802.3 10BASE-T specification	Exigido		
	IEEE 802.3u 100BASE-TX specification	Exigido		
	IEEE 802.3ab 1000BASE-T specification	Exigido		
	IEEE 802.3z 1000BASE-X specification	Exigido		
	Soporte de seguridad del puerto mediante filtrado por dirección MAC, limitación de direcciones MAC por puerto.	Exigido		
	Soporte de limitación de tráfico mediante lista de control de acceso (ACL) por direcciones MAC origen o destino y direcciones IP origen o destino.	Exigido		
	Soporte de portmirroring por puerto o por VLAN.	Exigido		
	Deberá soportar PrivateVLANs.	Exigido		
	Implementará políticas de clasificación de tráfico y reasignación (rewrite) de prioridad basadas en protocolo IP (direcciones origen y destino, puertos TCP/UDP origen y destino).	Exigido		
	Deberá soportar IGMP y DHCP snooping.	Exigido		

	Deberá permitir el control de tormentas de broadcast, multicast y unicast en cada puerto.	Exigido		
	Deberá poder realizar la inspección de paquetes ARP.	Exigido		
	Deberá soportar sincronización horaria por medio Network TimingProtocol (NTP).	Exigido		
Administración	Se deberán proveer los bloques de información de management (MIBs) necesarios.	Exigido		
	Deberá tener soporte de AAA utilizando Radius como mínimo.	Exigido		
	Posibilidad de configurar diferentes perfiles de usuarios de administración con diferentes grados de autorización para el acceso y ejecución de las distintas tareas de gestión de la red.	Exigido		
	Soporte de Autenticación de usuarios por puerto de acuerdo al estándar IEEE 802.1x.	Exigido		
	Almacenamiento de sistema operativo y configuración en memoria Flash reescribible con capacidad de actualización por medio de protocolo FTP según RFC 959 ó TFTP.	Exigido		
	Servicio de configuración por medio de puerto de consola.	Exigido		
	Servicio de configuración por medio de consola remota Telnet según RFCs 854/855 sobre transporte TCP/IP según RFCs 793/791.	Exigido		
	Soporte de Gestión Remota segura (SNMPv3 con cifrado, SSL y/o SSH).	Exigido		
	Capacidad de RemoteMonitoring (RMON), deberá soportar al menos 4 grupos (statistics, history, alarm, events).	Exigido		
Layer 3	Enrutamiento estatico	Exigido		
	Protocolos de enrutamiento Dinamico(IPv4): RIPv1; RIPv2; RIPng; OSPF	Exigido		
	Protocolos de enrutamiento Dinamico (IPv6): OSPF	Exigido		
	Policy-based Routing PBR	Exigido		
	PIM-SM	Exigido		
	IPv6	Exigido		

Certificaciones	UL 60950-1 Second Edition CAN/CSA-C22.2 No. 60950-1 Second Edition EN 60950-1 Second Edition IEC 60950-1 Second Edition EN55022 Class A ICES003 Class A VCCI Class A EN61000-3-2 EN61000-3-3 Reduction of Hazardous Substances (ROHS) 5	Exigido		
Garantías	La oferta deberá incluir soporte On-Site del proveedor, por todo el periodo de garantía del equipo.	Exigido		
	fabricante y ser parte del plantel estable del oferente.	Exigido		
	2 horas	Exigido		
	Las garantías, mantenimientos, entre otros, deben ser presentadas por escrito por el proveedor y al momento de la entrega definitiva de los equipos.	Exigido		
	Todos estos puntos son requerimientos mínimos 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, así como los servicios de post-venta (servicio técnico con mano de obra certificada por el fabricante, piezas originales, laboratorios autorizados por el fabricante).	Exigido		
	La oferta deberá considerar la provisión de todos aquellos materiales, accesorios, componentes o insumos que fuere necesario para la perfecta operatividad y que no esté contemplado en este pliego.	Exigido		
	Garantía escrita de un (1) año como mínimo, incluyendo Soporte de atención aplicada de 8 x 5 x 4 para Hardware, Mano de Obra y Repuestos incluyendo traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del proveedor.	Exigido		
		Exigido		

