

UNIVERSIDAD PEDAGÓGICA NACIONAL

VICERRECTORÍA ADMINISTRATIVA Y FINANCIERA
SUBDIRECCIÓN DE GESTIÓN DE SISTEMAS DE INFORMACIÓN

TÉRMINOS DE REFERENCIA
CONVOCATORIA PÚBLICA No. 05 DE 2021

OBJETO

“CONTRATAR LA ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UNA NUEVA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL (CLÚSTER DE FIREWALLS) Y DE APLICACIONES (FIREWALLS DE APLICACIONES WEB) PARA LA UNIVERSIDAD PEDAGÓGICA NACIONAL”

BOGOTÁ D.C., NOVIEMBRE DE 2021

INTRODUCCIÓN

La Universidad Pedagógica Nacional, pone a disposición de los interesados Términos de Referencia para la selección de los contratistas, encargados de ejecutar los contratos que resulten del mismo, cuyos objetos corresponden:

“CONTRATAR LA ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UNA NUEVA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL (CLÚSTER DE FIREWALLS) Y DE APLICACIONES (FIREWALLS DE APLICACIONES WEB) PARA LA UNIVERSIDAD PEDAGÓGICA NACIONAL”.

Los estudios y documentos previos, los Términos de Referencia, así como cualquiera de sus anexos está a disposición del público en la página web de la Universidad <http://contratacion.pedagogica.edu.co/#> , modalidades de contratación, CONVOCATORIA PÚBLICA, vigencia 2021.

Es de exclusiva responsabilidad del interesado verificar que la información adquirida, no siendo de recibo reclamo alguno al respecto.

La selección del contratista se realiza a través del proceso de CONVOCATORIA PÚBLICA, de conformidad con lo dispuesto en el Acuerdo 027 de 2018 *“Por el cual se expide el estatuto de contratación de la Universidad Pedagógica Nacional”*, las, y demás normas concordantes o complementarias. Para aquellos aspectos no regulados en las normas anteriores, se aplicarán las normas comerciales y civiles pertinentes.

• JUSTIFICACIÓN:

La Universidad Pedagógica Nacional, requiere de equipos y herramientas especiales de alta disponibilidad para la protección y conservación de la información institucional, por esta razón primordial, se requiere realizar la adquisición de una nueva infraestructura de seguridad perimetral la cual se encuentra compuesta por un clúster de firewalls perimetrales y un firewall de aplicaciones web. Los equipos con los cuales cuenta actualmente la Universidad Pedagógica Nacional tendrán soporte por parte del fabricante hasta el mes de mayo del 2022, por tal motivo después de esta fecha los equipos quedaran obsoletos y empezaran a generar vulnerabilidades de seguridad, las cuales pondrán en riesgo toda la infraestructura de servidores y aplicaciones de la universidad.

Es importante destacar que por estos equipos fluye todo el tráfico IP (Protocolo de Internet) que cursa por la universidad, es decir si una persona (Interna y/o Externa) quiere consultar cualquier aplicación de la universidad (Portales web, Portales académicos, entre otros) este tráfico cursa por estos equipos los cuales son los encargados de permitir o denegar este tráfico según las políticas de seguridad establecidas por los administradores de la SGSI (Subdirección de Gestión de Sistemas e Información) de la UPN. Es decir, cuando finalice el soporte por parte del fabricante por obsolescencia de estos equipos toda la infraestructura de servidores y aplicaciones de la universidad empezaran a quedar en riesgo de ataques informáticos.

GENERALIDADES:

