ADENDA N° 01
CONVOCATORIA N° 09 DE 2017

SECCION II
CONDICIONES PARTICULARES

ESPECIFICACIONES TÉCNICAS:

2.1 CARACTERISTICAS TECNICAS

SUMINISTRO DE EQUIPOS PARA ACTUALIZACIÓN DE LA SOLUCIÓN DE SEGURIDAD, INTEGRIDAD, CONFIABILIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN DEL CENTRO DE DATOS DE LA DIVISIÓN DE TECNOLOGÍAS Y COMUNICACIONES DE LA UNIVERSIDAD DEL CAUCA, los equipos que a continuación se describen y los cuales deben tener las las siguientes especificaciones:

Se requieren DOS (2) Firewall de Nueva Generación en HA y un dispositivo de recolección y almacenamiento de logs y reportes así:

1. FIREWALL DE NUEVA GENERACION (Dos Equipos)

Ítem	Requerimiento Técnico Mínimo (de obligatorio cumplimiento) FIREWALLS DE NUEVA GENERACION	Cumple
1	Generalidades. Adquisición de un sistema de seguridad informática perimetral e interna que sea del tipo Firewall de Nueva Generación y administración unificadas de amenazas (UTM), donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente documento. • Solución en alta disponibilidad, **dos equipos** físicos tipo appliance de la misma referencia funcionando en modo clúster. (A/A o A/P) • El dispositivo debe ser un equipo de propósito específico. • Basado en tecnología ASIC y que sea capaz de brindar una solución de “Complete Content Protection”. Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux. • Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC). • El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red. • El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador. • El equipo de seguridad debe soportar el uso del protocolo ICAP con el fin de poder delegar tareas a equipos terceros con el fin de liberar procesamiento del mismo. • El equipo debe entregar en tiempo real estadísticas de usuarios, aplicaciones, seguridad. Debe ser posible tener en formato de drilldown este tipo de información donde sea posible por usuario verificar que aplicaciones, sitios, categorías y amenazas de seguridad se han tenido en un tiempo mínimo de 24 horas. • El equipo deberá integrarse de forma nativa con una solución de sandbox, sin requerir desarrollos adicionales. • Se debe realizar el Proceso de Migración, instalación y configuración de esquema de seguridad actual.	

2	Rendimiento El equipo deberá cumplir con las siguientes características MINIMAS de desempeño ya activas y funcionales: • Rendimiento de Firewall 75 Gbps • Rendimiento de IPS 13 Gpps • Rendimiento Inspección SSL 10 Gbps • Rendimiento IPSec VPN 50 Gbps • Soporte de 11.500.000 sesiones concurrentes • Soporte a 9.000 usuarios VPN SSL	
3	Conectividad y especificaciones HW El equipo deberá contar con las siguientes interfaces mínimas de conexión, totalmente aprovisionadas: • 16 interfaces de 1Gbps SFP • 16 interfaces de 1Gbps RJ45 • 8 interfaces de 10Gbps SFP+ • Puerto de administración y puerto de consola. • Puerto USB. • El equipo debe contar con fuente de poder AC 100-240 V y fuente de poder redundante incluida. • El equipo de ser de tipo de montaje en rack, e incluir elementos de montaje. • El equipo debe ser certificado ICSA en Firewall, IPsec e IPS.	
4	Address Traslation • NAT y PAT • NAT estático • NAT: destino, origen • NAT, NAT64 persistente	
5	Funciones básicas de Firewall • Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. • Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall. • Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino. • Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando. • Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino. • Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo. • Capacidad de hacer traslación de direcciones estático, uno a uno, NAT, muchos a uno, PAT. • La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios. • La solución soportará políticas basadas en dispositivo. Esto Significa que podrán definirse políticas de seguridad de acuerdo al dispositivo (movil, laptop) que tenga el usuario. Esta característica no requerirá ningún tipo de licenciamiento adicional. • Debe ser posible hacer políticas basados en usuarios, grupos de usuarios y dispositivos sobre una misma política, de esta forma se lo mas granular posible en la definición de políticas. • Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos. • Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP) • Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario). • La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas. • En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID. • En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible. • El equipo deberá permitir la creación de políticas de tipo Firewall con capacidad de seleccionar campos como dirección, identificador de usuarios o identificador de dispositivos para el caso de dispositivos móviles como smartphones y tabletas. • La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. • La solución de seguridad deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada.	

