UNIVERSIDAD PEDAGOGICA NACIONAL

NIT: 899.999.124-4

VICERRECTORÍA ADMINISTRATIVA Y FINANCIERA
SUBDIRECCIÓN DE GESTIÓN DE SISTEMAS DE INFORMACIÓN

MEMORANDO

CODIGO: DGS-420

FECHA: 10 de Diciembre de 2014

PARA: **Dra. DENICE YAMILE MORA HOYOS**
Coordinadora - Grupo de Contratación

CORDIS: 2014IE13319

ASUNTO: Remisión Evaluación técnica de la invitación pública No. 20 de 2014.

En respuesta a la solicitud de evaluación de la oferta recibida dentro del marco de la invitación pública No. 20 de 2014, me permito remitir la evaluación técnica en catorce (14) folios y una (1) oferta correspondiente a:

- SOFSECURITY LTDA

Cordialmente,

GLORIA MÉNDEZ RUÍZ
Subdirectora de Gestión de Sistemas de Información

Anexo: Se anexa lo enunciado.

Proyectó y elaboró: William Rafael Crespo Arzuza

UNIVERSIDAD PEDAGOGICA NACIONAL
OFICINA JURIDICA - GRUPO DE CONTRATACION
SE RECIBE PARA REVISION
Fecha: 10/12/14 Hora: 10:32
Recibe:
El recibido de este documento NO implica su aceptación Ext: 146

VICERRECTORIA ADMINISTRATIVA Y FINANCIERA

SUBDIRECIÓN DE GESTION DE SISTEMAS DE INFORMACIÓN

ACTA DE EVALUACIÓN TÉCNICA

INVITACIÓN PÚBLICA No. 20 DE 2014

OBJETO: CONTRATAR LA ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN DE LA PLATAFORMA DE SEGURIDAD PERIMETRAL FIREWALL UTMS (UNIFIED THREAT MANAGEMENT) DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL, CON SERVICIOS DE FIREWALL, VPN, ANTIVIRUS, WEB FILTERING, CAPACIDADES ANTISPAM Y ANTIPHISHING Y FUNCIONES IPS BÁSICA, EN ALTA DISPONIBILIDAD.

A este proceso de invitación pública, se presentó una (1) empresa, a saber:

- SOFTSECURITY LTDA.

Desarrollo de la Evaluación

Aspectos evaluados desde lo técnico

2.2.1 ESPECIFICACIONES TECNICAS MINIMAS REQUERIDAS PARA EL SERVICIO DE RENOVACIÓN, INSTALACIÓN Y CONFIGURACIÓN DE LA PLATAFORMA DE SEGURIDAD PERIMETRAL

RENOVACION TECNOLOGICA DEL SISTEMA DE SEGURIDAD (UTM) UPN		
CARACTERISTICAS	DESCRIPCION	OFERTADO
CANTIDAD	Mínimo 2 equipos APPLIANCE y una consola de administración	Ofrecen dos (2) appliance y una (1) Consola SmartdashBoard para la administración.
MARCA	Indicar marca	CHECK POINT
MODELO	Indicar modelo	SG-12400
CHASIS	Metálico, Máximo dos (2) unidad de rack	CUMPLE
CARACTERISTICAS DE LA SOLUCION	Mínimo 2 puertos USB para instalación	CUMPLE
	Mínimo un puerto de consola RJ45	CUMPLE
	Mínimo un puerto 10/100/1000Base-T RJ45 de administración	CUMPLE
	Capacidad mínima dos (2) disco duro 500 GB, Hot-Swappable RAID-1	CUMPLE
	Mínimo 4 GB en Memoria RAM	CUMPLE
	Fuente de poder redundante	CUMPLE
	Mínimo 8 puertos 10/100/1000Base-T RJ45	CUMPLE
	Mínimo 4 puertos SFP 1000Base-F	CUMPLE
	Mínimo 4 puertos SFP 10GBase-F	CUMPLE
	Debe manejar IPv4 y IPv6	CUMPLE
	Mínimo debe permitir 1024 VLANs	CUMPLE
	Debe permitir interfaces virtuales	CUMPLE
	Debe tener mínimo en throughput de firewall 25 Gbps	CUMPLE
	Debe tener mínimo en throughput de IPS 12 Gbps	CUMPLE
	Debe permitir Layer 2 y Layer 3	CUMPLE
	Debe tener mínimos los siguientes certificados de seguridad: CB, UL/ c UL, CSA,TUV,NOM,CCC,IRAM,PCT/ GoST	CUMPLE
	Debe tener mínimo los siguientes certificados de emisiones: FCC, CE,VCCI,C-Tick, CCC, ANATEL,KCC	CUMPLE

	Debe tener mínimo el siguiente certificado ambiental: RoHS	CUMPLE

CARACTERISTICAS DEL FIREWALL	El gateway debe estar basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del gateway, y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.	CUMPLE
	Debe permitir crear controles de acceso a por lo menos 150 aplicaciones/servicios/protocolos predefinidos.	CUMPLE
	Debe proteger implementaciones de VoIP, soportando H323 v2/3/4 (incluido h.225 v.2/3/3 y h.254 v3/5/7), SIP. MGCP y SCCP.	CUMPLE
	Debe incluir la posibilidad de crear NATs dinámicos (N-1 o Hide) y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla.	CUMPLE
	Debe tener la opción de negar los parámetros de origen o destino, es decir que para una regla dada permite todas las conexiones de origen / destino excepto la especificada en la regla.	CUMPLE
	Debe permitir implementar reglas aplicadas a intervalos de tiempo específicos.	CUMPLE
	La comunicación entre los servidores de administración y los gateways, debe ser cifrada y autenticada.	CUMPLE
	El firewall debe soportar métodos de autenticación, por usuario, cliente y por sesión.	CUMPLE
	Debe ser capaz de autenticar sesiones de cualquier servicio.	CUMPLE
	Los siguientes esquemas de autenticación deben ser soportados por los módulos de firewall y VPN: tokens (por ejemplo, SecureID), TACACS, RADIUS, certificados digitales y dispositivos biométricos.	CUMPLE
	Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.	CUMPLE
	Debe soportar DHCP en modos server y relay.	CUMPLE
	El firewall debe poder conectarse modo transparente (bridged mode).	CUMPLE