1.11 Switch de 24 Puertos Full PoE para capa de Acceso.

Donde Dice:

1.11 Switch de 24 Puertos Full PoE para capa de Acceso.				
Marca:			**El bien ofertado cumple con los requerimientos**	
Modelo:				
Procedencia:				
Cantidad:	**6 (Seis) Unidades**			
Características	**Requerimientos**	**Carácter**	**Si**	**No**
Descripción	Switch de 24 puertos PoE	Exigido		
El equipo	Deben ser rackeables en infraestructuras de 19'' y deben incluir todos los accesorios necesarios para su montaje.	Exigido		
	Fuente de poder 220VAC/50Hz con cable de alimentación con toma tipo americano.	Exigido		
	Deberá soportar un rango de temperatura de operación entre -2° y 45° C y un rango de Humedad no condensada de 10 a 95%.	Exigido		
	Deberá soportar un rango de temperatura de almacenamiento entre -2° y 60° C y un rango de Humedad no condensada de 10 a 95%.	Exigido		
	Deberá tener un tiempo promedio entre fallas (MTBF) >= 300.000 horas.	Exigido		
	Deberá poder entregar una potencia PoE >= 370W (PoE 802.3af)	Exigido		
	Deberá permitir operar en stack, el stack no deberá ser menor a 8 equipos	Exigido		
	Ancho de Banda de Stack >= 80 Gbps	Exigido		
Cantidad de puertos	Puertos PoE auto-negociado 10/100/1000 Mbps Base-T no compartidos >= 24	Exigido		
	Gigabit SFP no compartidos >= 4	Exigido		
	Deberán proveerse 1 (un) módulo óptico(transceiver) de 1Gbps para Fibra Óptica MM/SM tipo SFP por switch.	Exigido		
	Deberá poder entregar al menos 15,4W en los 24 puerto, PoE IEEE 802.3af.	Exigido		
	Deberá poder entregar al menos 30W en almenos 12 puerto, PoE+ IEEE 802.3at.	Exigido		
Performance	Capacidad de switching >= 200 Gbps.	Exigido		
	Capacidad de forwarding >= 70 Mpps.	Exigido		

	Deberá soportar al menos 4096 VLANs.	Exigido		
	VLAN activas >= 1023	Exigido		
	El equipo deberá soportar frames de 9000 bytes como mínimo.	Exigido		
Protocolos y Funcionalidades	IEEE 802.1D	Exigido		
	IEEE 802.1s	Exigido		
	IEEE 802.1w	Exigido		
	IEEE 802.1x	Exigido		
	IEEE 802.3x	Exigido		
	IEEE 802.1p	Exigido		
	IEEE 802.1Q	Exigido		
	IEEE 802.1ab (LLDP)	Exigido		
	IEEE 802.3af	Exigido		
	IEEE 802.3at	Exigido		
	IEEE 802.3ah	Exigido		
	IEEE 802.3u 100BASE-T	Exigido		
	IEEE 802.3ab 1000BASE-T	Exigido		
	IEEE 802.3z 1000BASE-X	Exigido		
	IEEE 802.3ad Link aggregation Control Protocol (LACP)	Exigido		
	RFC 768 User Datagram Protocol (UDP)	Exigido		
	RFC 783 Trivial File Transfer Protocol (TFTP)	Exigido		
	RFC 791 Internet Protocol (IP)	Exigido		
	RFC 792 Internet Control Message Protocol (ICMP)	Exigido		
	RFC 793 Transmission Control Protocol (TCP)	Exigido		
	RFC 1112 Internet Group Management Protocol (IGMP)	Exigido		
	RFC 3376 IGMP v3	Exigido		
	RFC 1157 Simple Network Management Protocol Version 1 (SNMPv1)	Exigido		
	RFC 1901 SNMPv2c	Exigido		
	RFC 1907 Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)	Exigido		
	RFC 2474 Differentiated Services (DiffServ) Precedence	Exigido		
	Soporte de seguridad del puerto mediante filtrado por dirección MAC, limitación de direcciones MAC por puerto.	Exigido		
	Soporte de limitación de tráfico mediante lista de control de acceso (ACL) por direcciones MAC origen o destino y direcciones IP origen o	Exigido		