	• La solución será capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente. • El dispositivo de seguridad podrá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas • La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo. • La solución podrá crear e implementar políticas de tipo Multicast y determinar el sentido de la política, así como también la habilitación del NAT dentro de cada interface del dispositivo. • El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces. • El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS. • La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o especifica. • La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos. • El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico • Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis. • La solución permitirá bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH.	
6	Conectividad y Enrutamiento • Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP. • Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs. • Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. • El soporte a políticas de ruteo deberá permitir que, ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace. • Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP • Soporte a ruteo dinámico RIPng, OSPFv3 • La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes. • Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador. • Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa. • Soporte a ruteo de multicast PIM SM y PIM DM. • La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow o Netflow. • La solución podrá habilitar políticas de ruteo en IPv6 • La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6.	
7	VPN IPSEC El equipo deberá soportar las siguientes características: • Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) • Soporte para IKEv2 y IKE Configuration Method • Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES • Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits • Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14. • Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256. • Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site. • La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN) • En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall. • Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.	
8	VPN SSL • Capacidad de realizar SSL VPNs sin necesidad de licenciamiento por usuarios. • Soporte a certificados PKI X.509 para construcción de VPNs SSL. • Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN. • Soporte de autenticación de dos factores con token, la solución debe estar en la capacidad de suplir o integrarse con tokens físicos o basados en software. • Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.	

	• Soporte de renovación de contraseñas para LDAP y RADIUS. • Soporte a asignación de aplicaciones permitidas por grupo de usuarios. • Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL. • Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning) • La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS • Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL • Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente • Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios. • Los portales personalizados deberán soportar al menos la definición de: o Widgets a mostrar o Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC o Soporte para Escritorio Virtual o Política de verificación de la estación de trabajo • La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información. • Para la configuración de cluster, en caso de caída de uno de los dispositivos, la VPN SSL que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autentificación nuevamente.	
9	Autenticación El dispositivo deberá manejar los siguiente tipos de autenticación: • Capacidad de integrarse con Servidores de Autenticación RADIUS. • Capacidad nativa de integrarse con directorios LDAP • Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”. • Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet. • Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet. • Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site). • La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios. • Deben poder definirse usuarios y grupos en un repositorio local del dispositivo. • Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo: o Longitud mínima permitida o Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc. o Expiración de contraseña. • Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.	
10	Manejo de tráfico y calidad de servicio. • Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall • Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión • Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general. • Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo • Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo	
11	Antimalware • Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP. • El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma.	

	• El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruídos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente. • Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. • El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos. • El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6. • La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso. • El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad. • El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus. • El Antivirus deberá incluír capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red. • El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger. • El antivirus deberá ser capaz de filtrar archivos por extensión. • El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo • Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas). • El Antivirus deberá poder configurarse de forma que los archivos que pasan sean totalmente capturados y analizados, permitiendo hacer análisis sobre archivos que tengan varios niveles de compresión. • El Antivirus deberá integrarse de forma nativa con el sandbox, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis. • Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. • El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6. • El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging). • La solución debe soportar la integración con soluciones de Sandbox. • La solución deberá integrarse de forma nativa con una solución de sandbox local, si la necesidad de desarrollos adicionales o licencias adicionales. • La solución debe incluir mecanismos para detectar y detener conexiones a redes Botnet y servidores C&C.	
12	Filtrado WEB • Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 47 millones de sitios web en la base de datos. • Debe poder categorizar contenido Web requerido mediante IPv6. • La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación. • 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. • La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión (modo proxy) como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación (modo flujo). • Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. Estos mensajes de remplazo deberán poder aplicarse para conexiones http y https, tanto en modo proxy como en modo flujo. • Los mensajes de remplazo deben poder ser personalizados por categoría de filtrado de contenido. • Capacidad de filtrado de scripts en páginas web (JAVA/Active X). • Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso. • La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los	

	buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing. • Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos. • Será posible exceptuar la inspección de HTTPS por categoría. • El sistema de filtrado de URLs debe tener al menos 3 métodos de inspección: 1. Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa. 2. Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad. 3. Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado. • Se debe incluir la funcionalidad de reputación basada en filtrado de URLs. • Debe contar con la capacidad de implementar el filtro de Educación de Youtube por Perfil de Filtro de Contenido para trafico HTTP, garantizando de manera centralizada, que todas las sesiones aceptadas por una política de seguridad con este perfil, van a poder acceder solamente a contenido de tipo Educativo en Youtbube, bloqueando cualquier tipo de contenido no Educativo. • La funcionalidad de reputación busca que, al acceder a páginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc) se asigne un puntaje a cada usuario o IP cada vez visita una página de esta índole. De acuerdo a esto se extrae los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar zombies dentro de la red. • El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido. • La solución debe poder aplicar distintos perfiles de navegación de acuerdo al usuario que se esté autenticando. Estos perfiles deben poder ser aplicados a usuarios o grupos de usuarios. • La solución debe estar en la capacidad de filtrar el acceso a cuentas de google, permitiendo acceso solo a cuentas corporativas de google. • El filtrado debe ser sobre tráfico http y https.	
13	Protección contra intrusos (IPS) • El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. • Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. • Capacidad de detección de más de 4000 ataques. • Capacidad de actualización automática de firmas IPS mediante tecnología de tipo “Push” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas) • El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. • El sistema de detección y prevención de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / Rate base). • Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo. • Actualización automática de firmas para el detector de intrusos • El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios. • Métodos de notificación: o Alarmas mostradas en la consola de administración del appliance. o Alertas vía correo electrónico. o Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado. o La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma “indefinida”, hasta que un administrador tome una acción al respecto. o Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. • Se debe incluir protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir: 1. Protección contra botnets: Se deben bloquear intentos de conexión a servidores de Botnets, para ello se debe contar con una lista de los servidores de Botnet más utilizado. Dicha lista debe actualizarse de forma periodica por el fabricante.	

	2. Sandboxing: La funcionalidad de Sandbox hace que el archivo sea ejecutado en un ambiente seguro para analizar su comportamiento y, a base del mismo, tomar una acción sobre el mismo.	
14	Control de Aplicaciones • Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. • La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. • La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante. • El listado de aplicaciones debe actualizarse periódicamente. • Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log, resetear conexión y hacer traffic shapping. • Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log. • Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping. • Preferentemente deben soportar mayor granularidad en las acciones. • Debe ser posible inspeccionar aplicaciones tipo Cloud como dropbox, icloud entre otras entregando información como login de usuarios y transferencia de archivos.	
15	Inspección de Contenido SSL/SSH • La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3. • Debe ser posible definir perfiles de inspección SSL donde sea posible definir los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad. • Debe ser posible definir si la inspección se realiza desde múltiples clientes conectando a servidores (es decir usuarios que navegan a servicios externos con SSL) o protegiendo un servidor interno de la entidad. • La inspección deberá realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection. • Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado. • El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS • Debe ser posible inspeccionar tráfico SSH funcionalidades como Port-Fortward o X11. • La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.	
16	**Controlador Inalámbrico (Wireless Controller)** • El dispositivo debe tener la capacidad de funcionar como Controlador de Wireless • En modo de Controlador de Wireless tendrá la capacidad de configurar múltiples puntos de acceso (Access Points: APs) reales de forma tal de que se comporten como uno solo. Cómo mínimo deberá controlar los SSID, roaming entre APs, configuraciones de cifrado, configuraciones de autenticación. • Debe soportar la funcionalidad de detección y mitigación de puntos de acceso (APs). Rogue Access Point Detection. • El controlador de Wireless tendrá la capacidad de configurar la asignación de direcciones IP mediante DHCP a las estaciones de trabajo conectadas a los APs. • Deberá tener la capacidad de monitorear las estaciones de trabajo, clientes wireless, conectadas a alguno de los APs. • La solución debe contar con la funcionalidad de WIDS (Wireless IDS), la capacidad de monitorear el trafico wireless para detectar y reportar posibles intentos de intrusión. • Debe contar con un sistema de aprovisionamiento de usuarios invitados para red wifi, que permita la creación sencilla de accesos para invitados, por medio de un portal independiente. • El equipo debe tener capacidad de que estos usuarios invitados con acceso inalámbrico, tengan la opción de colocar o no contraseña, con tiempo limitado y configurable para la expiración de la cuenta. • El controlador inalámbrico debe estar en la capacidad de balancear la carga entre los puntos de acceso (Access Points) soportando por lo menos los siguientes métodos de balanceo: Access Point Hand-off, Frequency Hand-off. • Debe contar con la capacidad de realizar Bridge SSID, permitiendo que una red inalámbrica y un segmento cableado LAN pertenezcan a la misma rubred. • El dispositivo deberá ser capaz de administrar los dispositivos wireless AP de la misma plataforma, tanto en consola CLI como a través de una interfaz grafica (GUI)	