	Debe permitir el controlar el acceso a archivos compartidos de Microsoft usando CIFS, y que el administrador decida que carpetas se pueden acceder y cuáles no.	CUMPLE
	Debe soportar Alta Disponibilidad y Balanceo de Carga de gateways con sincronización de estados, incluyendo al menos la licencia para Alta Disponibilidad	CUMPLE
	La solución debe brindar la posibilidad de poner en cuarentena a equipos que se consideren maliciosos a través de la política del Gateway de firewall.	CUMPLE
	El Gateway debe soportar redundancia a enlaces, sin la necesidad de una licencia adicional o software / Hardware de terceros.	CUMPLE
	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.	CUMPLE
	El balanceo a servidores debe soportar al menos los siguientes métodos: carga de servidor, round-robin, random, y dominio.	CUMPLE
	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.	CUMPLE
	Con la finalidad de incrementar el performance, los APPLIANCE (out of the box), para las plataformas multinucleo, deben soportar la multi replicación del kernel del firewall y permitir que corran en otros nucleos.	CUMPLE
	Debe brindar un método para bloqueo sobre mensajería instantánea de al menos las siguientes opciones: video, voz, aplicaciones compartidas, transferencia de archivos y asistencia remota.	CUMPLE

CARACTERISTICAS IPSEC VPN	Deben ser soportadas tanto un CA Interna como una CA externa provista por un tercero.	CUMPLE
	Deben ser soportados 3DES y AES-256 para las fases I y II de IKE.	CUMPLE
	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).	CUMPLE
	Debe soportar integridad de datos con md5 y sha1.	CUMPLE

	Durante el tiempo de garantía, 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)	CUMPLE
	Brindar Soporte a VPNs client-to-site basadas en IPSEC, durante el tiempo de garantía.	CUMPLE
	Debe tener la posibilidad de realizar VPNs SSL sin cliente para acceso remoto, sin necesidad de instalar un cliente.	CUMPLE
	Brindar soporte a VPNs tipo L2TP, incluyendo el soporte al cliente L2TP del Iphone, durante el tiempo de garantía,	CUMPLE
	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)	CUMPLE
	Debe incluir un método simple y central, de crear túneles permanentes entre gateways del mismo fabricante.	CUMPLE
	El administrador debe poder aplicar reglas de control de tráfico, al interior de la VPN.	CUMPLE
	Debe soportar VPNs tipo "domain based" y "route based", usando al menos BGP y OSPF (requiere el blade de advanced networking).	CUMPLE
	Debe incluir un mecanismo para mitigar el impacto a ataques de denegación de servicio DoS a IKE, haciendo diferencia entre conexiones conocidas y desconocidas.	CUMPLE
	Debe poder establecer VPNs con gateways con direcciones IP dinámicas públicas.	CUMPLE
	Brindar soporte a compresión IP para VPNs client-to-site y site-to-site, durante el tiempo de garantía.	CUMPLE
	Debe ser posible crear una única asociación de seguridad (SA) por par de redes o subredes.	CUMPLE
	Debe soportar el uso del mecanismo de inyección de rutas (RIM) para la propagación del dominio de encriptación a través de ruteo dinámico.	CUMPLE
	Con la finalidad de mejorar la conectividad y el performance de la VPN, la solución debe permitir la habilitación del modo cable (wire mode).	CUMPLE

	Debe ser posible permitir al administrador forzar que el tráfico de la VPN vaya hacia un lado en específico de la comunidad y debe permitir también tráfico encriptado desde o hacia un Gateway de VPN que no esté definido dentro de la comunidad VPN.	CUMPLE
	La solución debe contar con un mecanismo que permita seleccionar qué enlace utilizar para tráfico de VPN entrante y saliente, además de escoger la mejor ruta pará dicho tráfico.	CUMPLE
	Dicho mecanismo debe contar con al menos las siguientes configuraciones: sondeo de disponibilidad, balanceo de carga para distribuir el tráfico y selección de enlace basada en servicio	CUMPLE
	La solución debe tener la posibilidad de establecer VPN's sitio a sitio con IP dinámicas.	CUMPLE

CARACTERISTICAS IPS	El IPS integrado, debe incluir al menos los siguientes mecanismos: Attack signatures, Protocol validation y Anomaly detection y Behavior-based detection.	CUMPLE
	Los módulos de IPS Integrado y de Firewall, deben estar integrados ofreciendo de esta manera, dos líneas de defensa.	CUMPLE
	El administrador debe poder configurar la inspección, solo para el tráfico entrante.	CUMPLE
	El IPS debe proveer al menos dos políticas o perfiles predefinidos, para ser usados inmediatamente.	CUMPLE
	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.	CUMPLE
	El IPS integrado, debe incluir la habilidad de detener temporalmente la inspección y bloqueo en el gateway, para efectos de "troubleshooting". Este procedimiento debe realizarse de una forma fácil y rápida.	CUMPLE

	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)	CUMPLE
	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	CUMPLE
	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.	CUMPLE
	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.	CUMPLE
	Debe poder realizar captura de paquetes para protecciones específicas.	CUMPLE
	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.	CUMPLE
	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.	CUMPLE
	Debe proteger contra ataques tipo DNS Cache Poisoning, y de esa manera prevenir a los usuarios el acceso a dominios bloqueados.	CUMPLE
	Debe incluir protecciones para los protocolos POP3 e IMAP.	CUMPLE
	Debe soportar y proteger protocolos de VoIP (H.323, SIP, MGP y SCCP), asegurando que todos los paquetes de VoIP son estructuralmente válidos.	CUMPLE
	Debe detectar y bloquear aplicaciones que realizan control remoto, incluyendo aquellas que son capaces de hacer tunneling en tráfico HTTP.	CUMPLE
	El administrador debe poder permitir chat MSN Messenger pero bloquear el Video.	CUMPLE

	Debe incluir protección a vulnerabilidades Citrix ICA e implementar cumplimientos de protocolo.	CUMPLE
	Debe permitir bloquear tráfico entrante, saliente o ambos correspondientes a determinados países, sin necesidad de actualizar manualmente los rangos IP correspondientes a cada país.	CUMPLE
CARACTERISTICAS IDENTIDAD DE USUARIOS	La identidad de los usuarios se debe poder compartir entre Gateways, de esta forma el usuario sólo se autenticará en un Gateway, y podrá navegar en otros Gateways del mismo fabircante ofertado con esta identidad.	CUMPLE
	La solución debe proteger a los usuarios de ataques IP-spoofing etiquetando los paquetes cuando estos provengan de los usuarios autentificados.	CUMPLE
	La solución debe proveer una forma de autentificación para los usuarios que no utilicen plataforma de Windows, además de dispositivos móviles.	CUMPLE
	La solución tiene que proveer configuración de acceso basado en tiempo para que los usuarios puedan entrar a los recursos de la red.	CUMPLE
	El Gateway de Identity awareness debe ser capaz de distinguir entre cuentas de servidores de aplicación y cuentas de usuario.	CUMPLE
	Debe soportar el uso de expresiones regulares para la exclusión de usuarios.	CUMPLE
	La solución debe proveer tres métodos para obtener las identidades de los usuarios: Sin agente haciendo búsquedas al directorio activo o agente instalado en los equipos del usuario final o portal cautivo. Estos tres métodos no deben ser mutuamente excluyentes.	CUMPLE
	Cuando se detecte que los usuarios no se han autentificado, la solución tiene que redireccionarlos a un portal cautivo, a través del protocolo http.	CUMPLE
	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.	CUMPLE

