UNIVERSIDAD DEL CAUCA

CONVOCATORIA PÚBLICA No. 015 de 2023

OBJETO:

RENOVACIÓN DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL, PARA GARANTIZAR LA INTEGRIDAD, CONFIABILIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN, NECESARIAS PARA LA CORRECTA PRESTACIÓN DE LOS SERVICIOS INSTITUCIONALES PARA EL CENTRO DE DATOS DE LA DIVISIÓN DE LAS TECNOLOGÍAS DE LA UNIVERSIDAD DEL CAUCA

POPAYÁN, MAYO DE 2023

CONVOCATORIA PÚBLICA No. 015 DE 2023

PROYECTO DE PLIEGO

INTRODUCCIÓN

En virtud del principio de publicidad La Universidad del Cauca se permite presentar a continuación el proyecto de pliego y sus anexos para el presente proceso, el cual contiene la información particular del proyecto y las condiciones y requisitos del proceso.

El interesado deberá leer completamente este documento y sus anexos, toda vez que, para participar en el proceso, se debe tener conocimiento de la totalidad del contenido del mismo.

El pliego de condiciones, así como cualquiera de sus anexos está a disposición del público en general en www.unicauca.edu.co/contratacion

Cualquier interesado y las veedurías ciudadanas podrán formular observaciones al proyecto de pliego de condiciones.

La Universidad del Cauca agradece todas las sugerencias u observaciones que se presenten dentro de los plazos señalados en el cronograma y que sean enviadas al correo electrónico: contratacion3@unicauca.edu.co, que estén dirigidas a lograr la claridad y precisión de las condiciones y exigencias propias del proceso.

Se adelantará la evaluación de las propuestas que se presenten con base en las reglas establecidas en el presente pliego de condiciones y en la ley.

CONSULTA DEL PLIEGO DE CONDICIONES, ATENCIÓN ADMINISTRATIVA Y RADICACIÓN DE DOCUMENTOS

La consulta del pliego de condiciones podrá hacerse a través del link www.unicauca.edu.co/contratacion

La correspondencia relativa al proceso de contratación deberá ser enviada por medio electrónico, al correo contratacion3@unicauca.edu.co ; excepto las ofertas (Sobre No.1 y Sobre No. 2) y los documentos subsanables, los cuales deberán ser radicados en la Vicerrectoría Administrativa calle 4 N° 5-30 piso 2; acorde a la cronología del proceso.

La radicación de las ofertas y documentos subsanables, si hubiera lugar a ellos, deberá hacerse en la Vicerrectoría Administrativa, calle 4 N° 5-30 piso 2. La atención al público es en horario laboral de lunes a jueves (8:00 a. m. a 12: 00 y de 2:00 p.m. a 4:00 pm) y viernes (8:00 a. m. a 12: 00 y de 2:00 p.m., a 3:00 p.m.). Siempre acorde a los límites de plazo establecidos en la cronología del proceso.

Todos los documentos deberán citar el proceso de selección al que se dirige, identificando el asunto o referencia de manera clara y precisa.

ESTUDIO TÉCNICO Y CERTIFICADO DE CONVENIENCIA Y OPORTUNIDAD.

Forman parte del presente pliego de condiciones la justificación de conveniencia y oportunidad, los estudios técnicos, el presupuesto oficial y el certificado de viabilidad administrativa, los cuales estarán disponibles en la carpeta contractual que puede ser consultada en la Vicerrectoría Administrativa de la Universidad del Cauca.

También, forma parte del pliego de condiciones, la matriz de riesgos, la cual de no presentarse observaciones por parte de los oferentes se considerará definitiva.

CAPÍTULO I

CONDICIONES GENERALES

1.1. OBJETO

RENOVACIÓN DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL, PARA GARANTIZAR LA INTEGRIDAD, CONFIABILIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN, NECESARIAS PARA LA CORRECTA PRESTACIÓN DE LOS SERVICIOS INSTITUCIONALES PARA EL CENTRO DE DATOS DE LA DIVISIÓN DE LAS TECNOLOGÍAS DE LA UNIVERSIDAD DEL CAUCA.

1.2. ESPECIFICACIONES TÉCNICAS

Las condiciones técnicas mínimas requeridas para el cumplimiento del objeto de la presente contratación se describen en el **numeral 1.11 del Capítulo I**, sin que el contratista se deba limitar a las mismas, esto es, pudiendo mejorar las condiciones a ofrecer.

El Estudio Técnico realizado por la Universidad del Cauca, será soporte fundamental y básico para la ejecución y cumplimiento del objeto de esta convocatoria.

Las propuestas deben referirse y sujetarse a todos y cada uno de los puntos contenidos en la presente convocatoria pública. La Universidad del Cauca no acepta ofertas alternativas.

NOTA 1: Con la presentación de la propuesta el oferente acepta que, en caso de resultar adjudicatario del presente proceso, cumplirá con las condiciones exigidas en pliego de condiciones y sus anexos y la propuesta aceptada por la Universidad.

1.3. MODALIDAD DE CONTRATACIÓN

La Universidad del Cauca para satisfacer la necesidad antes descrita realizará un CONTRATO DE COMPRAVENTA, de conformidad con lo establecido en el Acuerdo No. 064 de 2008.

1.4. NORMATIVIDAD APLICABLE

La presente convocatoria se realiza de conformidad con lo dispuesto en el artículo 209 de la Constitución Política, en la Ley 30 de 1992 y el Acuerdo 064 de 2008 emanado del Consejo Superior de la Universidad o Régimen propio de Contratación de la Universidad del Cauca.

En el presente documento se describen las condiciones técnicas, financieras, económicas y jurídicas, que los Proponentes interesados deben tener en cuenta para elaborar y presentar su propuesta. Con la presentación de la propuesta el proponente reconoce que estudió completamente las especificaciones que hacen parte de este pliego de condiciones; que recibió de La Universidad del Cauca, las aclaraciones necesarias a sus inquietudes y dudas; que está enterado a satisfacción en cuanto al alcance del servicio a prestar, y que ha tenido en cuenta todo lo anterior para fijar el precio y demás aspectos de su propuesta.

1.5. PRESUPUESTO OFICIAL

El presupuesto oficial para el objeto de la convocatoria incluido IVA se estima hasta la suma de **MIL CINCO MILLONES NOVECIENTOS TREINTA MIL CIENTO NOVENTA Y UN PESOS M/CTE ($1.005.930.191)**, de acuerdo al siguiente presupuesto:

PRESUPUESTO SEGURIDAD PERIMETRAL

ÍTEM	DESCRIPCIÓN	UND	CAN	VALOR UNITARIO	VALOR TOTAL
1	Dispositivo Hardware dedicado appliance con licenciamiento plus 24x7 con licenciamiento soporte y garantía, remplazo de partes y protección unificada (UTM) por 5 años mínimo. Incluyendo módulos de seguridad de filtrado web, control de aplicaciones, IPS/IDS, antivirus, sandbox en nube configuracion en HA y todas las especificaciones técnicas indicadas en el pliego.	**UN**	2	$ 300.157.200	$ 600.314.400

2	Módulos de conexión cable SPF+ Pasivo direct attach 10GB, incluidos transceiver 10GE SFP+ compatibilidad todos los sistemas con SFP+ longitud de 3 mts.	**UN**	12	$ 811.500	$ 9.738.000
3	soporte y garantia para fortimanager FMG-VMTM20008180 5 años. Gestion hasta 10 Fortinet devices/Virtual Domains, 1 GB/Day de Logs y 100 GB almacenamiento. Con soporte para todas las plataformas fortimanager-VM	**UN**	1	$ 16.839.488	$ 16.839.488
4	dispositivo hardware dedicado para analisis de log centralizado, 16 TB almacenamiento con licenciamiento de indicadores de compromiso (IOC) por 5 años. 4xGE, 2x GE SPF, garantia y soporte Por 5 años soporte dispositivos tipo fortinet. Según especificaciones técnicas del pliego	**UN**	1	$ 218.427.600	$ 218.427.600
SUBTOTAL					$ 845.319.488
IVA					$ 160.610.703
TOTAL					**$ 1.005.930.191**

Los elementos deben cumplir con las especificaciones del apartado de características técnicas mínimas descritas en el pliego de condiciones, no se aceptan equipos remanufacturados. El soporte, garantía y licenciamiento de todos los elementos hardware y software es a 5 años contados a partir del acta de recepción por parte de la universidad.

La universidad del cauca tiene implementados equipos de seguridad para diferentes segmentos incluyendo una solución de seguridad para servicios LAN y CORE que operan como Firewall de segmentación interna (ISFW), seguridad de la red Inalámbrica y sistema de correlación de eventos y sistema de reportería y estos son de referencia FORTINET. Paulatinamente se ha mejorado el esquema de seguridad en capas con estos dispositivos. Por conveniencia tecnológica y con el ánimo de tener total compatibilidad y funcionalidad con la infraestructura ya adquirida por la universidad, se requiere total compatibilidad con esta línea de marca, además de la compatibilidad e integración nativa hacia el sistema de reportaría y de eventos basado en fortianalyzer y el sistema de correlación de eventos basado en fortisiem, así como administración basada en fortimanager sistemas implementados en la institución y de esta forma garantizar un ecosistema de seguridad unificado, que permita la respuesta automática, la correcta integración, administración y reportes unificados.

El oferente seleccionado debe capacitar sobre la configuración y manejo de la solución en modalidad presencial o virtual, según especificaciones técnicas, dicha capacitación deberá ser certificada por el fabricante, igualmente deberá suministrar el servicio de soporte y acompañamiento mediante bolsa de horas para el proceso de instalación, según cronograma acordado con la Universidad.

El objeto de la convocatoria se respalda con el certificado de disponibilidad presupuestal expedido por la División de Gestión Financiera de La Universidad del Cauca, que se describe a continuación:

CDP	**VALOR**
D412-202301171 del 17 de mayo de 2023	$1.005.930.191

Parágrafo: En cumplimiento del Acuerdo 064 de 2008; la Universidad del Cauca descartará toda propuesta que se presente por encima del techo presupuestal fijado.

1.6. PROPONENTES

Podrán presentar propuestas las personas naturales, jurídicas, y asociativas como consorcio o unión temporal que cumplan con los requisitos establecidos en la presente convocatoria pública.

Las personas jurídicas nacionales deberán estar constituidas con antelación de al menos un (1) año contados a partir del cierre del presente proceso y acreditar que su duración no será inferior al plazo del contrato y un (1) año más.

1.7. ESTUDIO E INTERPRETACIÓN DE LOS TÉRMINOS DE LA CONVOCATORIA PÚBLICA

Los oferentes deben estudiar cuidadosa y detenidamente los términos de referencia, adendas, comunicaciones, especificaciones y toda la documentación existente referente al objeto del contrato, utilizando todos los medios disponibles para informarse a cabalidad de las condiciones y características de la convocatoria pública.

La información que la UNIVERSIDAD DEL CAUCA, pone a disposición de los oferentes para la preparación de la propuesta no los eximirá de la responsabilidad total de verificar, mediante investigaciones independientes, aquellas condiciones susceptibles de afectar el costo y la realización de la misma.

Los oferentes deberán realizar los estudios de costos respecto de las cantidades solicitadas por la Universidad del Cauca y para ello se recomienda realizar concienzudamente un análisis de precios unitarios que conlleven a estipular el monto de cada ítem del Anexo B “Oferta económica inicial”.

1.8. MATRIZ DE RIESGOS

La matriz en la cual se tipifican los riegos previsibles, preparada por la Entidad hace parte integrante del presente pliego de condiciones y los interesados podrán presentar sus observaciones durante el plazo establecido en la cronología del presente proceso.

La presentación de la oferta implica la aceptación por parte del proponente, de la distribución de riesgos previsibles efectuada por la Entidad en el pliego de condiciones y sus adendas.

Los proponentes deberán realizar todas las evaluaciones y estimaciones que sean necesarias para presentar su propuesta sobre la base de un examen cuidadoso de sus características, incluyendo los gastos de trasporte, stock de mercancías, proveedores, impuestos y verificaciones que consideren necesarios para formular la propuesta con base en su propia información, de manera tal que el proponente deberá tener en cuenta el cálculo de los aspectos económicos del proyecto, los cuales deben incluir todos los costos directos e indirectos que implique el cumplimiento del objeto del contrato, con todas las obligaciones y asunción de riesgos que emanan del mismo.

Si el proponente que resulte adjudicatario ha evaluado incorrectamente o no ha considerado toda la información que pueda influir en la determinación de los costos, no se eximirá de su responsabilidad por la ejecución completa de los bienes a suministrar de conformidad con el contrato, ni le dará derecho a reembolso de costos, ni a reclamaciones o reconocimientos adicionales de ninguna naturaleza.

La matriz de riesgos se relaciona en el (Anexo F).

1.9. OBLIGACIONES DEL PROPONENTE A INFORMAR ERRORES U OMISIONES

Los proponentes están en la obligación de informar a la Universidad cualquier error u omisión que encuentre en los presentes términos de la convocatoria pública y están en el derecho de pedir las aclaraciones pertinentes.

El hecho que la Universidad no observe errores u omisiones en sus documentos, no libera al contratista de su obligación de dar cumplimiento al contrato.

1.10. PRÓRROGA DE LA CONVOCATORIA Y MODIFICACIÓN DEL CRONOGRAMA

El plazo o cronograma señalado para la convocatoria, es decir, el tiempo transcurrido entre la apertura y el cierre, antes de su vencimiento podrá ser prorrogado por la Universidad del Cauca cuando lo estime conveniente, sin que dicha prórroga supere la mitad del plazo inicial.

Igualmente, la Universidad del Cauca se reserva el derecho de modificar el cronograma aquí establecido, lo cual será comunicado a los interesados previamente por medio de la página web institucional.