	• El dispositivo debe tener la capacidad de controlar varios puntos de acceso de la misma plataforma de forma remota. • El dispositivo debe poder cifrar la información que se envía hacia los puntos de acceso de la misma plataforma, sobre los cuales se esté teniendo control y gestión. • El dispositivo debe permitir la administración y manejo tanto de redes cableadas como inalámbricos dentro del mismo segmento de red. • El equipo debe tener la capacidad de reconocer y monitorear diferentes tipos de dispositivos de comunicación móvil como Smartphones Androide, Blackberry y Iphone; diferentes tipos de consolas de juego como Xbox, PS2, PS3, Wii, PSP; diferentes tipos de tabletas con SO Androide o tabletas Ipad, • El equipo debe tener la capacidad de controlar el acceso a la red de los diferentes dispositivos antes mencionados a través de ACLs por MAC • El equipo deberá permitir el crear diferentes niveles de acceso a la red en función del tipo de dispositivo que se conecte, siendo estos: Smartphones, Tabletas, Laptoos, PCs (tanto en Windows como en Linux) • El equipo debe permitir la separación de redes al menos entre usuarios internos e invitados, permitiendo la colocación de reglas en función de los dispositivos móviles conectados.	
17	**Filtraje de tráfico VoIP, *Peer-to-Peer* y Mensajería instantánea** • Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP). • El dispositivo deberá técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer), soportando al menos Yahoo! Messenger, MSN Messenger, ICQ y AOL Messenger para Messenger, y BitTorrent, eDonkey, GNUTella, KaZaa, Skype y WinNY para Peer-to-peer. • En el caso de los programas para compartir archivos (peer-to-peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual. • La solución debe contar con un ALG (Application Layer Gateway) de SIP • Debe poder hacerse inspección de encabezados de SIP • Deben poder limitarse la cantidad de requerimientos SIP que se hacen por segundo. Esto debe poder definirse por cada método SIP. • La solución debe soportar SIP HNT (Hosted NAT Transversal). • La solución deberá integrar la inspección de tráfico basado en flujo utilizando un motor de IPS dentro del mismo dispositivo para escaneo de paquetes • Deberá ser capaz de hacer inspección tráifco SSH en modo proxy explicito • La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explicito con las funcionalidades de IPS, Antivirus, Filtrado Web, Control de Aplicaciones y DLP, todo en un mismo dispositivo • El dispositivo tendrá la opción para configurar sus interfaces integradas en modo Sniffer con funcionalidades de Filtrado Web, Control de Aplicaciones, Antivirus e IPS	
18	**Optimización WAN y Web Caching** • La solución deberá permitir la creación de perfiles para la aplicación de Optimización WAN e indicar bajo que protocolos se ejecutara • Deberá ser capaz de activar en modo transparente dentro de los perfiles de Optimización WAN y seleccionar un determinado grupo de usuarios para autenticación de acceso • El dispositivo deberá soportar la desfragmentación dinámica de paquetes para detectar fragmentos persistentes de distintos archivos o datos adjuntos dentro del trafico bajo protocolos desconocidos • La solución debe ser capaz de generar y aplicar perfiles de Optimización WAN para los usuarios • El dispositivo de seguridad podrá integrar contenido de inspección dentro de sus políticas de seguridad con Optimización WAN • La solución integrara dentro de cada interface la capacidad de hacer túneles de Optimización WAN • Deberá ser capaz de configurar Optimización WAN en modo Activo/Pasivo • Solución capaz de aplicar web cache a tráfico HTTP y HTTPS dentro de las políticas de seguridad incluyendo también Optimización WAN y web proxy cache • Dispositivo capaz de habilitar el almacenamiento en caché web tanto en el lado del cliente y del lado de la solución • La solución podrá recibir el tráfico HTTPS en nombre del cliente, abrirá y extraerá el contenido del tráfico cifrado para inspeccionar y almacenar en cache para el envío al usuario final • El dispositivo tendrá la opción de integrar un certificado SSL determinado para la recifrado de tráfico • La solución capaz de configurar el cache de trafico HTTP y HTTPS bajo distintos puertos a los predeterminados (80 y 443). • La solución debe ser capaz de habilitar opciones para depurar la funcionalidad de Web Cache a determinadas URL	