	La solución debe tener un método de integración con el directorio activo sin usar las credenciales del administrador.	CUMPLE
	La solución debe soportar el uso del protocolo WMI (windows managemwnt instrumentation).	CUMPLE
	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.	CUMPLE
	Los agentes instalados en los equipos, deben proveer un sistema de autentificación SSO (single-sing-on).	CUMPLE
	Debe soportar al menos los siguientes métodos de autentificación: nombre de usuario y contrase, que podrá ser configurado en la base de datos interna del Gateway o en un servidor de LDAP y servidor de RADIUS.	CUMPLE
	Para una implementación sencilla, la solución debe proveer un wizard de configuración.	CUMPLE
	Todas las características de la solución deben estar integradas en un solo Gateway sin la necesidad de usar diferentes servidores.	CUMPLE
	En el Gateway de Identity awareness debe dar al administrador la posibilidad de elegir desde que zona de la red (Interna, externa o DMZ) pueden tener acceso los usuarios con agente instalado o portal cautivo.	CUMPLE
	La solución debe retener la identidad de los usuarios aun cuando estos cambien la dirección IP.	CUMPLE
	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.	CUMPLE
	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.	CUMPLE
	El Gateway de Identity Awareness debe poder implementarse en modo puente o en modo ruteo.	CUMPLE
	La solución debe ser capaz de restringir el acceso a la red cuando no se acepte el acuerdo de usuarios (Agreement).	CUMPLE

	Los agentes deben tener la capacidad de descubrir con cuál Gateway de Identity awareness deben conectarse al menos por los siguientes métodos: - Configuración de servidor basada en nombre de archivo: utiliza los datos del Gateway desde donde fue descargado el agente. - Descubrimiento de servidores basada en registros de DNS: Configurar las direcciones del Gateway de identity awareness en el servidor de DNS. - Configuración remota de registro: Configurando una política de grupo que permita modificar los valores del Gateway en el editor de registro de Windows. - Pre-empaquetado: creando una versión pre-empaquetada que tenga los datos del Gateway.	CUMPLE
	Los agentes deben reportar su estado en un intervalo de tiempo configurable.	CUMPLE
	Debe ser posible solicitar a los usuarios la re autentificación después de un intervalo de tiempo.	CUMPLE
	Debe ser posible configurar al Gateway de identity awarenes en un bosque de dominio	CUMPLE

CARACTERISTICAS CONTROL DE APLICACIONES	La solución debe integrar reglas de filtrado de URL y control aplicaciones en la misma licencia.	CUMPLE
	La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web.	CUMPLE
	La solución debe proveer una librería de aplicaciones que incluya aplicaciones Web 2.0, Widgets y base de datos de URL.	CUMPLE
	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.	CUMPLE
	La administración debe centralizar las políticas de seguridad del control de aplicaciones y filtrado URL en la misma consola.	CUMPLE
	Debe tener la capacidad de hacer un análisis avanzado que incluya, tráfico por sitios, graficas, reporteo, estadísticas, etc.	CUMPLE

	Tiene que crear políticas granulares para sitios Web, Web 2.0 y control de aplicaciones	CUMPLE
	Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales y grupos de usuarios.	CUMPLE
	Debe inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL	CUMPLE
	Debe contar con un repositorio en línea para identificar URLs y aplicaciones no clasificadas	CUMPLE
	Debe tener un servicio de clasificación basando en la nube que permita categorizar dinámicamente el tráfico Web.	CUMPLE
	Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.	CUMPLE
	Debe ser posible integrar la solución con Directorio Activo y 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	CUMPLE
	Debe ser posible usar al menos las siguientes cuatro acciones en una regal de control de aplicaciones y filtrado de URL: bloquear, monitorear, informar al usuario y preguntar al usuario	CUMPLE
	Debe ser posible crear, por regla, un portal cautivo para interacción con el usuario.	CUMPLE
	Se debe de poder crear un portal cautivo diferente cuando la conexión sea de dispositivos móviles.	CUMPLE
	Para todas las acciones que necesiten interacción con el usuario, la solución debe tener la opción de trabajar en "Modo de aprendizaje", esto quiere decir que la solución aprenderá la acción del usuario en la primera interacción y la recordará para los siguientes eventos similares.	CUMPLE
	La solución debe ser una arquitectura cliente-servidor con la posibilidad de instalar la consola de administración en cualquier servidor de Windows u open Server, el cual será responsable de lanzar las políticas para los módulos de control de aplicaciones y filtrado URL.	CUMPLE

	En cualquier escenario de instalación, debe ser posible tener HA para almacenamiento de registros, esto quiere decir que si el servidor de registros primario falla, los gateways de control de aplicaciones y filtrado de URL usarán un servidor de registros secundario.	CUMPLE
	En cualquier escenario de instalación, debe ser posible tener HA para almacenamiento de logs, esto quiere decir que si el servidor de logs primario falla, los gateways de control de aplicaciones y filtrado de URL usarán un servidor de registros secundario.	CUMPLE
	La solución debe proveer una arquitectura escalable y flexible, dando la posibilidad de dividir el repositorio de alertas, los Gateways de control de aplicaciones y filtrado URL y la administración del sistema.	CUMPLE
	De ser necesario, los servidores de administración y de logs, pueden ser instalados en el mismo Hardware y posteriormente ser separados, dando la posibilidad de crecer dentro de la red.	CUMPLE
	El proceso de comunicación entre los componentes de toda la solución, debe ser encriptado en todos sus puntos, durante la transmisión de información.	CUMPLE
	La solución debe soportar la integración con la infraestructura de red y seguridad existente, como Firewalls y routers.	CUMPLE
	Para escalabilidad y flexibilidad, los Gateways de control de aplicaciones, filtrado URL y administración deben tener la posibilidad de instalarse en servidores comunes (con requerimientos específicos dados por el fabricante)	CUMPLE
	La solución debe poder instalarse en el mismo equipo Firewall como una solución integrada UTM.	CUMPLE
	Debe ser posible instalar, en el mismo APPLIANCE o servidor, la consola de administración, el Gateway de control de aplicaciones y el Gateway de filtrado de URL.	CUMPLE