- a) Las propuestas, comunicaciones, audiencias, providencias, aclaraciones, adendas y todo lo referente al desarrollo de la presente convocatoria pública se harán en idioma español.
- b) El proceso de contratación se regirá con lo dispuesto en la Ley 30 de 1992, en el Acuerdo 027 de 03 de septiembre de 2018 del Consejo Superior Universitario de la Universidad Pedagógica Nacional y para lo no previsto, por las normas aplicables en materia comercial y civil.
- c) Si el proponente encuentra discrepancias u omisiones en estos términos, en los demás documentos que forman parte de la presente CONTRATACIÓN, o si presenta alguna duda relacionada con algún aspecto de la convocatoria, deberá dirigirse inmediatamente, por escrito y en las oportunidades previstas para tal fin, al correo procesosdeseleccion@pedagogica.edu.co para obtener las claridades necesarias antes de la presentación de su propuesta. En caso de no surtir este proceso, se entenderá que no existen inquietudes y que se aceptan totalmente las condiciones de los términos objeto de la presente CONTRATACIÓN.
- d) Sólo serán evaluadas las propuestas que se presenten hasta la fecha límite para entrega, previo al cierre de la convocatoria y según el Cronograma de Actividades del proceso de contratación, así como aquellas que cumplan con el lleno de requisitos contenidos en estos términos de referencia.
- e) La correspondencia de los proponentes deberá radicarse en la Oficina Grupo de Contratación, Bogotá, D.C., PBX 3471190, Carrera 16 A No. 79-08 – Tercer Piso, Edificio Administrativo, Referencia: CONVOCATORIA PÚBLICA 05 DE 2021.
- f) Los proponentes tendrán la oportunidad de conocer y controvertir los informes, conceptos y decisiones que se rindan o adopten, para lo cual se han señalado en estos términos de referencia, etapas que permiten el conocimiento de dichas actuaciones y la posibilidad de expresar sus observaciones.
- g) El desarrollo del presente proceso es de carácter público, respetando la reserva de que gocen legalmente las patentes, procedimientos y privilegios. Los proponentes deberán indicar en la carta de presentación de la propuesta cuáles de los documentos aportados son de carácter reservado e invocar el fundamento fáctico, jurídico y legal que ampara dicha reserva. Si el proponente no hace pronunciamiento expreso amparado en la Ley, se entenderá que toda la propuesta es pública.
- h) Cuando sobrevenga una inhabilidad o incompatibilidad dentro de la presente convocatoria, se entenderá que el proponente renuncia a la participación en el proceso de selección y a los derechos surgidos del mismo, para lo cual, deberá informar tal hecho oportunamente. Si la inhabilidad o incompatibilidad sobreviene en uno de los miembros de un Consorcio o Unión Temporal este cederá su participación a un tercero, previa autorización escrita de la Universidad Pedagógica Nacional. Se aclara que la cesión no es permitida entre quienes integran el Consorcio. (Art. 9 Acuerdo 027 de 2018 del Consejo Superior).
- i) Adelantar la revisión permanente de los correos electrónicos recibidos de la cuenta procesosdeseleccion@pedagogica.edu.co sobre este proceso de selección, ya que todos los documentos que se generen con ocasión del mismo serán puestos a disposición por la Universidad a través del referido mecanismo, en cualquiera de las 24 horas del día fijado en el cronograma para tal efecto. Por lo anterior, es responsabilidad exclusiva de los interesados conocer su contenido. Las Adendas serán enviadas en los días hábiles, entre las 7:00 a.m. y las 7:00 p.m., a más tardar el día hábil anterior al vencimiento del plazo para presentar propuestas a la hora fijada para tal presentación.
- j) Esta CONTRATACIÓN se rige por el principio de selección objetiva, con base en el cual la escogencia se hace sobre el ofrecimiento más favorable a los intereses de la Universidad y a los

finés que ella busca, sin tener en consideración factores de afecto, de interés o de cualquier otra clase de motivación subjetiva. El ofrecimiento más favorable es aquel que resulta ser el mejor para la Universidad, teniendo en cuenta exclusivamente los factores de selección y la ponderación precisa, detallada y concreta de los mismos, según estos términos.