1.11. ESPECIFICACIONES TECNICAS

La descripción general de las especificaciones técnicas y las cantidades de los bienes por suministrar se encuentran consignadas en el presupuesto oficial de la convocatoria, y en el presente ítem, con la presentación de la propuesta, se entiende que el oferente las ha aceptado, sin que el contratista se deba limitar a las mismas, esto es, pudiendo mejorar las condiciones a ofrecer.

El proponente deberá cumplir o superar con la presentación de la oferta las condiciones técnicas mínimas que se describen a continuación. Para ello deberá diligenciar y aportar **el (Anexo E)** donde se especifica que cumple con las especificaciones técnicas con las que ejecutará el contrato en caso de resultar adjudicatario del presente proceso y se lista los componentes de la solución. En caso de ofertar especificaciones técnicas inferiores a las solicitadas o no cumplir con los requisitos estipulados en el apartado técnico del presente proceso la oferta será rechazada.

NOTA IMPORTANTE: La Universidad no autoriza la reproducción, distribución y utilización de la información relacionada con los estudios y especificaciones técnicas para fines diferentes a los de la presente convocatoria; la utilización indebida de los mismos da derecho a la Universidad para reclamar los posibles perjuicios.

El Estudio Técnico realizado por la Universidad del Cauca, será soporte fundamental y básico para la ejecución y cumplimiento del objeto de esta convocatoria.

Las propuestas deben referirse y sujetarse a todos y cada uno de los puntos contenidos en la presente convocatoria pública. La Universidad del Cauca no acepta ofertas alternativas.

NOTA 1: Con la presentación de la propuesta el oferente acepta que, en caso de resultar adjudicatario del presente proceso, cumplirá con las condiciones exigidas en pliego de condiciones y sus anexos y la propuesta aceptada por la Universidad.

Nota 2: Los proponentes deben presentar la propuesta económica inicial en medio físico, tal como se indica en el formato del (Anexo B). El costo total de la oferta debe ser redondeado a cero (0) decimales. (El oferente debe utilizar la función “REDONDEAR” de Excel con cero decimales).

ESPECIFICACIONES TÉCNICAS MÍNIMAS

El proponente deberá cumplir o superar con la presentación de la oferta las condiciones técnicas mínimas que se describen a continuación. Para ello deberá diligenciar y aportar **el (Anexo E)** donde se especifica que cumple con las especificaciones técnicas con las que ejecutará el contrato en caso de resultar adjudicatario del presente proceso y se lista los componentes de la solución. En caso de ofertar especificaciones técnicas inferiores a las solicitadas o no cumplir con los requisitos estipulados en el apartado técnico del presente proceso la oferta será rechazada.

Mediante el presente proceso se aborda la actualización de la solución de seguridad perimetral de la universidad del cauca, para garantizar la integridad, confiabilidad y disponibilidad de la información, necesarias para la prestación de los servicios publicados a internet, así como el manejo de perfiles de seguridad incluyendo antivirus, control de aplicaciones, IPS/IDS, conectividad VPN Ipsec y SSL.

CONSIDERACIONES GENERALES:

No se aceptan equipos remanufacturados. El soporte, garantía y licenciamiento de todos los elementos hardware y software es a 5 años contados a partir del acta de recepción por parte de la universidad.

La universidad del cauca tiene implementados equipos de seguridad para diferentes segmentos incluyendo una solución de seguridad para servicios LAN y CORE que operan como Firewall de segmentación interna (ISFW), seguridad de la red Inalámbrica y sistema de correlación de eventos y sistema de reportería y estos son de referencia FORTINET. Paulatinamente se ha mejorado el esquema de seguridad en capas con estos dispositivos. Por conveniencia tecnológica y con el ánimo de tener total compatibilidad y funcionalidad con la infraestructura ya adquirida por la universidad, se requiere total compatibilidad con esta línea de marca, además de la compatibilidad e integración nativa hacia el sistema de reportaría y manejo de eventos basado en fortianalyzer y el sistema de correlación

de eventos basado en fortisiem, así como administración basada en fortimanager sistemas implementados en la institución y de esta forma garantizar un ecosistema de seguridad unificado, que permita la respuesta automática, la correcta integración, administración y reportes unificados.

La Universidad del Cauca en caso de obtener precios favorables, podrá aumentar las cantidades de los elementos a suministrar hasta completar el presupuesto oficial del proceso de selección.

El oferente seleccionado debe capacitar sobre la configuración y manejo de la solución en modalidad presencial o virtual, dicha capacitación deberá ser certificada por el fabricante e incluir vouchers para examen de certificación, igualmente deberá suministrar el servicio de soporte y acompañamiento mediante bolsa de horas para el proceso de instalación, según sea necesario.

La solución debe incluir todos los elementos y accesorios necesarios para la correcta instalación y configuración de la solución de seguridad perimetral. Todos los accesorios requeridos para la instalación, configuración y puesta en funcionamiento de la solución deben ser tenidos en cuenta e incluidos en el costo de la oferta.

Esto incluye, pero no se limita a: herrajes, tornillos, cables para conexión de cualquier tipo que sean necesarios, patchcords de fibra y/o de cobre, transceivers, accesorios adicionales para su funcionamiento, etc.

LISTA DE ELEMENTOS Y CANTIDADES SOLUCIÓN DE SEGURIDAD PERIMETRAL

El oferente deberá suministrar como mínimo la totalidad de los siguientes elementos que componen la solución de seguridad perimetral de nueva generación para la universidad del Cauca:

ÍTEM	DESCRIPCIÓN	UND	CAN
1	Dispositivo Hardware dedicado appliance con licenciamiento plus 24x7 con licenciamiento soporte y garantía, remplazo de partes y protección unificada (UTM) por 5 años mínimo. Incluyendo módulos de seguridad de filtrado web, control de aplicaciones, IPS/IDS, antivirus, sandbox en nube configuración en HA y todas las especificaciones técnicas indicadas en el pliego.	**UN**	2
2	Módulos de conexión cable SPF+ Pasivo direct attach 10GB, incluidos transceiver 10GE SFP+ compatibilidad todos los sistemas con SFP+ longitud de 3 mts.	**UN**	12
3	soporte y garantía para fortimanager FMG-VMTM20008180 5 años. Gestión hasta 10 Fortinet devices/Virtual Domains, 1 GB/Day de Logs y 100 GB almacenamiento. Con soporte para todas las plataformas fortimanager-VM	**UN**	1
4	dispositivo hardware dedicado para análisis de log centralizado, 16 TB almacenamiento con licenciamiento de indicadores de compromiso (IOC) por 5 años. 4xGE, 2x GE SPF, garantía y soporte Por 5 años soporte dispositivos tipo fortinet. Según especificaciones técnicas del pliego	**UN**	1

CARACTERÍSTICAS Y REQUERIMIENTOS TÉCNICAS DE SOLUCIÓN DE SEGURIDAD PERIMETRAL

La solución de seguridad perimetral brindada por el oferente deberá cumplir o superar la totalidad de las siguientes características técnicas:

1. REQUERIMIENTOS TÉCNICOS FIREWALL DE NUEVA GENERACION (2 appliance)
Brindar dos (2) sistemas de seguridad informática perimetral tipo appliance dedicado que sea del tipo Firewall de Nueva Generación NGFW, para su disposición en HA, cada uno de los cuales debe incluir las funcionalidades que se detallan a continuación: La solución debe estar en la capacidad de soportar alta disponibilidad. ● El dispositivo debe ser un equipo de propósito específico. ● El dispositivo debe contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de trafico ● 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. ● El equipo deberá poder ser configurado en modo Gateway o en modo transparente en la red. ● El equipo debe entregar en tiempo real estadísticas de usuarios, aplicaciones, seguridad. Presentar preferiblemente 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 de 24 horas. ● La plataforma debe tener la capacidad de permitir observar el consumo de ancho de banda en tiempo real por usuario, fuente IP, aplicación y páginas web. Con el fin de detectar algún tipo de problema referente a consumos altos de ancho de banda. ● Debe tener la capacidad de generar un widget de visualización, una vez se realiza el filtro de algún tipo de búsqueda específica. ● El dispositivo appliance debe incluir fuente de poder redundante, es decir debe venir mínimo con dos fuentes de poder, para garantizar su alta disponibilidad a nivel de potencia. ● Por funcionalidades de NGFW se entiende: Firewall, control de aplicaciones, prevención de amenazas, Filtrado de Contenido, Filtrado de DNS, DoS, identificación de usuarios, VPN IPSec, VPN SSL y prevención de fuga de información; ● Debe soportar SD-WAN de forma nativa sin requerir equipos o licenciamientos adicionales.
El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales: ● Rendimiento de Firewall mínimo 139 **Gbps trafico IPv4 e IPv6.** ● Rendimiento de IPS mínimo **14 Gbps** ● Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) mínimo 11 **Gbps** ● Rendimiento Protección de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) mínimo 10 **Gbps** ● Rendimiento IPSec VPN mínimo 55 **Gbps** ● Soporte de mínimo **8** Millones sesiones concurrentes ● Soporte por lo menos 500.000 nuevas conexiones por segundo. ● Rendimiento de Inspección SSL mínimo 9 **Gbps** ● Soporte a mínimo **10000** usuarios VPN SSL concurrentes. Incluido en licenciamiento. ● Rendimiento de VPN SSL mínimo 4 **Gbps** Dichos parámetros deben poder corroborarse por medio de documentación pública directamente del Fabricante.
Conectividad El equipo deberá contar como mínimo, con las siguientes interfaces: ● **2** interfaces de **1** Gbps para administración o para HA. ● **16** interfaces de **1** Gbps RJ45 ● **8** slots de **1** Gbps SFP ● **4** slots de **10** Gbps SFP+ ● **4** slots de **25** Gbps SFP28 con posibilidad de trabajar a 10 GE SFP+

- El dispositivo appliance debe incluir fuente de poder redundante, es decir debe venir mínimo con dos fuentes de poder, para garantizar su alta disponibilidad a nivel de potencia.
  Se debe incluir todos los cables de potencia tipo C13-C14 para su conexión.

- Soportar mínimo 10 sistemas virtuales lógicos por appliance. Incluido licenciamiento
- Posibilidad de Cluster en capacidad de funcionar en un esquema Activo-Activo o Activo-Pasivo, según se requiera.

Address Translation

La plataforma deber soportar lo siguiente tipos de traducción de direcciones:

- NAT y PAT
- NAT estático
- NAT: destino, origen
- NAT, NAT64 persistente

Funciones básicas de Firewall

- Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- Debe contar con políticas de control por puerto y protocolo;
- La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.
- Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones.
- 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 deberá incurrir en ningún tipo de licenciamiento adicional que ocasiones costos adicionales para la entidad.
- Debe ser posible hacer políticas basados en usuarios, grupos de usuarios y dispositivos sobre una misma política, y ser lo más granular posible en la definición de políticas.
- Debe contar con una herramienta de búsqueda de políticas por medio del GUI (Graphical User Interface) que determine cual política procesara un flujo de datos dado (Resaltando la política que coincide), usando distintos parámetros como IP de origen, destino, servicio, protocolo, interface de fuente entre otros
- Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada
- Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén predefinidos.
- Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS, Azure, Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP, TAG etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall.
- Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface) como por GUI (Graphical User Interface).
- La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP
- El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces
- El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.
- Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis.
- Tener la capacidad de utilizar objetos de direcciones para ser utilizados en el enrutamiento con el fin de facilitar la administración y la visibilidad.
- Debe estar en la capacidad de dar estadísticas de uso por políticas como: Ancho de banda actual, Sesiones activas, Ultimo vez usada.
- La solución debe permitir la implementación sin asistencia de SD-WAN
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
- Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
- Debe permitir la visualización de los países de origen y destino en los registros de acceso;

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 mínimo 4094 Tags 802.1q
- Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
- Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
- Soporte a políticas de ruteo (policy routing)
- Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP
- Soporte a ruteo dinámico RIPng, OSPFv3.
- Soporte de ECMP (Equal Cost Multi-Path) o balanceo de enlaces WAN por medio de lo siguiente métodos: Sesiones, IP Fuente, Volumen, Spillover .
- Soporte de reglas que permitan dirigir un tráfico especifico a través de un enlace WAN, ya sea por destino, aplicación (adobe, Facebook, youtube), servicio o fuentes (IP, Usuario).
- 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.
- La solución debe contar con una herramienta de búsqueda de rutas por medio del GUI (Graphical User Interface) sobre la tabla de enrutamiento, con el fin facilitar la lectura y control de la tabla de enrutamiento usando parámetros de destino ya sea IP o FQDN.
- La Solución deberá soportar balanceado de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional y de forma nativa basado en: aplicaciones cloud, SLA, Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes)
- El SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN.
- Integrar en una única interface lógica distintos tipos de enlaces WAN físicos para permitir balanceo de los mismos.
- Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;
- Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
- Los dispositivos de protección de red deben soportar DHCP Relay;
- Los dispositivos de protección de red deben soportar DHCP Server;
- Los dispositivos de protección de red deben soportar sFlow;
- Los dispositivos de protección de red deben soportar Jumbo Frames;
- Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
- Debe soportar SD-WAN de forma nativa sin requerir equipos o licenciamientos adicionales.