CARACTERISTICAS NETWORKING	Debe soportar al menos los siguientes protocolos de routing: BGP, OSPF, RIPv1 y RIPv2.	CUMPLE
	Debe soportar al memos los siguientes protocolos de multicast: IGMP, PIM-DM, PIM-SM	CUMPLE

	Weighted Fair Queuing (WFQ) debe soportarse para asignar un mínimo de ancho de banda a un grupo de conexiones o a una conexión específica.	CUMPLE
	Debe soportar la asignación de pesos para la definición de prioridades en la asignación de ancho de banda.	CUMPLE
	Debe poderse definir limites en el ancho de banda, para restringir aplicaciones no criticas de red.	CUMPLE
	Debe soportar Low latency queuing (LLQ) e Integrated Differentiated Services (DiffServ)	CUMPLE
	Debe incluir el balanceo entre servidores, de manera que no se necesite utilizar un balanceador externo para manejar tráfico de DMZ y LANs. Debe soportar al menos los siguientes métodos de balanceo: Server Load, Round Trip, Round Robin, Random and Domain. Debe soportar al menos 150 servicios/aplicaciones pre-definidos.	CUMPLE
	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.	CUMPLE
CARACTERISTICAS ACELERACION Y CLUSTERING	El hardware debe estar basado en una arquitectura abierta, usando procesadores Intel o AMD para mantener la flexibilidad y adaptarse a nuevas amenazas, sin disminuir el desempeño.	CUMPLE
	Debe incluir balanceo de carga de gateways con sincronización de estados, sin necesidad de usar un balanceador externo, para al menos 5 gateways en un solo cluster.	CUMPLE
	Debe proveer un mecanismo que permita la mejor utilización de todos los procesadores con que cuente el hardware.	CUMPLE
CARACTERISTICAS DE ADMINISTRACION	Debe soportar diferentes perfiles de administrador, incluyendo al menos los siguientes: read/write y read/only.	CUMPLE
	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.	CUMPLE
	Debe incluir una entidad CA (Certificate Authority) interna X.509, que genere certificados a los gateways y a los usuarios para una fácil autenticación en las VPNs.	CUMPLE

	Debe incluir la habilidad de confiar en CAs externas, que soporten standards PKCS#12, CAPI o Entrust.	CUMPLE
	Debe incluir la opción de crear diferentes perfiles de IPS, que pueden ser aplicados a diferentes gateways.	CUMPLE
	Debe incluir la opción de automáticamente habilitar nuevas protecciones de IPS basadas en: Severidad de la amenaza, Impacto de Desempeño y Nivel de Confidencia.	CUMPLE
	Debe incluir una manera de marcar las protecciones de IPS para un futuro seguimiento o análisis.	CUMPLE
	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.	CUMPLE
	Debe incluir la opción de segmentar las reglas de acceso, usando etiquetas o títulos de sección y de esa forma organizar mejor la política.	CUMPLE
	Debe incluir la opción de guardar la política completa o una específica parte de la política.	CUMPLE
	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.	CUMPLE
	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.	CUMPLE
	Debe incluir la habilidad de distribuir y aplicar centralizadamente nuevas versiones de software para los gateways.	CUMPLE
	Debe incluir una herramienta que administre centralizadamente la licencia de todos los gateways, controlados desde la estación de administración.	CUMPLE
CARACTERISTICAS DE ESTADO Y REGISTRO (LOG)	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.	CUMPLE
	Los logs deben poder estar en el servidor de administración o en un servidor separado.	CUMPLE

	Debe poderse diferenciar entre logs de usuarios regulares y los logs propios de la administración.	CUMPLE
	Los logs deben ser transferidos con seguridad entre los gateways y la el servidor de administración o el servidor de logs. De la misma manera desde y hacia la consola de administración del servidor.	CUMPLE
	Debe poderse exportar los logs en formato de base de datos.	CUMPLE
	Debe poderse realizar un cambio automático de logs, basados en programaciones de tiempo o del tamaño del archivo.	CUMPLE
	Debe permitir adicionar excepciones a las protecciones de IPS desde el log.	CUMPLE
REPORTES	Generación de Reportes personalizables.	CUMPLE
	Se debe gestionar eventos y vulnerabilidades de seguridad sobre la plataforma de información tecnológica.	CUMPLE

FUNCIONALIDADES DE LA SOLUCION	La solución ofertada debe soportar las funcionalidades a continuación descritas: - Realizar la instalación, configuración, pruebas y puesta en funcionamiento de la solución tipo APPLIANCE (hardware y software) requerida por la UNIVERSIDAD PEDAGOGOCA NACIONAL. - Monitoreo diario de su funcionalidad, verificación diaria de los dispositivos, para que estén funcionando correctamente, tanto a nivel físico como lógico. - Realizar las nuevas configuraciones. Después de realizar el proceso de implementación, se acordará el proceso de administración de cambios para la creación de nuevas reglas o configuraciones, previa aprobación de la UNIVERSIDAD PEDAGOGOCA NACIONAL. - Realizar la Actualización de nuevas versiones de software y parches, previa autorización de la UNIVERSIDAD PEDAGOGOCA NACIONAL y por medio del proceso de control de cambios. - Realizar backup de las configuraciones antes y después de cada cambio, con el fin de garantizar una respuesta oportuna en caso de alguna eventualidad que requiera la reconfiguración de los equipos utilizados en la solución. - Informes Bimensuales con el resultado de la administración y monitoreo de la plataforma administrada, en cuanto a alarmas, eventos y logs.	CUMPLE
	Monitoreo diario de su funcionalidad, verificación diaria de los dispositivos, para que estén funcionando correctamente, tanto a nivel físico como lógico.	CUMPLE
	Debe poder asociar cada IP correspondiente a usuarios internos con su correspondiente nombre de usuario y nombre de máquina, tomando esa información del Active Directory, sin necesidad de instalar ninguna aplicación en el Domain Controller ni en las PCs de los usuarios.	CUMPLE
	Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense.	CUMPLE
	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	CUMPLE