- k) La información relativa al análisis, aclaración, evaluación y comparación de las propuestas y las recomendaciones para la adjudicación del contrato no podrá ser revelada a los contratantes ni a otra persona que no participe oficialmente en dicho proceso hasta que EL COMITÉ DE EVALUACION comunique a los proponentes el resultado de evaluación de las propuestas.
- l) Las propuestas serán evaluadas por el Comité de Evaluación de la Universidad designado por el Rector. El Comité evaluador verificará la documentación presentada en las propuestas y conceptuará sobre posibles inexactitudes o errores.
- m) Las propuestas que se presenten después de la fecha y hora señaladas o en lugar distinto al indicado oficialmente, no serán recibidas. En caso de que esto ocurra no se tendrán en cuenta y se devolverán a los proponentes sin abrirlas.
- n) El proponente deberá entregar la propuesta en original y dos (2) copias, debidamente numeradas y foliadas escritas en cualquier medio impreso, acompañada de la carta de presentación según se señala en el Anexo No. 1, sin enmendaduras, tachones, sin modificación alguna ni borradores. Toda tachadura o enmendadura para ser tenida en cuenta, debe estar aclarada o convalidada con la firma al pie de la misma, de quien suscribe la carta de presentación de la propuesta.
- o) El proponente deberá allegar carta de presentación de la propuesta debidamente suscrita por el representante legal o apoderado según sea el caso, de acuerdo con el modelo suministrado por la Universidad que hace parte de los Términos de Referencia y se incluye como anexo.
- p) Queda entendido que la firma de la carta de presentación de la propuesta compromete al proponente en todo lo establecido en su propuesta, por ello deberá suscribirla el representante legal.
- q) La validez de la propuesta no podrá ser inferior a 3 meses contados a partir de la fecha límite de cierre del proceso de contratación. (En caso de no expresar el término de validez de la propuesta se entenderá como tal el término de vigencia de la garantía de seriedad de la propuesta.)
- r) Todos los costos asociados a la preparación y presentación de la propuesta son a cargo del proponente. No se aceptarán modificaciones a la propuesta con posterioridad a la fecha y hora de cierre de la CONTRATACION. La Universidad podrá solicitar la aclaración de cualquier documento o afirmación efectuada por el proponente en su propuesta, en el evento en que encuentre información equivoca, confusa o aparentemente contradictoria. Estas aclaraciones se aceptarán siempre que se puedan realizar sin modificar la propuesta. En el evento en que la aclaración implique una modificación de la propuesta, no se tendrá en cuenta. En el evento en que se presenten extemporáneamente las aclaraciones solicitadas, la Universidad rechazará la propuesta.
- s) En cumplimiento al Artículo No. 24 “SUBSANACIÓN DE LAS PROPUESTAS” del Acuerdo No. 027 de 2018 CS, en atención a los principios de igualdad y primacía del derecho sustancial, en los procesos de selección y en general en la gestión contractual de la Universidad, procederá lo sustancial sobre lo formal, de modo que la ausencia de requisitos o la falta de documentos, que no constituyan factor de comparación entre las propuestas, no servirán de título suficiente para el rechazo de las propuestas y podrán ser subsanados dentro del plazo previsto en los términos de referencia. Durante la evaluación la Universidad podrá solicitar a los proponentes las aclaraciones que considere, pero en ningún caso se podrán mejorar sus propuestas, considerando como mejora la modificación de la propuesta en los factores de comparación salvo en los procesos de subasta inversa o en aquellos en que sea posible la conformación dinámica de las propuestas.

- t) Si un proponente considera que una pro-forma impide mencionar o destacar algunos detalles o información que él considera de importancia para la evaluación de su propuesta, deberá presentar además de las pro-formas correspondientes, toda la información que considere necesaria para complementar su propuesta en un apéndice, marcando claramente la parte específica de la pro-forma de la propuesta, del cual hace parte como apéndice. Cuando una pro-forma necesite uno de éstos apéndices, se anotará debajo de la parte específica, la siguiente expresión: “Ver Apéndice No. ____
- u) Durante el proceso de selección el proponente no podrá retirar su propuesta, ni menoscabar o desconocer los efectos de esta.

ACCIONES ANTICORRUPCIÓN

Con la suscripción de la carta de presentación de la propuesta, las partes adquieren obligaciones de integridad en la función pública y de no tolerancia con la corrupción, razón por la cual, además de la connaturales al asunto se tienen las siguientes:

1. No ofrecer, no dar sobornos, ni ninguna forma de halago, dadiva a ningún funcionario público en relación con el contrato que se derive de la presente invitación pública, ni permitir que se realicen en su nombre.
2. Da aviso inmediato a la universidad, a las autoridades competentes de cualquier ofrecimiento, favor, dadiva o prerrogativa a los funcionarios públicos que intervengan en la suscripción del contrato.
3. El contratista manifiesta no incurrir en falsedad o adulteración de los documentos que acreditan para la suscripción del presente contrato.

En el evento de conocerse casos especiales de corrupción en las Universidades del Estado, se debe reportar el hecho al Programa Presidencial “Lucha contra la Corrupción” a través de los números telefónicos: (1) 562 9300, (1) 3341507 o al 01 8000913040; al FAX: 5658671; al correo electrónico buzon1@presidencia.gov.co o adminweb@presidencia.gov.co, en la página de Internet: www.anticorrupcion.gov.co; por correspondencia o personalmente, en la dirección Carrera 8 No 7-27 Edificio Galán, Bogotá, D.C.