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. VPNs IPSeC site-to-site y VPNs IPSec client-to-site.
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
- 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.
- Deberá tener la capacidad de crear conexiones VPNs por demanda (ADVPN), con el fin de permitir la fácil gestion de topologías Hub-Spoke y estas puedan convertirse en full-mesh al momento de comunicaciones directas entre Spokes.
- Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;

VPN SSL

- Capacidad de realizar SSL VPNs por usuarios sin incurrir en costos adicionales.
- 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, basados en software, SMS o correo
- Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.
- Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.
- La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de poner dentro del túnel SSL tráfico que no sea HTTP/HTTPS
- Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL
- Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente.
- Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.
- Los portales personalizados deberán soportar al menos la definición de:Widgets a mostrar. Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC. Soporte para Escritorio Virtual. 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. Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;

Autenticación

El dispositivo deberá manejar los siguientes tipos de autenticación:

- Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS, LDAP o TACACS+.
- 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”.
- Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID.
- Soporte autenticación de usuario a través de PKI y certificados.
- Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo

Identificación de Usuarios

- Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
- Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, entre otros.
- Debe tener integración con RADIUS para identificar a los usuarios y grupos que permitan granularidad de las políticas de control basados en usuarios y grupos de usuarios;
- Debe tener integración LDAP para la identificación de los usuarios y grupos que permitan granularidad en la política de control basados en usuarios y grupos de usuarios
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
- Debe permitir la integración con Azure AD por medio de SAML

Manejo de tráfico y calidad de servicio.

- Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente
- Debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming

- 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 y categoría URL de las mismas para la regla en general.
- Capacidad de poder definir ancho de banda garantizado en Kilobits por segundo
- Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo.
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen, dirección destino, por usuario y grupo, por aplicaciones incluyendo pero no limitando Skyope, Youtube, P2P.
- En QoS debe permitir la definición de colas de prioridad;
- Soportar marcación de paquetes DiffServ, incluso por aplicación;
- Soportar la modificación de los valores de DSCP para Diffserv;
- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
- Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

Prevención de Fuga de Información

- Deberá contar con un módulo de prevención de Fuga de información o DLP de Red, embebido en la solución, sin requerir ningún licenciamiento o dispositivo adicional.
- Debe Permitir la creación de filtros para archivos y datos predefinidos;
- Los archivos deben ser identificados por tamaño y tipo;
- Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;

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.MAPI
- 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.
- Debe soportar la inspección de archivos comprimidos como los son: GZIP, RAR, LZH, IHA, CAB, ARJ, ZIP entre otros con el fin de proteger contra estas técnicas de evasión.
- 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 una solución sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis.
- Proporcionar protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube).
- Antivirus en tiempo real, integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
- El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.
- La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso.
- El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).
- La solución debe incluir mecanismos para detectar y detener conexiones a redes Botnet y servidores C&C.

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 78 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.
- Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
- La solución de Filtrado 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 exceptuar la inspección de HTTPS por categoría.
- Debe contar con la capacidad de restringir contenido de youtube usando restricción strict o Moderate por medio del perfil de Filtro de Contenido para tráfico 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 Youtbube configurado por el administrador de la cuenta, bloqueando cualquier tipo de contenido distinto al permitido
- Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);
- La solución debe permitir controlar el acceso a sitios web por medio de palabras o patrones que se encuentren dentro de su contenido.
- El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.
- El sistema de filtrado URL debe incluir la capacidad de no solo poner una entrada URL de manera simple, sino que también por medio de meta caracteres (Wildcards o regular expressions)
- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;
- 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.
- Debe tener la funcionalidad de exclusión de URLs por categoría;
- Permitir página de bloqueo personalizada;
- Soporte de Explicit Web Proxy, soportar proxy web transparente;

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.
- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
- Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.
- Capacidad de detección de más de 7000 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 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.
- Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;

- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, Análisis para detectar anomalías de protocolo, Desfragmentación IP, Re ensamblado de paquetes TCP;
- Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
- Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
- Los eventos deben identificar el país que origino la amenaza;
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- Métodos de notificación:
  - Alarmas presentadas en la consola de administración del appliance.
  - Alertas vía correo electrónico.
  - Debe tener la capacidad de cuarentena, prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.
  - La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma “indefinida”, hasta que un administrador tome una acción al respecto.
  - Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

Control de Aplicaciones

- La 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 y resetear conexión
- 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.
- Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;
- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente
- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante.

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 y FTP en su versión segura
- Debe ser posible definir perfiles de inspección SSL donde se definan 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.

Alta Disponibilidad

- Los dispositivos deberán 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. Debe ser posible definir interfaces de gestión independientes para cada miembro en un clúster.
- Debe ser posible definir que Firewall Virtual estará activo sobre un miembro del Cluster para hacer una distribución de carga en caso de ser necesario.
- El equipo debe soportar hasta 4 equipos en esquema de HA.
- En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
- Debe soportar la creación de sistemas virtuales en el mismo equipo;
- Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, en modo activo-activo y activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;

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 orígenes 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 más consultados por los usuarios.
- Visibilidad de las amenazas o incidentes que han ocurrido o estén 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 ancho de banda que se está consumiendo en tiempo real por cada fuente, destino, sitio web, aplicación etc. Con el fin de tener una clara visión del consumo.
- Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma.
- De las aplicaciones Cloud como Dropbox que permiten compartir archivos, 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.
- Debe tener la capacidad de generar un diagrama de conexión lógicas. En el cual se visualice la plataforma y los equipos conectados a ella (por medio del tráfico que los mismos generan).

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).
- 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.
- 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.
- Soporte de SNMP versión 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, incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.

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 10 (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 tráfico 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.

SD-WAN

- Debe soportar microsegmentación de tráfico donde sea posible, aplicar políticas de IPS y Antivirus entre segmentos de LAN.
- Debe admitir NAT en el contexto de salida (NAT Outbound) a un grupo de IP públicos
- Debe proveer la capacidad de realizar inspección SSL para el tráfico https, bloqueo de malware y reconocimiento en capa 7 de aplicaciones en cada una de las sedes
- Debe proveer gestión centralizada en Cloud propia, con modalidad opcional para retención de registros en el período mínimo de 1 año
- Debe ser capaz de ofrecer una gestión multi-tenan en la plataforma de Cloud propia
- Debe ser capaz de proporcionar Zero Touch provisioning
- La funcionalidadde Zero Touch provisioning debe ser capaz de admitir direccionamiento estático y dinámico y que se admite en varios vínculos WAN
- La funcionalidadde Zero Touch debe ser escalable, soportando un mínimo de 15 dispositivos en una misma comunidad VPN

- Debe ser capaz de proveer una arquitectura de comunicación entre las sedes, de tal manera que puedan utilizar su canal local de internet para establecer una VPN con cualquier elemento de SD-WAN
- Debe ser capaz de medir el estado de salud del enlace basándose en criterios mínimos de: Latencia, Jitter y Packet Loss, donde sea posible configurar un valor de Threshold para cada uno de estos ítems, donde será utilizado como factor de decisión en las reglas de SD-WAN
- Debe ser capaz de medir el estado de salud con soporte para múltiples servidores.
- Debe permitir modificar la configuración del tiempo de chequeo en segundos para cada uno de los enlaces
- Debe permitir la configuración de reglas donde el Failback (retorno a la condición inicial) sólo ocurrirá cuando el enlace principal recuperado sea X% (con X variando de 10 a 50) de su valor de Salud mejor que el enlace actual
- Debe permitir la configuración de reglas donde el Failback (retorno a la condición inicial) sólo ocurra dentro de un espacio de tiempo de X segundos, configurable por el administrador del sistema
- Debe permitir la configuración de políticas de QoS en la capa 7, asociadas porcentualmente al ancho de banda de la interfaz SD-WAN
- Debe posibilitar la distribución de peso en cada uno de los enlaces que componen el SD-WAN, a criterio del administrador, de forma que el algoritmo de equilibrio utilizado pueda basarse en Número de sesiones, Volumen de tráfico, IP de origen y destino desbordamiento de Enlace (Spillover)
- La funcionalidad SD-WAN debe ofrecer solución de problemas en la consola de línea de comandos o gráfica, donde sea posible: Ejecutar Packet sniffer del tráfico interesante, filtrando por: IP y Puerto y Realizar depuración detallada de las fases de negociación VPN
- La funcionalidad SD-WAN debe ofrecer una visualización gráfica

Integración con la plataforma existe.

Actualmente la Universidad, cuenta con equipos de referencia fortinet , los cuales utiliza para dar una arquitectura de seguridad multicapa y proteger los segmentos lan y core en intranet incluyendo una solución de seguridad para red inalámbrica, servicios LAN que operan como Firewall de segmentación interna (ISFW), así como para la administración, gestión de logs y reportes e incidentes, por tanto La plataforma ofertada de seguridad para seguridad perimetral, deberá poder integrarse a los dispositivos y plataformas actuales, de manera transparente y nativa, sin incurrir en licenciamiento adicional ni en costos adicionales para el proyecto, con el fin de permitir que se compartan información de eventos de ciberseguridad que permita decidir de manera central las acciones a tomar ante un incidente, y así mismo verificar los cambios topológicos de arquitectura de seguridad en tiempo real, esto por conveniencia tecnológica y con el ánimo de tener total integración y funcionalidad con la infraestructura ya adquirida por la universidad,

Por conveniencia tecnológica se requiere compatibilidad e integración nativa hacia el sistema de logs, reportaría y manejo de eventos basado en fortianalyzer y administración basada en fortimanager, así como sistema de gestión de eventos e información de seguridad (Security Information and Event Management) SIEM basado en fortisiem, sistemas implementados en la institución para garantizar un ecosistema de seguridad unificado y responder así a los procesos de integración y automatización necesarios.

Licenciamiento y actualizaciones

- El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones VPN equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.
- La vigencia de las actualizaciones para los servicios protección ante amenazas, threat protection, Antivirus, AntiSpam, IPS, Application Control, URL Filtering debe proveerse por al menos **5** años.
- El NGFW ofertado, debe traer consigo integración con Sandbox en la nube del fabricante y este debe estar incluido como parte de la solución y durante el tiempo de la garantía.
- La plataforma es requerida por un periodo de **cinco** (**5**) años en un esquema **7**x**24** ante el fabricante. Incluir soporte, garantía, cambio de partes y licenciamiento.

2. APROVISIONAMIENTO DE TRANSCEIVERS

Se deben incluir con la solución los siguientes conectores o módulos transceiver:

- (12) Módulos de conexión cable SPF+ Pasivo direct attach 10GB, incluidos transceiver 10GE SFP+ en ambos extremos, con compatibilidad para todos los sistemas con SFP+ longitud de 3 mts.

3. LICENCIAMIENTO PARA FORTIMANAGER

Se debe incluir con la solución licenciamiento incluido soporte y garantía para fortimanager FMG-VMTM20008180 5 años. Gestión hasta 10 Fortinet devices/Virtual Domains, 1 GB/Day
de Logs y 100 GB almacenamiento. Con soporte para todas las plataformas fortimanager-VM

La universidad actualmente cuenta con un administrador centralizado para los dispositivos de seguridad, basado en el fortimanager. por lo que se solicita la renovación del soporte del mismo y se requiere que los dispositivos de firewall NGFW suministrados y de reportería tengan total compatibilidad de forma nativa con este, para facilitar la administración centralizada e integración del ecosistema de seguridad.

4. SISTEMA DE REPORTERIA

Se debe incluir un dispositivo hardware dedicado para análisis de log centralizado, de capacidad mínima de 16 TB de almacenamiento con licenciamiento de indicadores de compromiso (IOC) incluido por 5 años. 4xGE, 2x GE SPF, garantía y soporte Por 5 años soporte dispositivos tipo fortinet. Según las siguientes especificaciones:

Registros/Día [GB]:mínimo 200
Velocidad sostenida analítica mínima [logs/seg]: 4000
Tasa sostenida del colector mínimo [logs/seg]: 6000
Dispositivos soportados mínimo 200
Número máximo de análisis de días: 50
Factor de forma: 1 RU de montaje en rack
Interfaces GE RJ45: 4
Interfaces GE SFP: 2
Capacidad de almacenamiento [TB]: mínimo 16 TB
Discos duros extraíbles: Si
Niveles RAID admitidos: 0/1,1s/5,5s/10
Tipo de RAID: hardware/intercambiable en caliente
Fuente de Alimentación Redundante: Opcional
Debe soportar acceso vía SSH, WEB (HTTPS) para la gestion de la solución
Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía linea de comandos en consola de gestión.
Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
Soporte SNMP versión 2 y 3
Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH
Autenticación de usuarios de acceso a la plataforma via LDAP, radius, TACAS+
Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos, burbuja y tabla.
Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.

Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado
Contar con mecanismos de borrado automático de logs antiguos.
Permitir la importación y exportación de reportes
Debe contar con la capacidad de crear informes en formato HTMLPDF, XML,
Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
La solución debe contar con reportes predefinidos
Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución
Debe ser posible la duplicación de reportes existentes para su posterior edición.
Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.

Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
Debe poseer mecanismo de “Drill-Down” para navegar en los reportes de tiempo real.
Debe permitir descargar de la plataforma los archivos de logs para uso externo.
Tener la capacidad de generar y enviar reportes periódicos automáticamente.
Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
Permitir el envío por email de manera automática de reportes.
Debe permitir que el reporte a enviar por email sea al destinatario específico.
Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
Debe permitir el uso de filtros en los reportes.
Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
Permitir especificar el idioma de los reportes creados
Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.
Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.
Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.
Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.
Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo
Debe permitir visualizar en tiempo real los logs recibidos.
Debe permitir el reenvío de logs en formato syslog.
Debe permitir el reenvío de logs en formato CEF (Common Event Format).
Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red, los usuarios comprometidos, el trafico de aplicaciones y sitios web, las detecciones de amenazas, actividad de endpoints, actividad vpn, puntos de accesos wifi y ssids

Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3 Debe permitir generar alertas de eventos a partir de logs recibidos Debe permitir crear incidentes a partir de alertas de eventos para endpoint Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas. Debe permitir respaldar logs en nube publica de Amazon S3,Microsoft azure y Google Cloud. Debe soportar el estándar SAML para autenticación de usuarios administradores Reportes Debe contar con reporte de diferente tipo incluyendo pero no limitándose a: cumplimiento de PCI DSS, aplicaciones SaaS, VPN, IPS, reputación cliente, análisis de seguridad, amenazas cibernéticas, redes sociales, trafico DNS, correo electrónico, reporte de vulnerabilidades de solución gestionada de seguridad, entre otros. El sistema de reporteria ofertado debe tener total compatibilidad de manera nativa con la arquitectura de seguridad basada en equipos tipo Fortinet de los que dispone la Institución.