	Debe incluir la opción de que dinámicamente bloquee una conexión activa desde la interfaz gráfica, sin la requerir modificación de las reglas establecidas en el rule base.	CUMPLE
	Debe permitir integración con el Directorio Activo	CUMPLE
	El APPLIANCE debe tener una herramienta de diagnóstico de Hardware, ejecutable desde el LCD sin la necesidad de uso de cables o consolas, que permita al menos las siguientes opciones: identificar fallas en el APPLIANCE, cargar las diferentes imágenes precargadas de fábrica, etc.	CUMPLE
	Debe contar con una interfaz de administración que permita las siguientes acciones sobre el equipo: a. Encender la caja de manera remota. b. Acceso remoto a través de consola virtual KVM. c. Instalación remota utilizando una media virtual. d. Para solución de problemas debe permitir el conocer el último estado de la caja antes de reiniciarse. e. Monitoreo de estado a través del protocolo SNMP	CUMPLE
	Debe ofrecer administración centralizada de políticas, almacenando logs y monitoreando al menos dos. Proporcionando la habilidad de distribuir centralizadamente las políticas.	CUMPLE
COMPROMISOS CONTRATISTAS	Realizar la instalación, configuración, pruebas, certificación y puesta en funcionamiento de la solución tipo APPLIANCE (hardware y software) requerida por la UNIVERSIDAD PEDAGOGOCA NACIONAL.	CUMPLE
	Realizar las nuevas configuraciones. Después de realizar el proceso de instalación e implementación, se acordará el proceso de administración de cambios para la creación de nuevas reglas o configuraciones, previa aprobación de la UNIVERSIDAD PEDAGOGOCA NACIONAL.	CUMPLE
	Realizar la Actualización de nuevas versiones de software y parches, previa autorización de la UNIVERSIDAD PEDAGOGOCA NACIONAL y por medio del proceso de control de cambios.	CUMPLE
	Realizar backup de las configuraciones antes y después de cada cambio, con el fin de garantizar una respuesta oportuna en caso de alguna eventualidad que requiera la reconfiguración de los equipos utilizados en la solución.	CUMPLE

	Informe a la finalización del contrato con el resultado de la administración y monitoreo de la plataforma instalada, en cuanto a alarmas, eventos, políticas implementadas y logs.	CUMPLE
	Aplicar las mejores prácticas y aseguramiento de los servicios	CUMPLE
	La solución ofrecida debe quedar instalada y configurada en alta disponibilidad (dos equipos de igual modelo y características) que permitan tener un respaldo en línea	CUMPLE
	El proponente deberá entregar la documentación técnica detallada de toda la implementación realizada	CUMPLE
	Se debe brindar un servicio dentro de la solución ofertada para que identifique amenazas de redes bot, patrones de comunicación de ataques botnet y de forma sencilla se integre con reportes y administración unificada para el firewall de seguridad perimetral. Proveer análisis de tipo forense para analizar eventos. Investigar infecciones por malware detallando tipo de daño y usuario o maquina comprometida. Investigar infecciones por malware detallando tipo de daño y usuario o maquina comprometida.	CUMPLE
	El proponente deberá entregar un informe técnico mensual durante el tiempo de la garantía ofrecida y/o dar soporte sobre el desempeño de la plataforma instalada.	CUMPLE
FASES DEL PROYECTO	Planeación del proyecto, Cronograma, protocolo de comunicación y asignación de Niveles de Servicios (ANS),	CUMPLE
	Análisis de la plataforma tecnológica actual: hardware, software, red de comunicaciones, condiciones ambientales y sistemas de información.	CUMPLE
	Diseño de la arquitectura computacional con base en el análisis: hardware, software, red de comunicaciones, tendidos, arquitectura, almacenamiento y respaldo.	CUMPLE
	Implantación de la arquitectura computacional.	CUMPLE
	Transferencia de conocimiento en los productos ofrecidos.	CUMPLE
	Pruebas de funcionalidad.	CUMPLE
	Puesta en marcha de la solución.	CUMPLE
	Entrega formal del proyecto.	CUMPLE

	Administración, Seguimiento, monitoreo y garantía del proyecto.	CUMPLE
VISITAS DE MANTENIMIENTO, SOPORTE POR GARANTIA	Para la prestación del servicio se requiere que el proponente cuente con un esquema de mesa de ayuda, donde se puedan generar los reportes de incidentes frente a la prestación del servicio de soporte por garantía.	CUMPLE
	Atender oportunamente las solicitudes de soporte por garantía ante fallas de los equipos de la solución suministradas, de acuerdo a los siguientes niveles de servicio (SLAs). - Falla Crítica: Respuesta en máximo una (1) hora hábil. Afectación de más del 40% de la operación de la UNIVERSIDAD PEDAGOGOCA NACIONAL. - Falla Media: Respuesta en máximo dos (2) horas hábiles. Afectación entre el 15% y el 39% de la operación de la UNIVERSIDAD PEDAGOGOCA NACIONAL. - Falla Menor: Respuesta en máximo cuatro (4) horas hábiles. Afectación entre el 0% y el 14% de la operación de UNIVERSIDAD PEDAGOGOCA NACIONAL.	CUMPLE
	Brindar constantemente recomendaciones que permitan obtener un mejor nivel de mitigación de riesgos derivados del uso de la tecnología.	CUMPLE
	Se debe brindar un componente de alarma para la detección automática de eventos de seguridad, que faciliten la gestión de los mismos sobre la infraestructura tecnológica.	CUMPLE
	En caso de no ser posible la solución remota o telefónica, se requiere prestación del servicio en sitio, de acuerdo a los niveles de servicio pactados. Se requiere servicio de análisis de log permanente y generación de reportes de manera periódica.	CUMPLE
	Durante el tiempo de garantía, el contratista deberá realizar una visita mensual para validar el correcto funcionamiento de la solución instalada. El proponente debe realizar al menos dos (2) mantenimientos preventivos anuales a la solución.	CUMPLE
	Dentro del servicio de Seguridad debe realizar un análisis de vulnerabilidades con una máquina de propósito definido (tipo APPLIANCE), realizado por Ingeniero certificado por el fabricante del mismo y un auditor certificado en procesos de seguridad informática (Se debe adjuntar certificado(s) como expertos en el tema en mención, adjuntar una certificación del distribuidor mayorista en Colombia del fabricante donde	CUMPLE