FIN DE LA INTRODUCCIÓN

CAPÍTULO I INFORMACIÓN GENERAL

1.1. INVITACIÓN A LAS VEEDURÍAS CIUDADANAS

En concordancia con lo dispuesto en la Ley 850 de 2003, la Universidad Pedagógica, invita a todas las personas y organizaciones interesadas en hacer control social al presente Proceso de Contratación, en cualquiera de sus fases o etapas, a que presenten las recomendaciones que consideren convenientes, y a que consulten los documentos del proceso en la página web de la Universidad, y así acatar estrictamente el cumplimiento de los principios de transparencia, economía, y responsabilidad de los postulados que rigen la función administrativa, que conlleven al éxito del proceso contractual.

1.2. COSTOS DERIVADOS DE PARTICIPAR EN EL PROCESO DE CONTRATACIÓN

Cada proponente debe sufragar todos los costos, tanto directos como indirectos, relacionados con la preparación y presentación de su propuesta, por lo cual la Universidad Pedagógica Nacional, no será responsable en ningún caso de dichos costos, cualquiera que sea el resultado del proceso de selección y contratación.

Los proponentes tienen la responsabilidad de determinar, evaluar y asumir los impuestos, tasas y contribuciones, así como los demás costos tributarios y de cualquier otra naturaleza que conlleve la celebración del contrato, según la asignación de costos prevista en los Términos de Referencia.

1.3. DILIGENCIA DEBIDA E INFORMACIÓN SOBRE EL PROCESO DE SELECCIÓN

Será responsabilidad del proponente conocer todas y cada una de las implicaciones para el ofrecimiento de los objetos del presente proceso, y realizar todas las evaluaciones que sean necesarias para presentar su propuesta sobre la base de un examen cuidadoso de las características del negocio.

Por la sola presentación de la propuesta se considera que el proponente ha realizado el examen completo de todos los aspectos que inciden y determinan la presentación de la misma. La Universidad Pedagógica Nacional, no entregará para los fines de presentación y preparación de propuesta para el presente proceso, material, documentación o manuales de ninguna naturaleza asociados a las descripciones y especificaciones técnicas de los elementos que se van a adquirir, excepto la información suministrada en los términos de referencia. En consecuencia, es responsabilidad del proponente, al asumir los deberes de garantía asociados con el suministro de los bienes que se solicitan a través del presente proceso de selección, conocer plenamente las condiciones técnicas de los bienes a suministrar, sin perjuicio de la facultad que asiste a los interesados de solicitar por escrito información puntual que le permita precisar los aspectos que puedan incidir en la formulación de su propuesta.

La consulta por cualquier persona, o de cualquier información contenida en este documento o proporcionada en conjunto con el mismo o comunicada posteriormente a cualquier persona, ya sea en forma verbal o escrita, con respecto a una operación propuesta que involucra la Universidad, no podrá ni debe considerarse como una asesoría en materia de inversiones, legal, tributaria, fiscal o de otra naturaleza, por parte de los funcionarios, asesores, consultores externos o representantes de estos.

Se recomienda al proponente, que obtenga asesoría independiente en materia financiera, legal, fiscal, tributaria, técnica, económica y de cualquier otra naturaleza que consideren necesaria para la presentación de una propuesta. El proponente debe informarse sobre los requisitos legales aplicables en la jurisdicción del presente proceso de selección, es decir, la legislación vigente en la República de Colombia y del contrato que se celebrará como consecuencia de esta.

En el evento que el proponente no haya obtenido toda la información que pueda influir en la determinación de su oferta, no lo eximirá de la obligación de asumir las responsabilidades que le correspondan, ni les dará derecho a reclamaciones, reembolsos, ajustes de ninguna naturaleza o reconocimientos adicionales por parte del contratante, en el caso de que cualquiera de dichas omisiones derive en posteriores sobrecostos para el contratista.

Como consecuencia de lo anterior, el proponente, al elaborar su propuesta, debe tener en cuenta que el cálculo de los costos y gastos, cualesquiera que ellos sean, se deben basar estrictamente en sus propios estudios técnicos y en sus propias estimaciones.

1.4. COMUNICACIONES Y OBSERVACIONES AL PROCESO

Los interesados deben enviar las observaciones del Proceso de Contratación por electrónico.

La correspondencia electrónica debe enviarse al correo electrónico procesosdeseleccion@pedagogica.edu.co

Dicha solicitud debe:

- a. Contener el número del Proceso de Contratación.
- b. Dirigirse a la Oficina Grupo de Contratación
- c. Enviarse dentro del plazo establecido en el Cronograma del Proceso de Selección.
- d. Indicar los datos de contacto del remitente tales como el correo electrónico, la dirección y el número telefónico.