5. SERVICIOS DE SOPORTE E INSTALACIÓN
• El oferente deberá entregar todas las soluciones / equipos en los sitios/sedes indicados por la entidad. • Instalación, Implementación, configuración y puesta en marcha de las soluciones ofertadas. • Todas las plataformas deberán ser de propósito específico, no se aceptan soluciones genéricas. • Anexar carta de certificación del fabricante de la solución donde se acredite al proponente como distribuidor directo autorizado en Colombia de los productos ofertados, La certificación debe ser expedida por el fabricante; no se aceptan certificaciones a través de mayoristas. En caso de participar mediante consorcios o uniones temporales, esta certificación solo se le exigirá a uno de los miembros de dicha unión. Esta debe estar en idioma inglés o español.
El contratista deberá garantizar soporte y garantía para las plataformas ofertadas en un esquema **7x24** por **cinco** (**05)** años, incluyendo cambio de partes.
El oferente seleccionado debe suministrar capacitación sobre la configuración y manejo de la Solución. La capacitación puede ser dictada en modalidad presencial o virtual, con certificación oficial del fabricante incluido voucher de certificación. Se debe incluir mínimo: • curso de entrenamiento de FortiManager NSE5 • certificación para Fortinet NSE7 Enterprise Firewall. • certificación para Fortinet NSE7 Advanced Analytics. • certificación para Fortinet NSE7 FortiSiem.
Todos los elementos Software y Hardware de la solución de seguridad deben tener garantía, soporte y reemplazo de partes por mínimo 5 años directamente con el fabricante.
Se debe entregar el registro de los elementos en plataforma de soporte y brindar la posibilidad de soporte y tickets con el fabricante en modalidad web, mínimo por el tiempo de la garantía.
Se deben incluir todos los elementos necesarios para la instalación de los equipos, licencias, rieles, soportes, accesorios necesarios para su disposición en racks.

1.13. RECEPCIÓN Y PRESENTACIÓN DE OFERTAS.

Con la firma de la propuesta, el oferente declara bajo la gravedad de juramento que no se encuentra incurso en ninguna causal de incompatibilidad e inhabilidad para presentar la oferta.

La propuesta debe presentarse FOLIADA, en forma consecutiva ascendente y que sus folios coincidan exactamente con el ÍNDICE que presenten, en carpeta debidamente organizada, en español, sin enmendaduras, tachones ni borrones, y presentarse según cronología del proceso, en la Vicerrectoría Administrativa, calle 4 N° 5 -30, segundo piso.

Los sobres 1 y 2 deben marcarse claramente, con la siguiente información:

- Nombre del oferente
- Número de la Convocatoria
- El objeto
- Dirección y teléfono celular del proponente
- Correo electrónico

Sobre #1

En el sobre # 1 el proponente deberá presentar en su propuesta los documentos habilitantes, es decir los jurídicos, financieros y técnicos, y documentos que otorgan puntaje, excepto la oferta económica; los cuales deberán ser entregados por el ofertante dentro del término indicado en la cronología del proceso.

Sobre #2

El sobre # 2 deberá contener únicamente la propuesta económica en medio físico y en medio magnético (memoria USB) la cual debe ser diligenciada en programa Microsoft Excel Versión 2007 o superior, con el fin de que sea compatible con cualquier programa de Hoja de Cálculo. Se debe verificar que el archivo sea copiado correctamente pues muchas veces al realizar el proceso de copiado y pegado, el resultado es un archivo correspondiente a un acceso directo. Deberá ser entregado por el ofertante a la hora establecida y deberá depositarse en la urna que se le indique al momento de la presentación de la propuesta. El valor de cada ítem y el costo total de la oferta debe ser redondeado a cero (0) decimales. (El oferente debe utilizar la función “REDONDEAR” de Excel con cero decimales).

La propuesta deberá tener una vigencia mínima de noventa (90) días calendario, contados a partir de la fecha de cierre de la Convocatoria

1.14. DESCUENTOS

Los impuestos que aplican para el contrato que se deriva de este proceso son los siguientes:

CLASE DE DESCUENTO	PORCENTAJE
RETENCIÓN EN LA FUENTE (A título de impuesto de renta)	2,5% declarante y 3,5% no declarante sobre la base facturada antes de IVA o sobre el valor total para el régimen simplificado
RETENCIÓN DE IVA	15% de la base del IVA facturado
RETENCION INDUSTRIA Y COMERCIO - ICA	6 x 1.000 de la Base facturada antes de IVA o sobre el valor total para el régimen simplificado.

No se aceptarán propuestas enviadas vía fax, correo electrónico o entregadas en otras oficinas de la Universidad del Cauca, ni las entregadas después de la fecha y hora señalada en el cronograma.

Para efectos de establecer las inhabilidades previstas en la normatividad vigente, al momento de recibir la oferta, se dejará constancia escrita de la fecha y hora exacta de presentación, indicando de manera clara y precisa el nombre o razón social del proponente y el de la persona que en nombre o por cuenta de éste ha efectuada materialmente la presentación.

Los proponentes por la sola presentación de su propuesta autorizan a la Universidad del Cauca, para constatar y verificar toda la información que en ella suministra, dentro del proceso de revisión.

Una propuesta por oferente: el oferente deberá presentar solamente una propuesta, ya sea por sí solo o como integrante de un consorcio o unión temporal. El Oferente no podrá ser socio de una firma que

simultáneamente presente propuesta por separado, salvo el caso de las sociedades anónimas abiertas de lo contrario su propuesta será objeto de rechazo.

1.15. PROPUESTAS EXTEMPORÁNEAS

No se aceptarán propuestas presentadas por fuera del plazo de la presente convocatoria pública, acorde a la cronología del proceso**.**

1.16. RETIRO, MODIFICACIÓN O ADICIÓN DE LAS PROPUESTAS

Si un oferente desea retirar su propuesta deberá presentar una solicitud escrita en tal sentido, ante el presidente de la Junta de Licitaciones y Contratos de la Universidad del Cauca, antes de la fecha de cierre de la convocatoria pública.

No le será permitido a ningún participante, retirar, modificar o adicionar su propuesta después del cierre de la convocatoria pública**.**

1.17. ADJUDICACIÓN DEL CONTRATO O DECLARACIÓN DE DESIERTA DE LA CONVOCATORIA.

La Universidad del Cauca, adjudicará el contrato al proponente que oferte el menor precio en la puja dinámica, Al proponente favorecido con la adjudicación se le notificará la adjudicación y deberá presentarse dentro de los tres (3) días hábiles siguientes, con los documentos para su perfeccionamiento. Así mismo, asumirá el pago de todos los gastos necesarios para su legalización.

Si el adjudicatario no concurriere a suscribir el contrato o no hiciere las diligencias necesarias para su legalización dentro del plazo que para tal fin señale la entidad o no demuestre interés en suscribirlo, se adjudicará al siguiente en orden de elegibilidad, siempre y cuando cumpla con las condiciones del pliego y sea favorable para la universidad y se procederá hacer efectiva la póliza de seriedad aportada.

Esta adjudicación se refrendará mediante la resolución expedida por el ordenador del gasto. La notificación del acto administrativo de adjudicación se hará conforme a lo establecido con el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (ley 1474 de 2011) al proponente favorecido a través de la Secretaría General. La resolución de adjudicación es irrevocable y obliga a la entidad y al adjudicatario. El acto de adjudicación no tendrá recursos administrativos.

La Universidad del Cauca podrá declarar desierta la convocatoria pública 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 da derecho a los oferentes para solicitar indemnización alguna.

Contra la resolución de declaratoria desierta solo procede recurso de reposición, en el evento que se hayan presentado oferentes.

1.18. ACLARACIONES Y MODIFICACIONES MEDIANTE ADENDAS

Cualquier aclaración o modificación a los términos de la presente convocatoria pública, o el aplazamiento de las fechas establecidas en el cronograma que la Universidad considere oportuno hacer, será publicada previamente en su página institucional en la sección de contratación, las cuales serán de obligatoria observancia para la preparación de las ofertas.

Las respuestas a las observaciones serán publicadas en la página web institucional, en los tiempos estimados en la cronología del proceso.

1.19. RECHAZO DE LAS PROPUESTAS

a. Cuando se presenten dos o más Ofertas por el mismo Proponente, bajo el mismo nombre o con nombres diferentes o directamente o como miembro de un Consorcio o Unión temporal. En este caso se rechazarán las dos (2) o más Ofertas en las que concurra dicha situación.
b. Cuando la propuesta presentada por el oferente que también haga parte de una persona jurídica, consorcio o unión temporal que se haya presentado a la presente convocatoria.

c. Cuando el representante legal de la persona jurídica tenga limitaciones para presentar Oferta y definitivamente no se adjunte la autorización del órgano social para la presentación de la misma o presente una autorización que resulte insuficiente de conformidad con lo exigido en el Pliego.
d. Cuando, al momento del cierre del presente proceso, no se cumpla con el requerimiento del objeto social o con la duración exigida para las personas jurídicas.
e. Cuando se presente la Oferta en forma subordinada al cumplimiento de cualquier condición o modalidad no prevista en el Pliego de Condiciones.
f. Cuando el Consorcio o Unión Temporal modifique, durante la etapa pre-contractual, los porcentajes de participación de los integrantes.
g. Cuando el Proponente o alguno de sus integrantes se encuentre incurso en alguna inhabilidad o prohibición para contratar previstas en la legislación colombiana.
h. En caso de Ofertas suscritas a través de apoderados, cuando no se presente el respectivo poder junto con la Oferta o cuando éste no se encuentre suscrito por quien debe suscribirlo.
i. Si después de efectuada alguna corrección aritmética en la oferta inicial, el valor ofrecido de algún ítem exceda el valor establecido para cada ítem en el presupuesto oficial.
j. Cuando la persona jurídica Proponente individual o integrante de Consorcio o Unión temporal se encuentre en causal de disolución o liquidación obligatoria.
k. Cuando la Oferta sea presentada extemporáneamente de acuerdo con lo establecido en el Pliego de Condiciones.
l. Cuando la propuesta fuera presentada por personas naturales o jurídicas que hayan intervenido, directa o indirectamente en el estudio técnico o participado en la elaboración de los pliegos de condiciones, o por las firmas cuyos socios o personas a su servicio hayan tenido tal intervención.
m. Cuando revisados los documentos de la propuesta se encuentre prueba sumaria de la existencia de alguna ilegalidad o falsedad en los documentos presentados.
n. Cuando abiertos los sobres se encuentre prueba sumaria de la existencia de algún acto o conducta que tenga objeto de colusión o confabulación entre dos o más propuestas.
o. Cuando abiertos los documentos de las propuestas estén incompletas, en cuanto a que no cumplen lo especificado o dejen de incluir alguno de los documentos obligatorios, sin perjuicio del principio de subsanabilidad.
p. Cuando el proponente no incluya la oferta económica en medio impreso, o cuando esta no esté firmada por quien esté en la obligación de hacerlo.
q. Cuando se evidencie que la oferta económica no cumple con las especificaciones técnicas de todos los ítems del presente proceso.
r. Si después de efectuada alguna corrección aritmética en la oferta inicial, se rechazaran sólo aquellas ofertas que superen el presupuesto oficial.
s. Si después de efectuada la fórmula para verificar si la oferta presentada por el proponente, se encuentra que es una oferta con precios artificialmente bajos.
t. Cuando el proponente no haga entrega de la garantía de seriedad de la oferta junto con su propuesta.

1.20. CRONOLOGÍA DEL PROCESO

ACTIVIDAD	FECHA 2023	LUGAR
Publicación **PROYECTO DE PLIEGO DE CONDICIONES**	26 de mayo	Página web de la entidad http://www.unicauca.edu.co/contratacion
Plazo para presentar **OBSERVACIONES** al proyecto de pliego de condiciones, incluidas las referidas a la distribución de riesgos.	30 de mayo hasta 11:00 am	Únicamente en formato Word, al correo electrónico: contratacion3@unicauca.edu.co
RESPUESTA A LAS OBSERVACIONES de los interesados presentadas al proyecto de pliego de condiciones.	31 de mayo	Página web de la entidad http://www.unicauca.edu.co/contratacion
Resolución que ordena la **APERTURA** del proceso de licitación Pública	31 de mayo	Página web de la entidad http://www.unicauca.edu.co/contratacion
Publicación del **PLIEGO DE CONDICIONES DEFINITIVO** y consulta del mismo.	31 de mayo	Página web de la entidad http://www.unicauca.edu.co/contratacion

Plazo máximo para publicar **ADENDAS (en caso que sea necesario)**	01 de junio	Página web de la entidad http://www.unicauca.edu.co/contratacion
Cierre del plazo de la licitación pública para la presentación de propuestas y apertura en acto público de las propuestas **sobre No. 1**. (evaluación componentes jurídico y financiero)	2 de junio hasta las 02:30 pm	Sala de juntas Vicerrectoría Administrativa Calle 4 # 5-30 Segundo Piso Popayán - Cauca
Evaluación de las ofertas y publicación del informe de evaluación. (Componente técnico).	05 de junio	Sala de juntas Vicerrectoría Administrativa Calle 4 # 5-30 Segundo Piso Popayán – Cauca Publicación informe en Página web de la entidad http://www.unicauca.edu.co/contratacion
Presentación de observaciones y documentos subsanables	06 de junio hasta las 3:00 p.m.	Únicamente por escrito en la Vicerrectoría Administrativa Calle 4 # 5-30 Segundo Piso Popayán - Cauca
Respuesta a las observaciones formuladas y publicación del listado de proponentes habilitados	07 de junio	Página web de la entidad http://www.unicauca.edu.co/contratacion
Audiencia pública de apertura del **sobre No. 2**, corrección aritmética, formula de puntaje, orden de elegibilidad y adjudicación.	**08 de junio a las 10:00 a.m.**	Sala de juntas Vicerrectoría Administrativa Calle 4 # 5-30 Segundo Piso Popayán – Cauca

NOTA IMPORTANTE: Todas las horas se fijan de acuerdo al reloj estampador de la Vicerrectoría Administrativa, sobre las ofertas que lleguen en físico y las que lleguen en medio digital por la fecha y hora de recepción del mensaje.