	destino.			
	Soporte de portmirroring por puerto o por VLAN.	Exigido		
	Deberá soportar PrivateVLANs.	Exigido		
	Implementará políticas de clasificación de tráfico y reasignación (rewrite) de prioridad basadas en protocolo IP (direcciones origen y destino, puertos TCP/UDP origen y destino).	Exigido		
	Deberá soportar IGMP y DHCP snooping.	Exigido		
	Deberá permitir el control de tormentas de broadcast, multicast y unicast en cada puerto.	Exigido		
	Deberá poder realizar la inspección de paquetes ARP.	Exigido		
	Deberá soportar sincronización horaria por medio Network TimingProtocol (NTP).	Exigido		
Administración	Se deberán proveer los bloques de información de management (MIBs) necesarios.	Exigido		
	Deberá tener soporte de AAA utilizando Radius como mínimo.	Exigido		
	Posibilidad de configurar diferentes perfiles de usuarios de administración con diferentes grados de autorización para el acceso y ejecución de las distintas tareas de gestión de la red.	Exigido		
	Soporte de Autenticación de usuarios por puerto de acuerdo al estándar IEEE 802.1x.	Exigido		
	Almacenamiento de sistema operativo y configuración en memoria Flash reescribible con capacidad de actualización por medio de protocolo FTP según RFC 959 ó TFTP.	Exigido		
	Servicio de configuración por medio de puerto de consola.	Exigido		
	Servicio de configuración y gestión remota a travez de una red TCP/IP	Exigido		
	Soporte de Gestión Remota segura (SNMPv3 con cifrado, SSL y/o SSH).	Exigido		
	Capacidad de RemoteMonitoring (RMON), deberá soportar al menos 4 grupos (statistics, history, alarm, events).	Exigido		
Certificaciones y Cumplimientos	UL 60950-1 Second Edition	Exigido		
	CAN/CSA-C22.2 No. 60950-1 Second Edition	Exigido		
	EN 60950-1 Second Edition	Exigido		
	IEC 60950-1 Second Edition	Exigido		
	AS/NZS 60950-1	Exigido		

	47CFR Part 15 (CFR 47) Class A	Exigido		
	AS/NZS CISPR22 Class A	Exigido		
	CISPR22 Class A	Exigido		
	EN55022 Class A	Exigido		
	ICES003 Class A	Exigido		
	VCCI Class A	Exigido		
	EN61000-3-2	Exigido		
	EN61000-3-3	Exigido		
	KN22 Class A	Exigido		
	CNS13438 Class A	Exigido		
	EN55024	Exigido		
	CISPR24	Exigido		
	EN300386	Exigido		
	KN24	Exigido		
	Reduction of Hazardous Substances (RoHS)	Exigido		
Garantías	La oferta deberá incluir soporte On-Site del proveedor, por todo el periodo de garantía del equipo.	Exigido		
	fabricante y ser parte del plantel estable del oferente.	Exigido		
	4 horas	Exigido		
	Las garantías, mantenimientos, entre otros, deben ser presentadas por escrito por el proveedor y al momento de la entrega definitiva de los equipos.	Exigido		
	Todos estos puntos son requerimientos mínimos 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, así como los servicios de post-venta (servicio técnico con mano de obra certificada por el fabricante, piezas originales, laboratorios autorizados por el fabricante).	Exigido		
	La oferta deberá considerar la provisión de todos aquellos materiales, accesorios, componentes o insumos que fuere necesario para la perfecta operatividad y que no esté contemplado en este pliego.	Exigido		
	Garantía escrita de un (1) año como mínimo, incluyendo Soporte de atención aplicada de 8 x 5 x Siguiente día Habil para Hardware, Mano de Obra y Repuestos incluyendo traslado de los	Exigido		

	equipos de la oficina del cliente al proveedor y viceversa a cargo del proveedor.			
		Exigido		