19	Alta Disponibilidad • La solución deberá ofertarse en alta disponibilidad • El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 • Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico. • Posibilidad de definir al menos dos interfaces para sincronía • El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red • Será posible definir interfaces de gestión independientes para cada miembro en un clúster. • Debe ser posible definir que Firewall Virtual estará activo sobre que miembro del Cluster para hacer una distribución de carga en caso se der necesario. • El equipo debe soportar hasta 4 equipos en esquema de HA.	
20	Visibilidad La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional. • Menú tipo dropdown para navegar por la información. • Visualización de las sesiones top 100 • Mostrar los origenes del tráfico o usuarios que lo generan. • Mostrar las aplicaciones y su categorización según riesgo. • Visibilidad de aplicaciones Cloud usadas por el usuario. • Visibilidad de Destinos del tráfico. • Visibilidad de los sitios web mas consultados por los usuarios. • Visibilidad de las amenazas o incidentes que han ocurriendo en la red • En la información de sources, aplicaciones, navegación debe ser posible con un doble-click filtrar la información para ser más específica la búsqueda. • Se debe ver aplicaciones, sitios, amenazas por cada usuario. • Se debe ver el tiempo de navegación por cada sitio o categoría de sitios. • De las aplicaciones Cloud que permitan compartir archivos como Dropbox debe ser posible ver que archivos fueron subidos y descargados por los usuarios. • De aplicaciones de contenido como youtube debe ser posible ver que videos fueron vistos por los usuarios.	
21	Características de Administración • Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS). • La interface gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario. • Interface basada en línea de comando (CLI) para administración de la solución. • Puerto de consola dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto. • Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH) • El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales. • Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar. • El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, http o HTTPS. • El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional. • Soporte de SNMP versión 2, 3. • Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos • Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall. • Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red. • Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión. • Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica. • Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard).	

	• Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa. • Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.	
22	Virtualización • El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains” • La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS. • Se debe incluir la licencia para al menos 8 (diez) instancias virtuales dentro de la solución a proveer, de los cuales se deberán configurar como mínimo tres acorde a los requerimientos de la entidad. • Cada instancia virtual debe poder tener un administrador independiente • La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales. • Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red • Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual • Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual. • Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual. • Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente • Se debe poder ver el consumo de CPU y memoria de cada instancia virtual.	
23	**Análisis de Seguridad y Almacenamiento de Logs en la Nube** ▪ La solución de seguridad debe contar con una solución en la nube que permita centralización de reportes, análisis de trafico, administración de configuraciones, y almacenamiento de logs sin la necesidad de software o hardware adicional para esta función. ▪ Contar con funcionalidad de Análisis de archivos sospechosos en la nube en caso que no se cuente con suficiente información en la solución de seguridad para calificar el tráfico como legitimo o ilegitimo, por medio de técnicas de Caja de Arena o Sandboxing. ▪ Almacenamiento de Logs hasta 1 Giga por equipo incluido con capacidad de crecimiento en caso de requerirse. ▪ Debe permitir administración centralizada de todos los equipos de la solución de seguridad perimetral desde una misma interfaz. ▪ Permitir Monitoreo y alertas en tiempo real. ▪ Debe contar con Reportes predefinidos y la opción de personalización, así como contar con herramientas de análisis. ▪ Debe permitir visualizar de manera sencilla que todos los equipos de seguridad perimetral gestionados cuenten con la misma versión de firmware o sistema operativo para garantizar la homogeneidad en la red.	
24	**Actualizaciones de plataforma** ▪ La solución contara con el servicio de actualización de firmas para dispositivos sobre BYOD ▪ El dispositivo tendrá la opción de conectarse a los servidores NTP de los Laboratorios de Investigación y Actualización propietarios del mismo fabricante para actualización del horario de sistema local ▪ Sera capaz de hacer consultas a los servidores DNS de los Laboratorios de Investigación y Actualización del mismo fabricante para resolución y categorización de sitios web dentro de los perfiles para Filtrado Web ▪ Tendrá la capacidad de hacer consultas a los servidores DNS de los Laboratorios de investigación y Actualización mismos del fabricante sobre reputación de direcciones IP	
25	**Prevención de Fuga de Información (DLP)** • La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial. • La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos. • Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP. • Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento, • En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción. • La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo.	

	• La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares. • Se debe proveer la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se debe considerar como mínimo las siguientes: 1. Filtrado por tipo de archivo 2. Filtrado por nombre de archivo 3. Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos. 4. Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra. 5. Watermarking: Se insertará un "sello de agua" dentro del archivo considerado como confidencial. De acuerdo a esto se analizarán los archivos en busca de este sello de agua, este se detectará incluso si el archivo sufrió cambios.	
26	*** Tamaño de licencia** El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La licencia de funcionalidades. Soporte y garantía debe **ser mínimo por 3 años.** Las licencias deben incluir las características y funcionalidades como mínimo de: Actualizaciones, virtualización, UTM, NGFW, VPN, IPsec, antivirus, filtrado web, antispam, antimalware, control de aplicaciones, detección y protección de intrusos, prevención de fuga de información. La licencia debe incluir además el soporte de fabricante vía telefónica, y vía web mediante la generación de tickets. Además debe cubrir el remplazo de hardware en caso de falla de los equipos o de alguna de sus partes, con una duración de tres (3) años.	