1.21. VERIFICACION DE REQUISITOS HABILITANTES

La Junta de Licitaciones y Contratos y el comité evaluador designado realizará la verificación de requisitos habilitantes, los cuales deberán encontrarse en el sobre No. 1 con el fin de determinar cuáles de las ofertas son HABILITADAS y, en tal caso, podrán participar en la audiencia de adjudicación.

Se publicará en la página de la Universidad la evaluación de requisitos habilitantes identificando los proponentes que no se consideren habilitados y a los cuales se les concederá un plazo, para que subsanen la ausencia de requisitos técnicos, financieros o jurídicos y/o presenten las aclaraciones que estimen pertinentes, de acuerdo a la cronología del proceso, sin que se entienda que, en ejercicio de esta facultad, los oferentes puedan adicionar o mejorar sus propuestas.

Una vez cumplido el término para subsanar, se publicará en el portal web de contratación de la Universidad el listado de los proponentes que resulten HABILITADOS.

De conformidad con el parágrafo primero del artículo 5 de la ley 1150 del 2007 "Todos aquellos requisitos de la propuesta que no afecten la asignación de puntaje, deberán ser solicitados por las entidades estatales y deberán ser entregados por los proponentes hasta el término de traslado del informe de evaluación.

CAPÍTULO II

DOCUMENTOS HABILITANTES DE LA PROPUESTA

Se deberá tener en cuenta para la presentación de la propuesta a la presente convocatoria pública, las adendas que se le realicen, las aclaraciones que haga la Universidad del Cauca, las actas, notas importantes y resoluciones que se expidan en relación con esta convocatoria.

NOTA: Los documentos que no generan calificación, previo análisis de la Junta de Licitaciones y contratos, podrán ser subsanados dentro del plazo establecido en la cronología del proceso.

Podrán participar en el presente proceso de selección, todas las personas naturales, en forma individual o conjunta (consorcio o unión temporal), personas jurídicas legalmente constituidas, cuya actividad comercial u objeto social esté relacionada con el objeto a contratar en el presente proceso de selección, que cumplan con todos los requisitos exigidos en el presente documento y que no se encuentren dentro de las inhabilidades e incompatibilidades previstas en la Constitución Política de Colombia y en la ley; éste último hecho se debe expresar bajo la gravedad de juramento, en la Carta de Presentación de la propuesta, según el Anexo A.

La propuesta debe tener una vigencia de noventa (90) días calendario contados a partir de la fecha de cierre del presente proceso de convocatoria pública, de conformidad con la carta de presentación. Los proponentes deberán extender el período de validez, en razón de la prórroga en los plazos de adjudicación o firma del contrato, so pena de que se entienda que desisten de la misma.

Para realizar la verificación del cumplimiento o no de los requisitos habilitantes, de los proponentes a la presente convocatoria pública, se tendrán en cuenta los siguientes factores:

No.	FACTORES	CUMPLIMIENTO
1	DOCUMENTOS JURÍDICOS HABILITANTES	HÁBIL O NO HÁBIL
2	DOCUMENTOS FINANCIEROS HABILITANTES	HÁBIL O NO HÁBIL
3	DOCUMENTOS TÉCNICOS HABILITANTES	HÁBIL O NO HÁBIL

2.1. DOCUMENTOS JURÍDICOS (Sobre #1)

a) CARTA DE PRESENTACIÓN DE LA PROPUESTA

La propuesta deberá ser suscrita por el representante legal de la firma, el representante de la figura asociativa o la persona natural, utilizando como modelo la carta de presentación suministrada en esta convocatoria pública. Ver (Anexo A), el cual no podrá ser modificado en su contenido.

Con la firma de la propuesta, el oferente declara bajo la gravedad del juramento no estar inhabilitado para presentar la oferta como persona natural o persona jurídica o por quienes conforman el proponente plural.

b) GARANTÍA DE SERIEDAD DE LA OFERTA

La propuesta deberá acompañarse de una garantía bancaria o de una póliza **A FAVOR DE ENTIDADES PARTICULARES** otorgada por una compañía de seguros legalmente establecida en Colombia **acompañada de su correspondiente constancia de depósitos, recibo de pago o certificación expedida por la compañía en donde conste que la póliza no expira por falta de pago de la prima**, con el fin de asegurar la firma y perfeccionamiento del contrato por parte del proponente favorecido con la adjudicación.

En dicho documento se verificará lo siguiente:

a) Asegurado/Beneficiario: UNIVERSIDAD DEL CAUCA - NIT 891.500.319-2

b) Cuantía: El DIEZ POR CIENTO 10% del valor total del presupuesto oficial establecido para el presente proceso contractual

c) Vigencia: de noventa (90) días calendario contados a partir de la fecha prevista para el cierre de la invitación.

d) Tomador/Afianzado: la póliza o garantía deberá tomarse con el nombre del PROPONENTE o de la razón social que figura en el certificado de Existencia y Representación Legal expedido por la Cámara de Comercio.

Cuando la propuesta la presente un Consorcio o Unión Temporal, la garantía de seriedad debe ser tomada a nombre del Consorcio o Unión Temporal (indicando cada uno de sus integrantes y su porcentaje de participación).

e) Firma del representante legal: la póliza o garantía deberá firmarse por parte del representante legal del PROPONENTE (tratándose de uniones temporales o Consorcios por el representante designado en el documento de constitución).

El PROPONENTE deberá ampliar la vigencia de la garantía en caso de presentarse prórrogas en los plazos de la contratación, de la asignación, o de la suscripción del contrato, no cubiertas con la vigencia inicial.

Tanto al PROPONENTE favorecido con la contratación como a los demás participantes, se les devolverá la garantía de la seriedad de la propuesta cuando esté perfeccionado y legalizado el contrato derivado de la presente invitación, previa solicitud escrita en este sentido.

La UNIVERSIDAD hará efectiva la totalidad de la garantía, a título de indemnización por perjuicios en los siguientes casos:

1. Cuando el PROPONENTE se niegue a prorrogar la garantía de seriedad de la PROPUESTA, en caso que la UNIVERSIDAD decida modificar el calendario de la invitación.
2. Cuando el PROPONENTE, por cualquier motivo, salvo fuerza mayor o caso fortuito debidamente comprobado y aceptado por la UNIVERSIDAD, no cumpliere las condiciones y obligaciones establecidas en el pliego de condiciones o en su PROPUESTA, en especial no suscribir y legalizar el contrato dentro de los tres (3) días hábiles siguientes a la comunicación de su adjudicación.

c) EXISTENCIA Y CAPACIDAD LEGAL

- **PERSONA NATURAL:** Si el proponente es **persona natural** deberá aportar copia del documento de identidad; y registro mercantil expedido por la Cámara de Comercio con una antelación no superior a treinta (30) días a partir de la fecha prevista para el cierre del proceso, en el cual se indique que su objeto social contiene las actividades o servicios que correspondan al objeto de la presente invitación.

- **CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL.**

  Si el proponente es persona jurídica Nacional, deberá acreditar su existencia, objeto social, representación legal, facultades del representante y duración de la sociedad, mediante el Certificado de Existencia y Representación Legal expedido por la Cámara de Comercio o la autoridad competente, con una antelación no superior a treinta (30) días calendario de la fecha prevista para el cierre de esta invitación, en el cual se indique que su objeto social contiene las actividades o servicios que se relacionen con el objeto de la presente convocatoria. Las personas jurídicas deberán acreditar que su duración no es inferior al término de ejecución del contrato y por lo menos un (1) año más.

  Autorización para Comprometer a la persona jurídica Cuando el representante legal de la persona jurídica se halle limitado en sus facultades para contratar y comprometer a la misma, el proponente debe presentar copia del acta aprobada de la Junta de Socios o Asamblea respectiva u órgano competente, donde conste que ha sido facultado para presentar oferta y firmar el contrato hasta la cuantía señalada en el presente documento.

- **CÉDULA DE CIUDADANÍA**

  Fotocopia legible de la cédula de ciudadanía o extranjería si fuere el caso: Anexar documento del proponente persona natural y representante legal de la persona jurídica. Aplica para cada uno de los miembros de Consorcios y Uniones Temporales

- **DOCUMENTO DE CONFORMACIÓN DE CONSORCIO O UNIÓN TEMPORAL**

En el caso de los consorcios y uniones temporales, cada uno de sus integrantes acreditará los requisitos y documentos antes mencionados, tanto si el integrante es persona natural como si es persona jurídica y cada uno de los integrantes deberá tener una participación en la estructura plural no inferior al 30%

En caso de Consorcio o Unión Temporal, los proponentes indicarán dicha calidad, para lo cual anexará el documento de constitución, el cual debe establecer el nombre y/o razón social de todos sus integrantes, sus números de identificación, los términos y extensión de la participación, la designación de la persona que los representará, una dirección, teléfono y correo electrónico de contacto, y señalará las reglas básicas de la relación entre ellos y su responsabilidad.

El Proponente deberá presentar el documento que acredite la conformación del Consorcio y/o Unión Temporal, de acuerdo con el Anexo C, para el caso de consorcio y de acuerdo con el Anexo D para el caso de unión temporal, INDICANDO LA PARTICIPACIÓN Y RESPONSABILIDADES DENTRO DE LA UNIÓN TEMPORAL O CONSORCIO.

Si el adjudicatario es un Consorcio o Unión Temporal, dentro de los dos (2) días hábiles siguientes a la notificación de la adjudicación, deberán entregar el RUT y NIT correspondiente.

Los integrantes del Consorcio o de la Unión Temporal no pueden ceder sus derechos a terceros sin obtener la autorización previa, expresa y escrita de la Universidad del Cauca. En ningún caso podrá haber cesión del contrato entre quienes integran el consorcio o unión temporal.

La propuesta debe estar firmada por el representante legal que para el efecto designen los integrantes del consorcio o unión temporal.

En el caso de Consorcio y/o Uniones Temporales el representante deberá formar parte del Consorcio o Unión Temporal y anexar copia del documento de identificación.

d) INSCRIPCIÓN Y CLASIFICACIÓN EN EL REGISTRO ÚNICO DE PROPONENTES

El oferente deberá presentar el registro único de proponentes vigente y en firme, con fecha de expedición anterior al cierre de la presente convocatoria no mayor a treinta (30) días calendario.

Las personas que hayan renovado el RUP y se encuentre en firme deberán presentar el documento renovado en el año 2023, de no encontrarse en firme la renovación, deberán presentar el documento renovado en el año 2022, junto con el recibo de pago que indica que hay un proceso de renovación en trámite. En cualquiera de los dos casos, el oferente deberá presentar el registro único de proponentes con fecha de expedición anterior al cierre de la presente convocatoria no mayor a treinta (30) días calendario.

Aplica para cada uno de los integrantes del Consorcio o Uniones temporales.

e) RUT

Se debe presentar copia del Registro Único Tributario (RUT) indicando a qué régimen pertenece y que esté vigente. Aplica para cada uno de los integrantes del consorcio o unión temporal.

Si el adjudicatario es un Consorcio o Unión Temporal, deberá realizar oportunamente el trámite para obtener el RUT y NIT correspondiente.

f) ACREDITACIÓN DE LOS APORTES A LOS SISTEMAS DE SEGURIDAD SOCIAL INTEGRAL Y PARAFISCALES

Cuando el proponente sea una persona jurídica, Debe presentar una certificación (expedida por el Revisor Fiscal, cuando éste exista de acuerdo con los requerimientos de la Ley, o por el Representante Legal, cuando no se requiera Revisor Fiscal), en la que se indique que se encuentran al día en el pago de los aportes de sus empleados a los sistemas de salud, riesgos profesionales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje SENA, Dicho documento debe certificar que, a la fecha prevista para la recepción de documentos, ha realizado el pago de los aportes correspondientes a la

nómina de los últimos seis (6) meses, contados a partir de la citada fecha, en los cuales se haya causado la obligación de efectuar dichos pagos.

En caso de presentar acuerdo de pago con las entidades recaudadoras respecto de alguna de las obligaciones mencionadas deberá manifestar que existe el acuerdo y que se encuentra al día en el cumplimiento del mismo. En este evento el oferente deberá anexar certificación expedida por la entidad con la cual existe el acuerdo de pago.

Cuando se trate de Consorcios o Uniones Temporales, cada uno de sus miembros integrantes que sea persona jurídica, deberá aportar el certificado aquí exigido.

Cuando el proponente sea una persona natural, Debe presentar una certificación expedida por la persona natural oferente en la que declare bajo la gravedad de juramento que ha cumplido con el pago de los aportes a los sistemas de Salud, Riesgos Profesionales y Pensiones como persona natural e independiente y cuando ha habido lugar a ello a los aportes parafiscales a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje SENA, de sus empleados durante los seis (6) meses anteriores a la fecha de cierre de la presente convocatoria, en los cuales se haya causado la obligación de efectuar dichos pagos.