Debe decir

1.11 Switch de 24 Puertos Full PoE para capa de Acceso.				
Marca:	Cisco		**El bien ofertado cumple con los requerimientos**	
Modelo:	WS-C2960X-24PS-L			
Procedencia:	EEUU			
Cantidad:	**6 (Seis) Unidades**			
Características	**Requerimientos**	**Carácter**	**Si**	**No**
Descripción	Switch de 24 puertos PoE	Exigido		
El equipo	Deben ser rackeables en infraestructuras de 19'' y deben incluir todos los accesorios necesarios para su montaje.	Exigido		
	Fuente de poder 220VAC/50Hz con cable de alimentación con toma tipo americano.	Exigido		
	Deberá soportar un rango de temperatura de operación entre 0° y 40° C y un rango de Humedad no condensada de 10 a 95%.	Exigido		
	Deberá soportar un rango de temperatura de almacenamiento entre -2° y 60° C y un rango de Humedad no condensada de 10 a 95%.	Exigido		
	Deberá tener un tiempo promedio entre fallas (MTBF) >= 300.000 horas.	Exigido		
	Deberá poder entregar una potencia PoE >= 370W (PoE 802.3af)	Exigido		
	Deberá permitir operar en stack, el stack no deberá ser menor a 8 equipos	Exigido		
	Ancho de Banda de Stack >= 80 Gbps	Exigido		
Cantidad de puertos	Puertos PoE auto-negociado 10/100/1000 Mbps Base-T no compartidos >= 24	Exigido		
	Gigabit SFP no compartidos >= 4	Exigido		
	Deberán proveerse 1 (un) módulo óptico(transceiver) de 1Gbps para Fibra Óptica MM/SM tipo SFP por switch.	Exigido		
	Deberá poder entregar al menos 15,4W en los 24 puerto, PoE IEEE 802.3af.	Exigido		
	Deberá poder entregar al menos 30W en almenos 12 puerto, PoE+ IEEE 802.3at.	Exigido		

Performance	Capacidad de switching >= 100 Gbps.	Exigido		
	Capacidad de forwarding >= 70 Mpps.	Exigido		
	Deberá soportar al menos 4094 VLANs.	Exigido		
	VLAN activas >= 1023	Exigido		
	El equipo deberá soportar frames de 9000 bytes como mínimo.	Exigido		
Protocolos y Funcionalidades	IEEE 802.1D	Exigido		
	IEEE 802.1s	Exigido		
	IEEE 802.1w	Exigido		
	IEEE 802.1x	Exigido		
	IEEE 802.3x	Exigido		
	IEEE 802.1p	Exigido		
	IEEE 802.1Q	Exigido		
	IEEE 802.1ab (LLDP)	Exigido		
	IEEE 802.3af	Exigido		
	IEEE 802.3at	Exigido		
	IEEE 802.3ah	Exigido		
	IEEE 802.3u 100BASE-T	Exigido		
	IEEE 802.3ab 1000BASE-T	Exigido		
	IEEE 802.3z 1000BASE-X	Exigido		
	IEEE 802.3ad Link aggregation Control Protocol (LACP)	Exigido		
	RFC 768 User Datagram Protocol (UDP)	Exigido		
	RFC 783 Trivial File Transfer Protocol (TFTP)	Exigido		
	RFC 791 Internet Protocol (IP)	Exigido		
	RFC 792 Internet Control Message Protocol (ICMP)	Exigido		
	RFC 793 Transmission Control Protocol (TCP)	Exigido		
	RFC 1112 Internet Group Management Protocol (IGMP)	Exigido		
	RFC 3376 IGMP v3	Exigido		
	RFC 1157 Simple Network Management Protocol Version 1 (SNMPv1)	Exigido		
	RFC 1901 SNMPv2c	Exigido		
	RFC 1907 Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)	Exigido		
	RFC 2474 Differentiated Services (DiffServ) Precedence	Exigido		
	Soporte de seguridad del puerto mediante filtrado por dirección MAC, limitación de direcciones MAC por puerto.	Exigido		