2. Dispositivo de recolección, consolidación de logs y administración de reportes

Ítem	Requerimiento Técnico Mínimo (de obligatorio cumplimiento) Dispositivo de recolección, consolidación de logs y administración de reportes.	Cumple
1	Generalidades. Adquisición de un sistema de reporte, análisis y almacenamiento de bitácoras, que incluye capacidades de correlación y análisis de vulnerabilidades en la red para dispositivos de Administración Unificada de Amenazas (UTM por sus siglas en inglés, Unified Threat Management). • Sistema de Almacenamiento de Logs y Reportes. • Dispositivo tipo appliance de propósito específico. • Sistema operativo propietario • Interface de administración gráfica (GUI) vía Web (HTTPS) • Interface de administración vía CLI (Línea de comando), vía ssh y consola serial • Permite la definición de dominios administrativos independientes para dividir o segmentar el control de la información recibida y almacenada por dispositivo. • Tiene la posibilidad de definir administradores para la solución, de modo que pueda segmentarse la responsabilidad de los administradores por tareas operativas • Permite la posibilidad de utilizar repositorio de datos externos (bases de datos) • Permite integrar dispositivos para que reporten, y establezcan comunicaciones seguras con dichos dispositivos • Permite asignar cuotas de espacio en disco por dispositivo, de modo que un solo dispositivo no consuma la totalidad del disco de la solución • Todas las funciones están consolidadas en el dispositivo y/o debe además ofrecer la posibilidad de ser una solución de arquitectura escalable, mediante la asignación de roles específicos o modos de operación a los componentes de la solución (recolector y/o analizador), para optimizar así el manejo y el procesamiento de los logs. • Tiene la posibilidad de enviar logs a base de datos remotas de SQL.	
2	Generación de reportes • Permite generar reportes personalizados, permite al administrador de la solución el determinar el contenido de los reportes. • El contenido de los reportes incluye los datos en formato tabular (tablas) y/o gráficas Genera reportes de: Utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos. • Genera reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente y/o por destino. • Genera reportes de las páginas y/o categorías de URL visitadas con mayor frecuencia, por fuente y/o por destino. • Permite de generar la incidencia de virus detectados/removidos a nivel red por fuente y/o por destino. • Permite generar un reporte de las actividades administrativas (entradas de administradores, cambios de	

	configuración) realizadas. • Permite personalizar los criterios bajo los cuales será obtenido el reporte, tales como fuentes, destinos, servicios, fechas y/o día de la semana. • Permite especificar el período de tiempo específico para el cual el reporte va a ser obtenido, por períodos relativos (hoy, ayer, esta semana, semana pasada, este mes, mes pasado) o bien por períodos absolutos (de la fecha día/mes/año a la fecha día/mes/año). • Permite la calendarización de reportes. • Permite generar reportes en formato PDF y DOC. • Tiene la opción de generar reportes en idioma inglés y en idioma español • Permite enviar el reporte vía correo electrónico. (pie-chart, graph-chart)	
3	Análisis forense, correlación y vulnerabilidades: • Permite hacer búsquedas por username o dirección IP, para que toda la información almacenada de dicho username o dirección IP sea mostrada en un reporte donde pueda darse seguimiento a su actividad. • Permite hacer análisis de vulnerabilidades y generar un reporte de cuáles vulnerabilidades fueron encontradas. No deberá tener límite de equipos a analizar.	
4	Almacenamiento de Contenido • Permite recibir bitácoras de los protocolos http, SMTP para poder almacenar los mensajes que han fluido en la red a través de dichos protocolos, para su posterior visualización • Los mensajes pueden ser almacenados completamente, o solo un "resumen" de la conexión. El mensaje completo exhibirá el contenido completo, mientras que el resumen solo mostrará fuente y destino de la comunicación, así como su duración. • Permite hacer búsquedas sobre los mensajes almacenados	
5	Otras Consideraciones • Almacenamiento incluido como mínimo de 10 TB • Maneja por lo menos 450 Logs por segundo. • Índice de recolección 700 logs por segundo • Conectividad 4 Interfaces GE. • El Equipo es montable en rack. • Licencia, soporte y garantía a 3 años.	

Solo se aceptan Los equipos y licenciamiento que reúnan las especificaciones técnicas requeridas en la presente invitación.

El proponente debe señalar si cumple o no cumple con las especificaciones técnicas.