En caso de no estar obligado al pago de parafiscales deberá anexar declaración en tal sentido (precisando que no está obligado por no tener personal dependiente) Cuando se trate de Consorcios o Uniones Temporales, cada uno de sus miembros integrantes que sea persona natural, deberá aportar la certificación aquí exigida.

g) COMPROMISO DE TRANSPARENCIA:

El proponente deberá presentar el formulario previsto en el (Anexo J), debidamente diligenciado y suscrito por el proponente, su representante legal, representante o apoderado.

h) PAZ Y SALVO EXPEDIDO POR LA DIVISIÓN DE GESTIÓN FINANCIERA DE LA UNIVERSIDAD DEL CAUCA

Con una vigencia menor a treinta (30) días calendario a la fecha de la audiencia de adjudicación de la presente convocatoria según la forma como se constituya el proponente: de la persona natural, de la Persona Jurídica y de cada uno de los integrantes del Consorcio o Unión Temporal, este documento podrá ser expedido con posterioridad al cierre siempre y cuando no sobrepase el término establecido para subsanar.

El trámite para la solicitud y expedición DE PAZ Y SALVOS deberá realizarse de la siguiente manera:

Se deberá solicitar la factura, indicando el NIT o número de documento de identidad y adjuntando copia escaneada del mismo al correo institucional credito@unicauca.edu.co , con copia al correo institucional viceadm@unicauca.edu.co , una vez cancelada la factura se deberán remitir los siguientes documentos: factura cancelada, solicitud y anexos, al anexos, al correo pazysalvosfinanciera@unicauca.edu.co , con copia a wbenavides@unicauca.edu.co .

i) CERTIFICADO DE ANTECEDENTES FISCALES, DISCIPLINARIOS Y JUDICIALES, con fecha de expedición no mayor a treinta (30) días anteriores a la fecha de cierre de la presente convocatoria.

En caso que los antecedentes del proponente (persona natural/persona jurídica) o el representante o integrante del proponente plural, presenta inhabilidad para contratar con el estado, la Universidad RECHAZARÁ la propuesta.

j) REGISTRO NACIONAL DE MEDIDAS CORRECTIVAS

En atención a la entrada en vigencia de la Ley 1801 de 2016 (Código de Policía) la página web de la Policía Nacional puso a disposición el sitio **Sistema Registro Nacional de Medidas Correctivas RNMC** para la consulta de infracciones a la mencionada Ley. Es importante tener en cuenta que la persona que no pague las multas establecidas en la Ley 1801 de 2016 "Por la cual se expide el Código Nacional de Policía y Convivencia" no podrá celebrar o renovar contratos con el Estado.

En caso de que el proponente (persona natural/persona jurídica) o el representante o integrante del proponente plural esté reportado en el citado registro, quedará inhabilitado para contratar con el estado y por ende su propuesta será RECHAZADA.

2.2. DOCUMENTOS FINANCIEROS (Sobre #1)

La evaluación financiera se realizará con base en la información consignada en el Registro Único de Proponentes. Los siguientes documentos deben ser presentados por cada uno de los oferentes que se presenten ya sea en forma individual o como integrantes del Consorcio o Unión Temporal.

CAPACIDAD FINANCIERA.

Los indicadores financieros miden la fortaleza financiera del oferente y para el presente proceso el mismo deberá acreditar los siguientes requisitos de capacidad financiera:

Capital de Trabajo = Activo Corriente – Pasivo Corriente **El proponente deberá demostrar un capital trabajo igual o superior a 100 % del presupuesto oficial** Para el cálculo del Capital de Trabajo para consorcios y uniones temporales, será el resultado de la sumatoria del capital de trabajo de cada uno de sus miembros.
Índice de liquidez = Activo Corriente /Pasivo Corriente **El proponente deberá demostrar un índice de liquidez mayor o igual a 1.2.** Para el cálculo del Índice de liquidez para Consorcios o Uniones Temporales, será el cociente de la sumatoria de los activos corrientes de cada uno de sus miembros sobre la sumatoria de los pasivos corrientes de cada uno de los miembros.
Índice de Endeudamiento = Pasivo Total / Activo total **El proponente deberá tener un nivel de endeudamiento menor o igual a 0.6** Para el cálculo del Nivel de endeudamiento para Consorcios o Uniones Temporales, será el cociente de la sumatoria de los pasivos totales de cada uno de sus miembros sobre la sumatoria de los activos totales de cada uno de los miembros.

2.3. DOCUMENTOS TÉCNICOS (Sobre #1)

2.3.1 EXPERIENCIA ESPECÍFICA DEL PROPONENTE:

Con el fin de verificar la experiencia específica para la contratación del objeto de la presente convocatoria, el proponente debe demostrar la ejecución de:

MÁXIMO CUATRO (04) contratos, donde se pueda verificar que los elementos e insumos suministrados estén relacionados con los de la presente convocatoria pública, y cuya sumatoria del valor total ejecutado sea igual o superior al presupuesto oficial.

La experiencia específica se acreditará mediante la presentación de las correspondientes actas de liquidación y/o certificaciones de la ejecución de los contratos relacionados en el formulario de experiencia específica (Anexo G) suscritas por la entidad contratante y en las que sea posible verificar las actividades relacionadas con objeto del presente proceso requerido por la Universidad. Los contratos que aporte el oferente para demostrar su experiencia, deberán haberse ejecutado y liquidado antes del cierre de la presente convocatoria.

Los documentos presentados para acreditar la experiencia deberán contener como mínimo el número del contrato, objeto del contrato, fecha de inicio, fecha de finalización, el valor total ejecutado, las actividades ejecutadas, y el porcentaje de participación cuando se haya ejecutado en forma asociativa.

De no contener la información podrá ser complementado con otro documento firmado por el contratante. Si existiese en los documentos que acrediten la experiencia, nota o salvedades que indiquen directamente inconformidades o insatisfacción con el recibo del objeto del contrato, la entidad no considerará válida esa experiencia.

En caso de que el proponente relacione o anexe un número superior a **CUATRO (04)** contratos, para efectos de evaluación de la experiencia, únicamente se tendrán en cuenta los **CUATRO (04)** primeros contratos relacionados en el Formulario de experiencia (Anexo G) en orden consecutivo. Los proponentes deberán diligenciar toda la información requerida en el Formulario de experiencia.

Los contratos deberán haber sido suscritos por el oferente ya sea individualmente o en consorcio o unión temporal, con entidades públicas o privadas, estás últimas necesariamente deberán ser personas jurídicas.

En ofertas presentadas por consorcios o uniones temporales, cada uno de los integrantes debe acreditar como mínimo el 30% de la experiencia específica en máximo TRES (3) contratos relacionada con el criterio del valor total ejecutado (VTE); pudiendo incluir los contratos que se aportan para acreditar la experiencia específica del proponente plural, aunque no necesariamente debe ser coincidente la experiencia específica que aporta el proponente plural con la mínima exigida a cada miembro de la figura asociativa, sin embargo, se mantienen idénticos los requisitos del proponente plural para que pueda ser considerada experiencia específica habilitante del integrante.

La Universidad de Cauca tendrá en cuenta la experiencia que presenten los proponentes en calidad de Consorcio y Unión Temporal, proporcional a su participación en dichas alianzas comerciales.

Para la sumatoria del VALOR TOTAL EJECUTADO (VTE) que acredita la experiencia específica se tendrá en cuenta el valor facturado actualizado de los contratos aportados por el proponente.

Para tales efectos, deberá allegar diligenciado con su propuesta, el formato que se especifica según Anexo G “EXPERIENCIA ACREDITADA DEL PROPONENTE”, previsto en el pliego de condiciones.

Cada contrato que el proponente aporte como experiencia debe estar inscrito en el registro único de proponentes – RUP, en al menos UNO (01) de los códigos UNSPSC que se describen a continuación. El RUP deberá estar vigente y en firme, de lo contrario el proponente quedará INHABILITADO.

UNSPSC	SEGMENTO	FAMILIA	CLASE
432225	**43** difusión de Tecnologías de Información y Telecomunicaciones	**22** equipos o plataformas y accesorios de redes multimedia o de voz y datos	**25** Equipos de Seguridad de red.
432226	**43** difusión de Tecnologías de Información y Telecomunicaciones	**22** equipos o plataformas y accesorios de redes multimedia o de voz y datos	**26** Equipo de servicio de red.

Cuando el contrato o su respectiva certificación den cuenta que el Contratista actuó bajo la modalidad de Consorcio o Unión Temporal, se deberá especificar y certificar el porcentaje (%) de participación de cada uno de los miembros, ya que para la sumatoria del VALOR TOTAL EJECUTADO solo se tendrá en cuenta el porcentaje en que haya participado en cada contrato aportado.

Si el contrato incumple cualquiera de los requisitos anteriores NO SERÁ tenido en cuenta para la evaluación.

VALOR TOTAL EJECUTADO

El valor total ejecutado de cada proponente, se calculará mediante la siguiente expresión:

$$VTE = \sum_{j=1}^{U} VFA_j$$

Donde,

VTE	=	Valor total ejecutado, expresado en SMML.
VFAj	=	Valor facturado actualizado de cada contrato válido para acreditar experiencia, expresado en SMML.
J	=	Número de contrato válido para acreditar experiencia.
U	=	Número máximo de contratos válidos para acreditar experiencia – máximo CUATRO (04).

A partir del valor facturado por concepto de cada contrato presentado, se determina el valor facturado actualizado (VFAj) de cada contrato (j) expresándolo en salarios mínimos mensuales legales, así:

Se tomará el valor en SMMLV correspondiente a la fecha de terminación del contrato; para tal fin se tendrá en cuenta la EVOLUCIÓN DEL SALARIO MÍNIMO MENSUAL LEGAL.

EVOLUCIÓN DEL SALARIO MÍNIMO MENSUAL LEGAL

PERÍODO	MONTO MENSUAL
---	---
Enero 1 de 1980 a Dic. 31 de 1980	4.500,00
Enero 1 de 1981 a Dic. 31 de 1981	5.700,00
Enero 1 de 1982 a Dic. 31 de 1982	7.410,00
Enero 1 de 1983 a Dic. 31 de 1983	9.261,00
Enero 1 de 1984 a Dic. 31 de 1984	11.298,00
Enero 1 de 1985 a Dic. 31 de 1985	13.558,00
Enero 1 de 1986 a Dic. 31 de 1986	16.811,00
Enero 1 de 1987 a Dic. 31 de 1987	20.510,00
Enero 1 de 1988 a Dic. 31 de 1988	25.637,00
Enero 1 de 1989 a Dic. 31 de 1989	32.560,00
Enero 1 de 1990 a Dic. 31 de 1990	41.025,00
Enero 1 de 1991 a Dic. 31 de 1991	51.716,00
Enero 1 de 1992a Dic. 31 de 1992	65.190,00
Enero 1 de 1993 a Dic. 31 de 1993	81.510,00
Enero 1 de 1994 a Dic. 31 de 1994	98.700,00
Enero 1 de 1995 a Dic. 31 de 1995	118.934,00
Enero 1 de 1996 a Dic. 31 de 1996	142.125,00
Enero 1 de 1997 a Dic. 31 de 1997	172.005,00
Enero 1 de 1998 a Dic. 31 de 1998	203.826,00
Enero 1 de 1999 a Dic. 31 de 1999	236.460,00
Enero 1 de 2000 a Dic. 31 de 2000	260.100,00
Enero 1 de 2001 a Dic. 31 de 2001	286.000,00
Enero 1 de 2002 a Dic. 31 de 2002	309.000,00
Enero 1 de 2003 a Dic. 31 de 2003	332.000,00
Enero 1 de 2004 a Dic. 31 de 2004	358.000,00
Enero 1 de 2005 a Dic. 31 de 2005	381.500,00
Enero 1 de 2006 a Dic. 31 de 2006	408.000,00
Enero 1 de 2007 a Dic. 31 de 2007	433.700,00
Enero 1 de 2008 a Dic. 31 de 2008	461.500,00
Enero 1 de 2009 a Dic. 31 de 2009	496.900,00
Enero 1 de 2010 a Dic. 31 de 2010	515.000,00
Enero 1 de 2011 a Dic. 31 de 2011	535.600,00
Enero 1 de 2012 a Dic. 31 de 2012	566.700,00
Enero 1 de 2013 a Dic. 31 de 2013	589.500,00
Enero 1 de 2014 a Dic. 31 de 2014	616.000,00
Enero 1 de 2015 a Dic.31 de 2015	644.350,00
Enero 1 de 2016 a Dic.31 de 2016	689.455,00
Enero 1 de 2016 a Dic.31 de 2017	737.717,00
Enero 1 de 2018 a Dic.31 de 2018	781.242,00
Enero 1 de 2019 a Dic. 31 de 2019	828.116,00
Enero 1 de 2020 a Dic. 31 de 2020	877.803,00
Enero 1 de 2021 a Dic. 31 de 2021	908.526,00
Enero 1 de 2022 a Dic. 31 de 2022	1.000.000,00
Enero 1 de 2023 a Dic. 31 de 2023	1.160.000,00

Para determinar el valor facturado actualizado, se aplica la siguiente expresión:

$$VFA_j = \frac{VF_j}{SMML(\text{año de terminación del contrato})}$$

Donde,

VFAj = Valor facturado actualizado de cada contrato válido para acreditar experiencia, expresado en SMML.

VFj = Valor facturado total de cada contrato válido para acreditar experiencia, expresado en pesos.

SMML = Salario mínimo mensual legal, del año de terminación del contrato válido para acreditar experiencia.
J = Número de contrato válido para acreditar experiencia.