	Soporte de limitación de tráfico mediante lista de control de acceso (ACL) por direcciones MAC origen o destino y direcciones IP origen o destino.	Exigido		
	Soporte de portmirroring por puerto o por VLAN.	Exigido		
	Deberá soportar PrivateVLANs.	Exigido		
	Implementará políticas de clasificación de tráfico y reasignación (rewrite) de prioridad basadas en protocolo IP (direcciones origen y destino, puertos TCP/UDP origen y destino).	Exigido		
	Deberá soportar IGMP y DHCP snooping.	Exigido		
	Deberá permitir el control de tormentas de broadcast, multicast y unicast en cada puerto.	Exigido		
	Deberá poder realizar la inspección de paquetes ARP.	Exigido		
	Deberá soportar sincronización horaria por medio Network TimingProtocol (NTP).	Exigido		
Administración	Se deberán proveer los bloques de información de management (MIBs) necesarios.	Exigido		
	Deberá tener soporte de AAA utilizando Radius como mínimo.	Exigido		
	Posibilidad de configurar diferentes perfiles de usuarios de administración con diferentes grados de autorización para el acceso y ejecución de las distintas tareas de gestión de la red.	Exigido		
	Soporte de Autenticación de usuarios por puerto de acuerdo al estándar IEEE 802.1x.	Exigido		
	Almacenamiento de sistema operativo y configuración en memoria Flash reescribible con capacidad de actualización por medio de protocolo FTP según RFC 959 ó TFTP.	Exigido		
	Servicio de configuración por medio de puerto de consola.	Exigido		
	Servicio de configuración y gestión remota a travez de una red TCP/IP	Exigido		
	Soporte de Gestión Remota segura (SNMPv3 con cifrado, SSL y/o SSH).	Exigido		
	Capacidad de RemoteMonitoring (RMON), deberá soportar al menos 4 grupos (statistics, history, alarm, events).	Exigido		
Certificaciones y Cumplimientos	UL 60950-1 Second Edition	Exigido		
	CAN/CSA-C22.2 No. 60950-1 Second Edition	Exigido		
	EN 60950-1 Second Edition	Exigido		

	IEC 60950-1 Second Edition	Exigido		
	EN55022 Class A	Exigido		
	ICES003 Class A	Exigido		
	VCCI Class A	Exigido		
	EN61000-3-2	Exigido		
	EN61000-3-3	Exigido		
	Reduction of Hazardous Substances (RoHS)	Exigido		
Garantías	La oferta deberá incluir soporte On-Site del proveedor, por todo el periodo de garantía del equipo.	Exigido		
	fabricante y ser parte del plantel estable del oferente.	Exigido		
	4 horas	Exigido		
	Las garantías, mantenimientos, entre otros, deben ser presentadas por escrito por el proveedor y al momento de la entrega definitiva de los equipos.	Exigido		
	Todos estos puntos son requerimientos mínimos 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, así como los servicios de post-venta (servicio técnico con mano de obra certificada por el fabricante, piezas originales, laboratorios autorizados por el fabricante).	Exigido		
	La oferta deberá considerar la provisión de todos aquellos materiales, accesorios, componentes o insumos que fuere necesario para la perfecta operatividad y que no esté contemplado en este pliego.	Exigido		
	Garantía escrita de un (1) año como mínimo, incluyendo Soporte de atención aplicada de 8 x 5 x Siguiente día Habil para Hardware, Mano de Obra y Repuestos incluyendo traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del proveedor.	Exigido		
		Exigido		

Sección 2 Plan de Entregas

QUEDA REDACTADA DE LA SIGUIENTE MANERA:

Los
GENERAL DE MIGRACIONES, sito en Eligio Ayala Esq. Caballero, hasta 70 (Setenta
compra por parte del Proveedor, previa firma del Contrato por ambas partes.

ambas Partes, caso contrario empezara a correr el pl

ECON. REINALDO RUIZ DIAZ VERA
Coordinador S.U.O.C.
Dirección General de Migraciones