PARAGRAFO. Las mejores condiciones económicas y adicionales existentes que se presenten y existan dentro del mercado, se entenderán incorporadas en forma automática al contrato.

LICENCIAMIENTO: El software que poseen los equipos, deben cumplir las disposiciones sobre el licenciamiento, es decir que la Universidad solo acepta equipos con la correspondiente licencia.

NOTA 1: El oferente deberá aportar certificación de fabricante o mayorista como distribuidor autorizado de la solución de seguridad.

Nota 2: El oferente deberá hacer entrega a la Universidad / División de Sistemas, una bolsa de diez (10) horas de soporte técnico especializado

2.2. PLAZO DE ENTREGA: El plazo de entrega de los elementos será máximo 30 días calendario a partir de la fecha de legalización del contrato, los equipos y las licencias deberán ser entregadas en la División de Tecnologías de la Información y las Comunicaciones de la Universidad del Cauca de la ciudad de Popayán y se deberá realizar el proceso de migración de la solución de seguridad actual.

2.3. SUPERVISION

La supervisión de la presente convocatoria la realizará el Servidor Universitario que para el efecto designe el Rector de la Universidad, el cual asumirá las funciones y responsabilidades conforme al Acuerdo 064 de 2008, la ley 734 de 2002.

2.4. PRESUPUESTO OFICIAL

Para la ejecución del presente proyecto, la Universidad del Cauca dispone de un presupuesto total incluido IVA de, **TRESCIENTOS DOS MILLONES DE PESOS M/CTE ($**302.000.000.oo**)** de conformidad con los Certificados de Disponibilidad Presupuestal: No. 201700575 del 21 de febrero de 2017, Emanado de la División Financiera de la Universidad del Cauca.

2.5. FORMA DE PAGO

La Universidad del Cauca pagará el valor del contrato a celebrar en pesos colombianos, así: 100% contra entrega previo recibo a satisfacción por parte del Supervisor y la factura o la cuenta de cobro respectiva.

2.6. REQUISITOS PARA PARTICIPAR EN LA CONVOCATORIA

Para participar en la presente convocatoria los ofertantes deberán cumplir los siguientes requisitos y condiciones, que de no cumplirse invalidará la propuesta para ser evaluada:

a) No hallarse incurso dentro de las inhabilidades e incompatibilidades consagradas en la Constitución Nacional, el Articulo 74 del Acuerdo 064 de 2008, o Estatuto Propio de Contratación.

b) Estar debidamente inscritos, en el registro de Proveedores y contratistas de la Universidad disponible en la página web de la universidad: disponible en la página web de la universidad: www.unicauca.edu.co – Descargas - FTP Unicauca – Diversos Documentos y Programas – Documentos Públicos - Área Comercial – Formato Proveedores.

c) Elaborar la propuesta de acuerdo con lo establecido en estos términos de referencia y anexar la documentación exigida.

d) Cuando el ofertante fuere una persona jurídica, ésta deberá acreditar que su duración no es inferior al plazo ofrecido para la ejecución del contrato y un (01) año más, contados a partir de la fecha de cierre de la presente convocatoria.

SECCIÓN IV
DOCUMENTOS DE LA PROPUESTA

4.1.1.1 DOCUMENTOS JURIDICOS

d. Inscripción en el Registro Único de Proponentes.

Conforme a lo establecido en el acuerdo 032 de 2015, los proponentes y cuando se trate de consorcio o unión temporal, cada uno de los integrantes deben estar inscritos y clasificados en el Registro único de proponentes de las Cámaras de Comercio, para ello deberá anexarse el Certificado expedido por la respectiva Cámara de Comercio en el que se debe reflejar la capacidad de contratación como proveedor y la imposición de multas y sanciones en caso de que hayan existido. La fecha de expedición no podrá ser anterior a treinta (30) días calendario a la fecha de cierre de la convocatoria, y deberá estar inscrito en los siguientes códigos:

SEGMENTO	FAMILIA	CLASE
43	22	25

Nota: Todas las anotaciones elaboradas en el RUP deberán encontrarse en firme de conformidad con lo dispuesto en el Artículo 221 del Decreto Ley 19 de 2012

SECCIÓN V
REVISIÓN DE LAS PROPUESTAS FRENTE A LAS EXIGENCIAS DE LOS TÉRMINOS DE LA CONVOCATORIA PÚBLICA

5.3.2 Factor habilitador de la capacidad financiera

Se define la capacidad financiera como una condición que se verificará para habilitar una oferta, previa a la calificación, y se efectuará teniendo en cuenta los siguientes índices

Personas jurídicas o empresas unipersonales

El valor del patrimonio líquido deberá ser mayor o igual al 100% del valor del presupuesto oficial de la convocatoria incluido IVA. La Universidad evaluara las condiciones anteriores para verificar la capacidad del proponente en el respaldo de sus obligaciones, y se encuentra en causales de disolución o liquidación obligada. En caso de consorcios o uniones temporales uno de los integrantes deber tener como mínimo el 80% de relación patrimonial mínima requerida, y la sumatoria de estos debe ser mayor o igual al 100% del presupuesto oficial incluido IVA.