	certifique la venta del dispositivo con el objeto de realizar demos y pruebas e indique marca, modelo y serial, adicionalmente, el oferente deberá adjuntar a la propuesta mínimo una certificación de haber realizado un análisis de vulnerabilidad de este tipo en una entidad superior a 500 usuarios y otra certificación adicional en una entidad de 3000 usuarios.	
	El oferente debe ser distribuidor autorizado del fabricante del equipo ofertado, lo cual debe acreditar, mediante presentación de certificación vigente, expedida por el representante en Colombia y dirigida al UNIVERSIDAD PEDAGOGOCA NACIONAL, donde se especifique que se encuentra autorizado para vender y soportar técnicamente las soluciones seguridad en Colombia.	CUMPLE
	La garantía de los equipos adquiridos debe ser de (3) tres años, a partir de la fecha de expedición del recibo a satisfacción por parte de la Universidad Pedagógica Nacional. El oferente deberá realizar el correspondiente soporte técnico en sitio cada vez que se solicite el servicio por fallas de funcionamiento del producto durante el tiempo de vigencia de las garantías. El soporte, durante el tiempo de garantía, deberá incluir la puesta en marcha de RELEASE y PATCHES necesarios para corregir problemas y efectuar mejoras sobre la solución y mantenerla actualizada en su última versión disponible en el mercado.	CUMPLE
	Durante la vigencia de las garantías, el proponente debe especificar claramente en su propuesta los datos mediante los cuales La UNIVERSIDAD PEDAGOGICA podrá solicitar los servicios de soporte, los cuales deberán ser como mínimo: Una dirección de correo electrónico, un sistema de tickets vía web, un teléfono fijo y por lo menos una línea de celular, ésta última disponible 7 días x 24 horas.	CUMPLE
	La garantía ofrecida por el fabricante debe cubrir todos los incidentes por fallas de hardware. Si la falla no puede ser resuelta por el fabricante dentro de las 12 horas siguientes al reporte del incidente (Interrupción del servicio altamente critica para La Universidad Pedagógica), el proponente se debe comprometer a gestionar con el fabricante, el cambio del equipo por un equipo nuevo de las mismas o mejores condiciones técnicas, y a restablecer el servicio en un periodo adicional de máximo de 24 horas.	CUMPLE

CERTIFICACIONES	El gateway debe tener la certificación Common Criteria EAL4, para al menos los siguientes componentes: Firewall, VPN, IPS, Gateway de acceso remoto para IPSEC y SSL.	CUMPLE
	El gateway debe Tener certificaciones ISO 14001 y 9000	CUMPLE

OTRAS CERTIFICACIONES Y CAPACITACIÓN DEL SISTEMA	OFRECIDO
Los proponentes deben adjuntar certificaciones vigentes del fabricante dirigidas a la Universidad que incluya los siguientes aspectos: * Autorización para vender la solución. * Indicando que son actos para el diseño en implementación de la tecnología ofrecida. * Implementación de VLAN	CUMPLE
El proponente debe haber contratado, instalado, configurado mínimo 2 soluciones del mismo fabricante de la solución ofertada y que hayan sido en alta disponibilidad (7x24). Adjuntar Certificaciones. Con la calificación, nombre, teléfono de quien firma la certificación.	CUMPLE
El proponente debe capacitar y certificar mínimo 2 personas directamente con la marca de los equipos ofrecidos y entregar los medios (Bauchers) para obtener la certificación.	CUMPLE
Deben entregar manifiestos de aduana y certificaciones del proveedor que los equipos son completamente nuevos.	CUMPLE
El proponente debe entregar en físico y digital diseño y planos de la solución	CUMPLE
El proponente debe tener mínimo dos (2) Ingenieros expertos en la solución adquirida. Certificados por el fabricante Un ingeniero como Certified Security Administrator CCSA y el segundo ingeniero como Certified Security Expert CCSE.	CUMPLE
El proponente deberá aportar con su propuesta certificación firmada por la representante del mismo o del fabricante dirigida a la UNIVERSIDAD PEDAGOGICA, donde garantice el suministro y distribución de repuestos durante al menos tres (3) años a partir del recibo a satisfacción de los equipos adquiridos; así mismo que los equipos ofertados no se encuentran declarados EOL. (End Of Live)	CUMPLE
CERTIFICACIÓNES. - Un gerente para el proyecto de implementación de seguridad perimetral, el cual debe acreditar como mínimo 3 años de experiencia dirigiendo proyectos similares al contratado. Certificación laboral que acredite: Auditor de la solución Certificación de formación y aprobación como Auditor Líder ISO 27001 y Certificación de formación y aprobación y/o certificado Ethical Hacking. Entre su experiencia laboral se certifique por parte del empleador; contratante y/o representante del proveedor o fabricante.	CUMPLE

Auditor de Solución instalada e implementada	Académica	Certificación de formación y aprobación como "Auditor Lider ISO 27001.	CUMPLE
	Experiencia laboral	Entre su experiencia laboral; se certifique por parte del empleador; contratante y/o representante del proveedor o fabricante; donde conste que entre sus funciones se encontraban: Haber dirigido al menos un equipo de auditores como auditor líder en ISO 27001	CUMPLE
Ingeniero		Para el servicio de Ethical Hacking. Adjuntando el certificado CEH de la EC-COUNCIL.	CUMPLE

VERIFICACIÓN DE REQUERIMIENTOS MÍNIMOS.

El proveedor cumple con los requerimientos mínimos exigidos.

3.4.1.9 REGISTRO ÚNICO DE PROPONENTES (RUP)

EMPRESA	CODIGOS RUP
SOFTSECURITY LTDA	CUMPLE

Se verifica en la página 29

4.1. CALIFICACIÓN DE LAS OFERTAS – FACTORES: ECONOMICO, TECNICO Y APOYO A LA INDUSTRIA NACIONAL (100 PUNTOS)

Las ofertas que hayan acreditado el cumplimiento de los requisitos habilitantes, se calificarán de conformidad con los siguientes criterios:

FACTOR DE EVALUACION	PUNTAJE
ECONÓMICO	30
TÉCNICO	60
APOYO A LA INDUSTRIA NACIONAL	10
TOTAL	100

Desarrollo:

4.1.1 ECONOMICO – VALOR DE LA OFERTA – PUNTAJE (30 PUNTOS)

El valor de la propuesta fue de $ 295.800.000

El puntaje económico es de 30 puntos por ser la única oferta presentada.