Para efectos de la evaluación de EXPERIENCIA por VALOR TOTAL EJECUTADO se aplicará la siguiente fórmula:

VTE ≥ PO
Donde,

VTE = Valor Total ejecutado, expresado en SMMLV.
PO = Presupuesto oficial del módulo al cual presenta oferta, expresado en SMMLV.

Si el proponente no cumple este requisito se calificará NO HÁBIL para el proceso al cual presenta propuesta.

Si el contrato aportado para acreditar la experiencia se ejecutó bajo la modalidad de consorcio o unión temporal, el valor a considerar será el equivalente al porcentaje de participación que tuvo el integrante que la pretenda hacer valer**.**

El oferente deberá diligenciar el (Anexo G): EXPERIENCIA ESPECIFICA DEL PROPONENTE que se publicará en el presente proceso, este documento deberá presentarse debidamente firmado.

2.3.2. CATALOGOS O FICHAS TECNICAS

El oferente deberá anexar catálogos y/o fichas de la solución de seguridad Perimetral ofertada, los cuales deben cumplir mínimo con las especificaciones técnicas descritas en el presente documento.

2.3.3 CERTIFICACION COMO DISTRIBUIDOR AUTORIZADO

Anexar certificación del fabricante, donde se pueda verificar que es distribuidor autorizado de la solución de seguridad perimetral ofertada para Colombia y enumerando la plataforma ofertada para el presente proyecto.

2.3.4 ESPECIFICACIONES TÉCNICAS MÍNIMAS HABILITANTES

El proponente deberá cumplir o superar con la presentación de la oferta las condiciones técnicas mínimas que se describen en el apartado técnico. Para ello deberá diligenciar y aportar **el (Anexo E)** donde se especifica que cumple con las especificaciones técnicas con las que ejecutará el contrato en caso de resultar adjudicatario del presente proceso y se listan los componentes de la solución. En caso de ofertar especificaciones técnicas inferiores a las solicitadas en el presente proceso la oferta será rechazada

2.3.5 PROPUESTA ECONÓMICA (Sobre #2)

Propuesta económica

Para ser tenida en cuenta la propuesta, deberá utilizarse el modelo suministrado en esta convocatoria pública y ser suscrita por el representante legal o por la persona legalmente autorizada para ello debidamente diligenciado (ANEXO B) indicando las cantidades, precios unitarios y valores totales, en cifras redondeadas sin decimales (Con la función redondear de Excel), además, deberá entregarse en medio físico debidamente firmado y en medio magnético (memoria USB en formato Excel versión 97 o superior)

Valor de la oferta

Los valores deberán expresarse en pesos colombianos, a precios unitarios fijos vigentes.

La propuesta deberá presentarse en ANEXO B de la presente convocatoria pública, INDICANDO LOS PRECIOS UNITARIOS Y VALORES TOTALES EN CIFRAS REDONDEADAS SIN DECIMALES, ADEMÁS, DEBERÁ ENTREGARSE EN MEDIO FÍSICO DEBIDAMENTE FIRMADO Y EN MEDIO MAGNÉTICO, EN FORMATO EXCEL (versión 97 o superior). Este anexo debe diligenciarse

contemplando todas y cada uno de los ítems. Igualmente, si la propuesta económica, precios unitarios y valor total de la propuesta no están debidamente firmado por quien está en la obligación legal de realizarlo, la Universidad lo entenderá como falta de ofrecimiento en el aspecto económico lo cual llevará al rechazo de la propuesta.

Con el diligenciamiento de la propuesta económica, el proponente acepta que conoce en su totalidad las especificaciones técnicas.

CAPÍTULO III

CRITERIOS DE ASIGNACIÓN DE PUNTAJE (1000 PUNTOS)

Los documentos requeridos para la asignación de puntaje deberán ser aportados junto con la propuesta.

Las propuestas que hayan cumplido con los requisitos de admisibilidad y no se encuentren incursas en causal de rechazo, se calificarán con el siguiente puntaje:

No.	CRITERIOS DE EVALUACION			PUNTAJE
A	PRECIO			**700 puntos**
B	SERVICIOS DE VALOR AGREGADO	EQUIPOS WIFI PARA COBERTURA SEGURA DE SEDES	300	**300 puntos**
TOTAL PUNTOS				**1000 puntos**

A. PRECIO (700) PUNTOS

Se asignarán 700 puntos como máximo al proponente que ofrezca el menor precio en la oferta total, incluido IVA; los demás se calificarán en forma proporcional descendente, de acuerdo con la siguiente fórmula:

$$\text{Puntaje Oferta} = \frac{\text{Menor valor} * 700}{\text{Valor ofrecido}}$$

Se tendrá en cuenta hasta el tercer (3°) decimal del valor obtenido como puntaje.

B. SERVICIOS DE VALOR AGREGADO (300) PUNTOS

- EQUIPOS WIFI PARA COBERTURA SEGURA DE SEDES (300) PUNTOS

Con el objetivo de extender las capacidades de la solución de seguridad a sedes y oficinas remotas universitarias, se estipula el servicio de valor agregado del suministro de dispositivos de conexión inalámbrica que aprovechen las redes seguras para ofrecer acceso inalámbrico seguro al borde de la LAN de la institución. Los dispositivos entregados deben integrarse de manera nativa a la solución de seguridad brindada para ofrecer un ecosistema de seguridad único, consistente e integrado, brindando visibilidad de la red de extremo a extremo, y respuesta automatizada a amenazas.

Los dispositivos entregados deben permitir la gestión de la red inalámbrica y la seguridad con la misma consola del sistema de seguridad perimetral brindado en la oferta, para optimizar la administración y tener un ecosistema integrado, permitiendo implementar políticas de seguridad consistentes en redes cableadas e inalámbricas.

Los dispositivos deben permitir junto con las características SD-WAN de la solución de seguridad, el establecimiento de SD-Branch segura, Así como la posibilidad del acceso a la red corporativa de manera segura a los trabajadores remotos mediante la implementación de AP remotos.

Los dispositivos deben soportar hasta 512 clientes por radio
Los dispositivos deben soportar 3 radios + 1 radio BLE Bluetooth Low Energy

Internal: x4 Dual band Wi-Fi + x4 Tri-band Wi-Fi & Scanning + 1 Single band 2.4GHz BLE/ ZigBee
Los dispositivos deben soporta capacidad en 2.4 Ghz, 5GHz y 6Ghz, con velocidad por radio de hasta 1148 Mbps, 2402 Mbps y hasta 4804 Mbps.

Para la obtención del puntaje el proponente deberá presentar documento, debidamente suscrito, donde indique la cantidad de Dispositivos a entregar y su referencia y modelo.

Para la obtención de los puntos se seguirá la siguiente relación:

Puntaje Valor agregado=. N de dispositivos entregados *100

Siendo el máximo puntaje posible asignado de 300 puntos. Cada dispositivo debe cumplir con los requerimientos establecidos en este numeral.

C. DESEMPATE:

En caso de presentarse un empate en la calificación de dos (2) o más PROPONENTES, la UNIVERSIDAD seleccionará al PROPONENTE, con base en las disposiciones del artículo 35 de la ley 2069 del 2020.

Si el empate se mantiene, se realizará sorteo mediante el sistema de balotas.

CAPITULO IV

ASPECTOS GENERALES DEL CONTRATO

3.1. PLAZOS DE SUSCRIPCIÓN Y LEGALIZACIÓN

PRESENTACIÓN DE DOCUMENTOS PARA PERFECCIONAMIENTO, LEGALIZACIÓN Y EJECUCIÓN

El adjudicatario deberá suscribir el contrato dentro de los tres (03) días calendario siguientes a la fecha de notificación de la resolución de adjudicación.

El contratista deberá legalizar el contrato (constitución de póliza) dentro del plazo establecido en el artículo 47 del acuerdo 064 de 2008.

Si el adjudicatario no suscribe el contrato ni cumple con los requisitos de legalización dentro de los plazos señalados, la Universidad podrá adjudicar el contrato al proponente calificado en segundo lugar, mediante resolución motivada, dentro de los dos (02) días hábiles siguientes.

Si el adjudicatario no suscribe el contrato y demás trámites necesarios para su legalización dentro del término señalado, quedará a favor de la Universidad del Cauca en calidad de sanción, el valor de la garantía de seriedad de la propuesta, sin menoscabo de las acciones legales conducentes al reconocimiento de perjuicios causados y no cubiertos por el valor de la misma.

El plazo de la ejecución rige a partir de la legalización del contrato.

El contratista se obliga a atender las instrucciones impartidas por el Interventor designado por la Universidad del Cauca.

El adjudicatario para suscribir el contrato deberá encontrarse a paz y salvo con las entidades u organismos del Estado.

3.2. FORMA DE PAGO

La Universidad del Cauca pagará el valor del contrato de la convocatoria pública, en pesos colombianos cien por ciento (100%) contra entrega, previa presentación de los siguientes documentos:

- Factura o documento equivalente de conformidad con la normatividad que se encuentre vigente.
- Acta de ingreso de los bienes entregados al almacén de la Universidad del Cauca.
- Certificaciones de cumplimiento y el acta de recibo a satisfacción expedidas por parte del supervisor, en las que se consignarán las cantidades suministradas, los precios unitarios y los valores totales de los elementos e insumos entregados.
- Certificación expedida por el revisor fiscal o representante legal donde conste la afiliación obligatoria y pago actualizado del personal que requiera en desarrollo del contrato, al Sistema General de Seguridad Social y parafiscales conforme a la Ley.
- Evaluación de proveedor suscrita por el supervisor del contrato**.**

La UNIVERSIDAD sólo adquiere obligaciones con el proponente favorecido en el presente proceso y bajo ningún motivo o circunstancia aceptará pagos a terceros.

El pago será cancelado en pesos colombianos, a través de la consignación en la cuenta bancaria que el contratista señale de las entidades financieras afiliadas al sistema automático de pagos, previos los descuentos de Ley, por intermedio de la Universidad.

3.3. ANTICIPO: Para el presente proceso la Universidad del Cauca NO entregará anticipo

3.4. LA SUPERVISIÓN

La supervisión de la presente convocatoria pública la realizará un 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, ley 1474 de 2011 y ley 734 de 2002.

3.5. GARANTÍAS

El proponente favorecido con la adjudicación del contrato deberá constituir a favor de la Universidad las siguientes pólizas:

- **Cumplimiento,** en cuantía del veinte por ciento (20%) del valor total del contrato, y con una vigencia igual a la duración del contrato y dos (2) meses más**.**

- **Calidad y correcto funcionamiento,** en cuantía equivalente al cincuenta por ciento (50%) del valor total del contrato, con vigencia de un (1) año contado a partir contado a partir del recibo final del contrato**.**

Para efectos de tramitar el acta de aprobación de la póliza el Contratista deberá:

a) Entregar a la universidad las garantías para su aprobación.
b) Restablecer el valor de la garantía cuando éste se haya visto reducido por razón de las reclamaciones efectuadas por LA UNIVERSIDAD.
c) Ampliar el valor de la garantía otorgada o su vigencia, en cualquier evento en que se adicione el valor del contrato o se prorrogue su término, según el caso.

Una vez iniciada la ejecución del contrato, en caso de incumplimiento del respectivo contratista de la obligación de obtener la ampliación de la garantía, su renovación, de restablecer su valor o de otorgar una nueva garantía que ampare el cumplimiento de las obligaciones que surjan por razón de la celebración, ejecución y liquidación del contrato, el contratista autoriza a la UNIVERSIDAD a solicitar la modificación correspondiente y asume el valor de la prima.

3.6. OBLIGACIONES DEL OFERENTE FAVORECIDO.

El proponente a quien se le adjudique el contrato, además de estar obligado al cumplimiento del objeto contractual, de acuerdo con los bienes a suministrar establecidos en la presente convocatoria, deberá cumplir con las siguientes obligaciones:

a) Suministrar e instalar dentro del plazo establecido en el presente proceso, la totalidad de los bienes a suministrar de acuerdo con las características técnicas exigidas en los ítems requeridos por la Entidad, según lo establecido en el Anexo No. B “OFERTA ECONÓMICA INICIAL”.
b) Hacer entrega en perfecto estado, el objeto del contrato.
c) Constituir la garantía única de cumplimiento requerida por la Entidad dentro de los tres (3) días calendario siguientes al perfeccionamiento del contrato.
d) Allegar a la UNIVERSIDAD para el trámite del pago, certificación del representante legal o del revisor fiscal según el caso, sobre el pago de los aportes al Sistema de Seguridad Social (salud, pensión y riesgos laborales) y parafiscales (Caja de Compensación Familiar, SENA e ICBF), de los empleados del CONTRATISTA, de conformidad con lo establecido en el artículo 50 de la Ley 789 de 2002, y demás normas concordantes.
e) Acatar las instrucciones que para el desarrollo del contrato le imparta la UNIVERSIDAD por conducto del supervisor del Contrato.
f) Informar oportunamente al supervisor del contrato sobre las imposibilidades o dificultades que se presenten en la ejecución del mismo y ofrecer alternativas para garantizar la buena ejecución del contrato.
g) Suscribir los documentos contractuales necesarios para la ejecución y el acta de liquidación, si hubiere lugar.
h) Las demás que sean necesarias para dar cumplimiento al objeto contractual o que se hayan indicado en la oferta o anexos.

3.7. OBLIGACIONES POR PARTE DE LA UNIVERSIDAD

- Aprobar la póliza que garantiza el contrato
- Suministrar oportunamente la información suficiente y requerida por el contratista para la ejecución del contrato. E instalación de los bienes objeto del contrato.
- Aprobar por intermedio del supervisor la entrega recepción de los elementos suministrados objeto del contrato.
- Efectuar los trámites necesarios para el pago.

- Realizar los pagos previa presentación de los documentos requeridos correcta por parte del contratista.
- Las demás que sean necesarias, acorde con la naturaleza del contrato.