- Patrimonio líquido deberá ser mayor o igual al 100% del valor del presupuesto oficial de la convocatoria incluido IVA.
- Liquidez: El índice de liquidez: mayor o igual a 1.5
- Nivel de endeudamiento: Menor o igual al 50%.

La Universidad evaluara las condiciones anteriores para verificar la capacidad del proponente en el respaldo de sus obligaciones, y se encuentra en causales de disolución o liquidación obligada. En caso de consorcios o uniones temporales uno de los integrantes deber tener

como mínimo el 80% de relación patrimonial mínima requerida, y la sumatoria de estos debe ser mayor o igual al 100% del presupuesto oficial incluido IVA.

5.3. Procedimiento para la adjudicación.

El procedimiento para la adjudicación se realizará conforme a las previsiones del Acuerdo 064 de 2008, artículo 42 parágrafo, adicionado por el Acuerdo 017 de 2011, el cual ha previsto:

La Audiencia Pública será presencial, donde los proponentes presentan sus propuestas técnicas y económicas en público, frente a los demás oferentes y a los comités técnico, financiero y jurídico de la Universidad conformados para cada audiencia.

La Audiencia Pública tendrá varias rondas para que los oferentes a través de lances mejoren su propuesta económica teniendo en cuenta la entrega del número de bienes objeto de la convocatoria por un menor valor. Las ofertas para todos los casos deben ser escritas y se desarrollarán de manera presencial.

La subasta pública durará por lo menos una hora y se adelantará por el sistema de puja dinámica, sobre la oferta de menor cuantía reservándose el nombre del proponente; y solo serán validos los lances que, observando el margen mínimo de mejora en relación con el ultimo lance valido ocurrido durante la subasta. Los lances se deben diligenciar dentro de los formatos que entregue la Universidad, se ordenaran de forma descendente, y se dará a conocer el menor precio ofertado, retirando de la puja los proponentes que no presentaron lance. Una vez superado el tiempo de la puja la Universidad hará público el resultado incluyendo la identidad de los proponentes, y en caso de empate se adjudicara al proponente que presento el menor precio al número de bienes objeto de la propuesta inicial.

Finalmente los comités evaluarán las ofertas y recomendarán al Rector, para su adjudicación.

NOTA: Únicamente podrán hacer lances de mejora de su propuesta económica en la audiencia pública de adjudicación los proponentes que sean habilitados jurídica, técnica y financieramente.

SECCIÓN VI

6.1. ADJUDICACIÓN.

La adjudicación del contrato se hará a la propuesta que ofrezca el menor en el proceso de puja dinámica, Igualmente se señalará el proponente favorecido en segundo lugar. En el evento en que no se suscriba el contrato con el proponente calificado en primer lugar dentro del plazo establecido para el efecto, si la oferta del calificado en segundo lugar, se considera igualmente favorable para la entidad, podrá suscribirse el contrato con éste.

La notificación del acto administrativo de adjudicación se hará personalmente al proponente favorecido. A los no favorecidos se les comunicará, a través de la página web, dentro de los cinco (5) días calendario siguientes a su expedición.

La resolución de adjudicación es irrevocable y obliga a la Entidad y al adjudicatario. El acto de adjudicación no tendrá recursos por la vía gubernativa.

La Universidad del Cauca podrá declarar desierta la invitación a cotizar dentro del término de adjudicación del contrato, únicamente por motivos o causas que impidan la escogencia objetiva de acuerdo con los términos del artículo 6 del Acuerdo 064 de 2008 o porque sobrevengan razones de fuerza mayor o graves inconvenientes que impidan a la Universidad cumplir con las obligaciones contractuales futuras, la anterior circunstancia no derecho a los oferentes para solicitar indemnización alguna.

En todo caso no procederá declaratoria desierta de la invitación cuando solo se presente una propuesta hábil y esta pueda ser considerada favorable para la entidad, de conformidad con los criterios legales de selección objetiva.

YANETH NOGUERA RAMOS
Presidenta
Junta de Licitaciones y Contratos