4.1.2 TECNICO – PUNTAJE (60 PUNTOS)

ITEM	CRITERIO DE EVALUACION	PUNTOS
1	Características técnicas superiores a las mínimas exigidas.	20
2	Demostrar mayor experiencia de la Empresa	5
3	Valores agregados	10
4	Soporte Post-Venta	25

FORMATO DE CALIFICACION TECNICA				
Ítem	Máximo Puntaje	Requerimiento	Descripción	CALIFICACIÓN
1	15	Características técnicas superiores a las mínimas exigidas (El proponente debe relacionar, enumerar y resaltar las características superiores de los equipos ofrecidos)	• Una (1) Característica técnica superior (5 puntos.) • Tres (3) Caracteristicas técnicas superiores (10 puntos.) • Más de Tres (3) Características técnicas superiores (15 puntos.)	(El detalle se verifica en la Página 77 de la Oferta) 15 puntos
2	5	Demostrar mayor experiencia de la Empresa (El proponente debe relacionar, enumerar y enunciar el número de certificaciones presentadas. Se aplicará regla de tres directa para asignación de puntajes a partir del mayor número presentado)	• Demostrar experiencia relacionada con el objeto del mayor número de proyectos similares ejecutados adicionales a lo mínimo solicitado. (5 puntos)	El detalle se verifica en la Página 77 – 88 de la Oferta) 5 puntos
3	20	Valores agregados	• El Fabricante o Mayorista de la marca ofertada, deberá realizar un Análisis de Mapeo en 3D a la Red de la Universidad. Deberá entregar un informe del análisis realizado con las recomendaciones respectivas. El Oferente deberá entregar la	No ofrece valores agregados (0 Puntos)

			carta de compromiso en el plan de trabajo, si es adjudicado. (5 puntos.) • Realizar Capacitación certificada de sensibilización en seguridad informática al personal que designe la Universidad. El Curso no debe ser inferior a 20 horas. (5 puntos) • Ofrecer mínimo 100 horas de soporte en sitio, para la solución o prevención de problemas. (10 puntos.)	
4	1. 10 2. 10 Total Ítem 4 → 20	Soporte Post-Venta	1. Reubicación, instalación y puesta en funcionamiento de los equipos de seguridad Perimetral que la Universidad tiene actualmente. (10 puntos.) 2. Ofrecimiento de Mantenimientos Preventivos – Correctivos después de la garantía • Un (1) Mantenimiento a los equipos de la nueva solución. (5 puntos.) • Dos (2) Mantenimientos - Un (1) Mantenimiento a los equipos de la nueva solución. - Un (1) Mantenimiento a los equipos de la antigua solución. (7 puntos.) • Más de dos (2) Mantenimientos - Dos (2) Mantenimientos a los equipos de la nueva solución - Dos (2) Mantenimiento a los equipos de la antigua solución. (10 puntos.)	No ofrece Soporte Post-Venta (0 Puntos)

Total	60			

El puntaje técnico fue de 20 puntos de 60 posibles. (Se verifica en la Página 77 - 88).

4.1.3 APOYO A LA INDUSTRIA NACIONAL (10 PUNTOS)

El puntaje es de 10 puntos, porque demuestra apoyo a la Industria Nacional, porque los servicios serán prestados por personal colombiano. (Se verifica en la Página 185).

Resultado general de la Evaluación

FACTOR DE EVALUACION	PUNTAJE
ECONÓMICO	30
TÉCNICO	20
APOYO A LA INDUSTRIA NACIONAL	10
TOTAL	60

Conclusión

- La Subdirección de Gestión de sistemas de Información, después de revisar la propuesta recibida, realizar la verificación de los requisitos mínimos y la evaluación correspondiente, concluye que la empresa **SOFSECURITY LTDA** cumple desde lo económico, lo técnico y apoya la industria nacional.

Esta Evaluación Técnica se firma en Bogotá. D.C, a los 09 días del mes de Diciembre de 2014

GLORIA MÉNDEZ RUIZ
Subdirectora de Gestión de Sistemas de Información

- /Revisó, elaboró y proyectó: William R. Crespo Arzuza y Yeizon Velandia Castellanos.

Bogotá, D.C. Diciembre 5 de 2014.

Doctora
DENICE YAMILE MORA HOYOS
Coordinadora Grupo de Contratación
Universidad Pedagógica Nacional
Ciudad.-

ASUNTO: **VERIFICACIÓN DE REQUISITOS HABILITANTES JURÍDICOS. INVITACION PUBLICA No.020 DE 2014,** cuyo objeto es: **"CONTRATAR LA ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN DE LA PLATAFORMA DE SEGURIDAD PERIMETRAL FIREWALL UTMS (UNIFIED THREAD MANAGEMENT) DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL, CON SERVICIOS DE FIREWALL, VPN, ANTIVIRUS, WEB FILTERING, CAPACIDADES ANTIPHISHING Y FUNCIONES IPS BÁSICA EN ALTA DISPONIBILIDAD".**

De acuerdo con lo establecido en el inciso final del artículo 27 del Decreto 1510 de 2013, la invitación pública y el documento que contiene la designación del Comité Verificador y Evaluador para el proceso de INVITACION PUBLICA No.20 DE 2014", a continuación me permito realizar la verificación jurídica correspondiente a la **UNICA PROPUESTA** presentada por la firma **SOFT SECURITY.**

La verificación de requisitos habilitantes jurídicos consistió en la comprobación o en el examen de los diversos requisitos que habilitan a un proponente para presentar una oferta válida y hacen relación, en general, con los requisitos referentes a su capacidad jurídica para actuar, el lleno de las exigencias contenidas en la invitación Pública y en la ley para que puedan considerarse hábiles.

La mayoría de la información de este tipo, en caso de no entregarse o presentarse alguna deficiencia en la misma, es subsanable, siempre que la respuesta o entrega del documento respectivo se haga dentro del plazo establecido.