3.8. DOCUMENTOS DEL CONTRATO

Los siguientes son los documentos del contrato y a él se consideran incorporados:

- El estudio técnico junto con sus anexos.
- El Pliego de Condiciones y sus anexos
- Las adendas expedidas por la UNIVERSIDAD.
- La propuesta en todas sus partes y aceptada por la UNIVERSIDAD.
- El informe de evaluación.
- Acta de audiencia de puja dinámica presencial
- La resolución de adjudicación.
- La Garantía Única aprobada por la UNIVERSIDAD.
- Las demás actas y documentos correspondientes a la ejecución contractual.

Atentamente,

DEIBAR RENE HURTADO HERRERA
Rector
Universidad del Cauca

Proyectó: Laura Victoria Rodríguez Muñoz– Componente Jurídico – Vicerrectoría Administrativa
Deicy Leandra Martínez Maca – Componente Jurídico – Vicerrectoría Administrativa
Revisó: Lady Cristina Paz - Componente Jurídico – Oficina Asesora Jurídica
Diana Carolina Tovar - Componente Jurídico – Oficina Asesora Jurídica
Jorge Alberto Martínez Gallego – Componente Técnico –Tic´s
Aprobó: Pablo Zambrano Simmonds – Jefe Oficina Asesora Jurídica

ANEXO A
FORMATO DE CARTA DE PRESENTACIÓN DE LA PROPUESTA

Popayán, _____2.023

Señores
UNIVERSIDAD DEL CAUCA
Ciudad.

El suscrito_____legalmente autorizado para actuar en nombre de _____de acuerdo con las estipulaciones establecidas en la convocatoria pública Nº _____ de 2023, de la Universidad del Cauca, hago llegar a Ustedes la siguiente propuesta para realizar "RENOVACIÓN DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL, PARA GARANTIZAR LA INTEGRIDAD, CONFIABILIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN, NECESARIAS PARA LA CORRECTA PRESTACIÓN DE LOS SERVICIOS INSTITUCIONALES PARA EL CENTRO DE DATOS DE LA DIVISIÓN DE LAS TECNOLOGÍAS DE LA UNIVERSIDAD DEL CAUCA".

Para tal efecto declaro:

- Que esta propuesta y el contrato que llegare a celebrarse, solo compromete al firmante de esta carta o a quien representa.
- Que ninguna entidad o persona distinta del firmante tienen interés comercial en esta propuesta, ni en el contrato probable que de ella se derive.
- Bajo la gravedad de juramento, que se entiende presentado con la firma de la propuesta, que conozco el área donde se suministraran los bienes, que he investigado sobre las características, localización y naturaleza de sus instalaciones, así mismo sobre, la mano de obra, transporte, proveedores, distribuidores, fabricantes y disponibilidad de los bienes a suministrar.
- Que en los precios unitarios se han incluido todos los costos correspondientes al suministro, transporte y acopio si llegara el caso; lo mismo que otros aspectos de acuerdo a las especificaciones técnicas del presente proceso
- Que he leído, conozco y aceptó las especificaciones técnicas establecidas por la Universidad del Cauca en el presupuesto oficial.
- Que he leído, conozco la información general y demás documentos de la presente convocatoria y acepto las especificaciones y demás requisitos en ellos contenidos.
- Que asumo el reconocimiento y asunción de los riesgos previsibles que puedan surgir en la ejecución del contrato.
- Que la información correspondiente a la experiencia requerida y sus soportes, son veraces.
- Bajo la gravedad de juramento que no me hallo incurso en ninguna de las causales de inhabilidades e incompatibilidades señaladas por la ley.
- Bajo gravedad de juramento que me encuentro a paz y salvo por concepto de impuestos sobre la renta y complementarios a la fecha de cierre de la presente convocatoria.
- Que el régimen tributario al cual pertenezco es _____
- Que me comprometo a suministrar los elementos en el plazo establecido en la presente convocatoria, a partir de la legalización del contrato.
- Que el proponente, los miembros que lo integran si fuere el caso y el representante legal no está (n) reportado (s) en el Boletín de Responsables Fiscales, disciplinarios y judiciales, expedido por la Contraloría General de la República, Procuraduría y Policía respectivamente.
- Que el valor de mi propuesta inicial está consignado en el (sobre # 2) de la oferta económica.
- Que la presente propuesta técnico-jurídica-financiera consta de: _____ ( ) folios debidamente numerados _____
- Acusamos recibo de las adendas Nros._____

Atentamente,

Firma del proponente _____

Nombre del proponente _____

C. No. _____de _____

Dirección de correo _____

Correo electrónico _____

Teléfono _____

Ciudad _____

ANEXO B
OFERTA ECONÓMICA INICIAL

CONVOCATORIA PÚBLICA No. _____ DE 2023

"RENOVACIÓN DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL, PARA GARANTIZAR LA INTEGRIDAD, CONFIABILIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN, NECESARIAS PARA LA CORRECTA PRESTACIÓN DE LOS SERVICIOS INSTITUCIONALES PARA EL CENTRO DE DATOS DE LA DIVISIÓN DE LAS TECNOLOGÍAS DE LA UNIVERSIDAD DEL CAUCA".

PRESUPUESTO SOLUCIÓN DE SEGURIDAD PERIMETRAL					
ITEM	**DESCRIPCIÓN**	**UNID**	**CANT**	**VALOR UNITARIO**	**VALOR TOTAL**
1	Dispositivo Hardware dedicado appliance con licenciamiento plus 24x7 con licenciamiento soporte y garantía, remplazo de partes y protección unificada (UTM) por 5 años mínimo. Incluyendo módulos de seguridad de filtrado web, control de aplicaciones, IPS/IDS, antivirus, sandbox en nube configuración en HA y todas las especificaciones técnicas indicadas en el pliego.	UN	2		
2	Módulos de conexión cable SPF+ Pasivo direct attach 10GB, incluidos transceiver 10GE SFP+ compatibilidad todos los sistemas con SFP+ longitud de 3 mts.	UN	12		
3	Soporte y garantía para fortimanager FMG-VMTM20008180 5 años. Gestión hasta 10 Fortinet devices/Virtual Domains, 1 GB/Day de Logs y 100 GB almacenamiento. Con soporte para todas las plataformas fortimanager-VM	UN	1		
4	Dispositivo hardware dedicado para análisis de log centralizado, 16 TB almacenamiento con licenciamiento de indicadores de compromiso (IOC) por 5 años. 4xGE, 2x GE SPF, garantía y soporte Por 5 años soporte dispositivos tipo fortinet. Según especificaciones técnicas del pliego.	UN	1		
			SUBTOTAL		
			IVA		
			TOTAL		

_____
FIRMA

NOMBRE DEL PROPONENTE: _____
NIT / CÉDULA: _____
REPRESENTANTE LEGAL: _____

ANEXO C
PARTICIPACIÓN CONSORCIO

Señores
UNIVERSIDAD DEL CAUCA
Popayán

Los suscritos _____ y _____, quienes actuamos en nombre de _____ y _____, manifestamos nuestra decisión de participar como Consorcio, en la CONVOCATORIA Nº ___ de 2023, cuyo objeto se refiere a realizar el "RENOVACIÓN DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL, PARA GARANTIZAR LA INTEGRIDAD, CONFIABILIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN, NECESARIAS PARA LA CORRECTA PRESTACIÓN DE LOS SERVICIOS INSTITUCIONALES PARA EL CENTRO DE DATOS DE LA DIVISIÓN DE LAS TECNOLOGÍAS DE LA UNIVERSIDAD DEL CAUCA".

1. Denominación: el Consorcio se denomina _____

2. Integración: El Consorcio está integrado por:

	Nombre	**Nit o CC.**	**% de participación**
A.	_____	_____	_____
B.	_____	_____	_____

3. Duración: La duración del Consorcio se extenderá desde la presentación de la propuesta, por el término del contrato y año más.
4. Responsabilidad: Los consorciados responderemos solidariamente por el cumplimiento total de todas y cada una de las obligaciones derivadas de la propuesta y del contrato.
5. Representante: Para todos los efectos, el representante de consorcio es _____ identificado (a) con la cédula de ciudadanía No. _____expedida en _____, quien está expresamente facultado para firmar y presentar la propuesta y, en caso de ser favorecido en la adjudicación, para celebrar el contrato y efectuar su liquidación, con el fin de cumplir con las obligaciones contractuales que adquiera el Consorcio.

6. Sede del Consorcio:

Dirección: _____
Teléfono: _____
Correo Electrónico: _____

Para constancia se firma en Popayán, a los _____ de 2023

Firma Firma

C. C. No. _____ de_____ C. C. No. _____ de _____

ANEXO D
PARTICIPACIÓN UNIÓN TEMPORAL

Señor
Rector
UNIVERSIDAD DEL CAUCA
Popayán

Los suscritos _____ y _____, quienes actuamos en nombre de _____ y _____, manifestamos nuestra decisión de participar como Unión Temporal, en la CONVOCATORIA Nº ___ de 2023, cuyo objeto se refiere a realizar el "RENOVACIÓN DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL, PARA GARANTIZAR LA INTEGRIDAD, CONFIABILIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN, NECESARIAS PARA LA CORRECTA PRESTACIÓN DE LOS SERVICIOS INSTITUCIONALES PARA EL CENTRO DE DATOS DE LA DIVISIÓN DE LAS TECNOLOGÍAS DE LA UNIVERSIDAD DEL CAUCA".

1. Denominación: La Unión Temporal se denomina _____
2. Integración: La Unión Temporal está integrada por:

	Nombre	**Nit o CC.**	**% de participación**
A.	_____	_____	_____
B.	_____	_____	_____

3. Duración: La duración de la Unión Temporal se extenderá desde la presentación de la propuesta, por el término del contrato y año más.
4. Responsabilidad: Los miembros de la U.T. responderemos individualmente de acuerdo con la participación de cada uno de nosotros en la ejecución del contrato, por el cumplimiento total de todas y cada una de las obligaciones derivadas de la propuesta y del contrato.
5. Representante: Para todos los efectos, el representante de la U.T. es _____ identificado (a) con la cédula de ciudadanía No. _____ expedida en _____, quien está expresamente facultado para firmar y presentar la propuesta y en caso de ser favorecido en la adjudicación, para celebrar el contrato y efectuar su liquidación, con el fin de cumplir con las obligaciones contractuales que adquiera la Unión Temporal.

6. Sede de la Unión Temporal:

Dirección: _____
Teléfono: _____
Correo Electrónico: _____

Para constancia se firma en Popayán, a los _____de 2023

Firma Firma

C. C. No. _____ de _____ C. C. No._____ de _____

ANEXO E

ESPECIFICACIONES TÉCNICAS MÍNIMAS

CONVOCATORIA PÚBLICA No. _____DE 2023

Señores
Universidad del Cauca
Popayán

Por medio del presente documento, el suscrito_____ legalmente autorizado para actuar en nombre de la empresa _____, manifiesto que, en caso de resultar adjudicatario del proceso de selección cumpliré con las especificaciones técnicas habilitantes, establecidas en el numeral 1.11 "**ESPECIFICACIONES TÉCNICAS**" del pliego de condiciones, con el fin de ejecutar el objeto del contrato "RENOVACIÓN DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL, PARA GARANTIZAR LA INTEGRIDAD, CONFIABILIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN, NECESARIAS PARA LA CORRECTA PRESTACIÓN DE LOS SERVICIOS INSTITUCIONALES PARA EL CENTRO DE DATOS DE LA DIVISIÓN DE TECNOLOGÍAS".

La solución ofertada se compone de los siguientes elementos:

N ítem	Marca	Referencia	Cantidad
1			
2			
3			
4			

_____

FIRMA

NOMBRE DEL PROPONENTE: _____

NIT: _____

REPRESENTANTE LEGAL: _____

CARTA DE COMPROMISO DE TRANSPARENCIA

CONVOCATORIA PÚBLICA No. ___ DE 2023

[Fecha]

Señores
UNIVERSIDAD DEL CAUCA
Popayán - Cauca

Nombre del representante legal (Proponente), identificado como aparece al pie de mi firma, [obrando en mi propio nombre o en mi calidad de representante legal de [nombre del Proponente], manifiesto que:

1. Apoyamos la acción del Estado colombiano y de la Universidad del Cauca para fortalecer la transparencia y la rendición de cuentas de la administración pública.

2. No estamos en causal de inhabilidad alguna para celebrar el contrato objeto del Proceso de Contratación N° _____ de 2023.

3. Nos comprometemos a no ofrecer y no dar dádivas, sobornos o cualquier forma de halago, retribuciones o prebenda a servidores públicos o asesores de la Entidad Contratante, directamente o a través de sus empleados, contratistas o tercero.

4. Nos comprometemos a no efectuar acuerdos, o realizar actos o conductas que tengan por objeto o efecto la colusión en el Proceso de Contratación N° _____ de 2023.

5. Nos comprometemos a revelar la información que sobre el Proceso de Contratación N° _____de 2023 nos soliciten los organismos de control de la República de Colombia.

6. Nos comprometemos a comunicar a nuestros empleados y asesores el contenido del presente Compromiso Anticorrupción, explicar su importancia y las consecuencias de su incumplimiento por nuestra parte, y la de nuestros empleados o asesores.

7. Conocemos las consecuencias derivadas del incumplimiento del presente compromiso anticorrupción.

En constancia de lo anterior firmo este documento a los [ ] días del mes de de 2023.

Nombre del proponente _____
Nombre del Representante Legal _____
C. C. No. _____ de _____

_____
(Firma del proponente (s) o de su Representante Legal)

NOTA: LOS ANEXOS F Y G SE ANEXARÁN COMO DOCUMENTOS ADICIONALES