SOFT SECURITY (Única propuesta)

No.	DOCUMENTO	REQUISITO	
1	**CARTA DE PRESENTACIÓN DE LA PROPUESTA.** Debe estar suscrita por el representante legal o apoderado según sea el caso, de acuerdo con el modelo suministrado por la Universidad que hace parte de los Términos de Referencia en la pro-forma No. 01 y anexos 1 y 2.	**CUMPLE.** Folios- 2-6	
2	**CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL,** expedido por la Cámara de Comercio.	Expedición no mayor a 30 días calendario anteriores a la estipulada como fecha límite para presentar propuestas	**CUMPLE.** Folio 07
		Objeto social que le permita desarrollar la actividad, gestión u	**CUMPLE.** Folio 07 anverso

		operación que se requiere contratar.	
		Facultades del representante legal.	**CUMPLE.** Folio 8
		Vigencia de la sociedad; Igual o superior al plazo del contrato y tres (3) años más.	**CUMPLE.** Folio 07 Anverso
3	Fotocopia de la cedula de ciudadanía de la persona natural o del representante legal de la persona jurídica.	**CUMPLE**	
4	Fotocopia de la libreta militar si la persona natural o el representante legal es varón menor de 50 años.	**CUMPLE.**	
5	**CERTIFICACIÓN DE PAGO DE APORTES AL SISTEMA INTEGRAL DE SEGURIDAD SOCIAL Y PARAFISCALES** Certificación de Representante legal o revisor fiscal (según corresponda) en la que se acredite el cumplimiento de sus obligaciones con los sistemas de salud, riesgos profesionales, pensiones y aportes a las Cajas de Compensación Familiar, ICBF y SENA de sus empleados cuando a ello hubiere lugar, en el caso de personas jurídicas. El documento deberá certificar que a la fecha de presentación de su propuesta, el proponente ha realizado el pago de los aportes correspondientes a la nómina de los últimos seis (6) meses anteriores a la fecha de entrega de propuestas del presente proceso de selección	**CUMPLE.** Folio 10	
6	**AUTORIZACIÓN DEL REPRESENTANTE LEGAL Y/O APODERADO.** Cuando el representante legal de la persona jurídica, se encuentre limitado para presentar oferta o para contratar o comprometer a la sociedad, deberá anexar la AUTORIZACIÓN del órgano social correspondiente, que lo autorice para presentar la oferta, suscribir el contrato en el caso que le sea adjudicado, realizar todos los actos necesarios para el cumplimiento del objeto del presente proceso, etc.	**NO APLICA** (Folio 8)	
7	**GARANTIA DE SERIEDAD DE LA OFERTA** **(FOLIO 11)**	**BENEFICIARIO:** Universidad Pedagógica Nacional NIT: 899.999.124-4.	
		CUANTIA: Diez por ciento (10%) del presupuesto oficial. ($29.600.000).	
		VIGENCIA: Tres (3) meses, contados a partir de la fecha límite de presentación de las propuestas. (Desde 04 de Diciembre de 2014 hasta Marzo 14 de 2015)	

	IDENTIFICACIÓN TRIBUTARIA. El proponente deberá indicar su identificación tributaria e información sobre el régimen de impuestos al que pertenece, adjuntando para tal efecto, copia del Registro Único Tributario – RUT y del documento NIT correspondiente.	**CUMPLE.** Folio 21
	BOLETIN DE RESPONSABLES FISCALES (Contraloría General de la Republica) .	**CUMPLE. Folio 22**
	REGISTRO UNICO DE PROPONENTES (RUP)	**43222500. Equipo de seguridad de red.**
		43222501. Equipo de seguridad de red cortafuegos.
		43222502. Equipo de seguridad de redes VPN.
		43222503. Equipos de seguridad de evaluación de vulnerabilidad

La propuesta presentada por la firma **SOFT SECURITY, CUMPLE** jurídicamente.

Cordialmente,

ENA CONSUELO TINOCO HERRERA
Miembro Comité Asesor y Verificador
Abogada/contratista

PRESUPUESTO OFICIAL
296,000,000

UNIVERSIDAD PEDAGOGICA NACIONAL
VICERRECTORIA ADMINISTRATIVA Y FINANCIERA
EVALUACION ECONOMICA Y FINANCIERA INVITACION PUBLICA No.20 DE 2014

		DOCUMENTOS SOLICITADOS (APORTADOS EN LOS FOLIOS)								INFORMACION DE LOS ESTADOS FINANCIEROS				RESULTADO DE EVALUACION FINANCIERA					
	PROPONENTE	ESTADOS FINANCIEROS COMPARATIVOS 2013_2013	NOTAS ESTADOS FINANCIEROS DIC_2013	DICTAMEN DE LOS ESTADOS FINANCIEROS	COPIA TARJETA PROFESIONAL CONTADOR	CERTIFICADO DE ANTECEDENTES DISCIPLINARIOS CONTADOR	COPIA TARJETA PROFESIONAL REVISOR FISCAL	CERTIFICADO DE ANTECEDENTES DISCIPLINARIOS REVISOR	REGISTRO UNICO TRIBUTARIO -RUT-	ACTIVO CORRIENTE	PASIVO CORRIENTE	ACTIVO TOTAL	PASIVO TOTAL	INDICE DE LIQUIDEZ (=> 1.2 VECES)	NIVEL DE ENDEUDAMIENTO (=< AL 60%)	CAPITAL DE TRABAJO (=> AL 50%)	VALOR PROPUESTA SIN IVA	IVA	VALOR PROPUESTA CON IVA
1	SOFTSECURITY LTDA	52-55	56-67	68,69	70	72	71	73	21	$ 2,500,315,975	$ 1,339,051,106	$ 2,704,315,504	$ 1,568,787,047	1.87	58.01	$ 1,161,264,869	$ 255,000,000	$ 40,800,000	$ 295,800,000

CLAUDIA PATRICIA GOYENECHE BAEZ
Subdirectora Financiera

Elaboró: Marysol Guerra Leguizamón - Profesional Especializado - Contabilidad

3.4.3 DE CARÁCTER FINANCIERO
ASPECTOS FINANCIEROS A EVALUAR

$ 296,000,000 PRESUPUESTO OFICIAL

SOFTSECURITY LTDA							
CAPACIDAD FINANCIERA:							
	FACTOR DE VERIFICACION FINACIERA	ACTIVO CORRIENTE	PASIVO CORRIENTE	ACTIVO TOTAL	PASIVO TOTAL	INDICADORES	CUMPLE
INDICE DE LIQUIDEZ (= > 1.2 VECES)	$ 355,200,000	$ 2,500,315,975	$ 1,339,051,106			1.87	SI
NIVEL DE ENDEUDAMIENTO (=< AL 60%)	$ 177,600,000			$ 2,704,315,504	$ 1,568,787,047	58.01	SI
CAPITAL DE TRABAJO (=> AL 50%)	$ 148,000,000	$ 2,500,315,975	$ 1,339,051,106			1,161,264,869	SI

CLAUDIA PATRICIA GOYENECHE BAEZ
Subdirectora Financiera

Elaboró: Marysol Guerra Leguizamón - Profesional Especializado - Contabilidad