La Universidad responderá las solicitudes recibidas antes del cierre del proceso por medio del correo electrónico procesosdeseleccion@pedagogica.edu.co, por lo que se deberá estar atento a las comunicaciones recibidas de este.

1.5. IDIOMA

Los documentos, las comunicaciones y en general, todos los documentos publicados, o expedidos por los proponentes o por terceros para efectos del presente proceso de Contratación o para ser tenidos en cuenta en el mismo, deben ser otorgados y presentados en castellano.

Para que los documentos en un idioma distinto al castellano puedan ser tenidos en cuenta en el proceso de contratación deben ser presentados en su lengua original junto con la traducción oficial al castellano. El proponente puede presentar con la oferta los documentos con una traducción simple y entregar la traducción oficial al castellano dentro del plazo previsto para la subsanación. La traducción oficial debe ser el mismo texto presentado.

En el caso de documentos especializados como, por ejemplo, las especificaciones o fichas técnicas, que en el mercado sean de amplia utilización y aceptación en idioma distinto al castellano, el proponente deberá aportarlos en su lengua original acompañados de una traducción simple al castellano, dentro del plazo previsto para la subsanación.

La traducción oficial debe realizarse en los términos del artículo 251 del Código General del Proceso, cumpliendo el trámite de apostilla o consularización. Lo anterior de conformidad con lo establecido en la Circular Externa Única de Colombia Compra Eficiente, que incluye las actualizaciones del 16 de abril de 2019, emitida por Colombia Compra Eficiente.

1.6. DOCUMENTOS OTORGADOS EN EL EXTERIOR

Los documentos públicos expedidos en el exterior por un país signatario de la Convención de La Haya de 1961, sobre la abolición del requisito de legalización, deben apostillarse. En cambio, deben legalizarse los documentos públicos expedidos en el exterior por un país signatario de la Convención de Viena de 1963. Los documentos privados otorgados en el extranjero no requieren apostilla ni legalización, salvo los que con posterioridad sean intervenidos por un funcionario público, en cuyo caso requieren apostilla o legalización, en la forma antes indicada.

Para el trámite de apostilla o legalización de documentos otorgados en el exterior y la acreditación de la formación académica obtenida en el exterior, las Universidades aplicarán los parámetros establecidos en las normas que regulen la materia, en especial la Resolución No. 1959 de 2020 del Ministerio de Relaciones Exteriores, o la norma que la modifique, sustituya o complemente.

1.7. DEFINICIONES

Las expresiones utilizadas en el presente documento con mayúscula inicial deben ser entendidas con el significado que a continuación se indica. Los términos definidos son usados en singular y en plural de acuerdo como lo requiera el contexto en el cual son utilizados.

Los términos no definidos a continuación deben entenderse de acuerdo con su significado natural y obvio.

DEFINICIONES	
ADENDAS	Es el documento por medio del cual la Universidad modifica los términos de referencia, las cuales en ningún caso pueden expedirse ni el mismo día ni con posterioridad al día previsto para el cierre del proceso de selección.
ADJUDICACIÓN	Es la decisión final de la Universidad, expedida por medio de un acto administrativo, que determina el adjudicatario del presente Proceso de Contratación.
CLASIFICADOR DE BIENES Y SERVICIOS	Es el sistema de codificación de las Naciones Unidas para estandarizar productos y servicios, conocido por las siglas UNSPSC.
CONTRATISTA	Es el Proponente que resulte adjudicatario y suscriba el Contrato objeto del presente Proceso de Selección.



CONTRATO	Es el negocio jurídico que se suscribirá entre la Universidad y el adjudicatario, por medio del cual se imponen a las partes obligaciones recíprocas y se conceden derechos correlativos que instrumentan la relación contractual que se busca establecer a través del presente Proceso de Contratación.
CRONOGRAMA	Es el documento en el cual la Universidad establece las fechas, horas y plazos para las actividades propias del Proceso de Contratación y el lugar en el que estas deben llevarse a cabo.
DOCUMENTOS DEL PROCESO	Son: (a) los estudios y documentos previos; (b) los términos de referencia (c) las Adendas; (e) la oferta; (f) el informe de evaluación; (g) el contrato; y cualquier otro documento expedido por la Universidad durante el Proceso de Contratación.
UNIVERSIDAD	Hace referencia a la Universidad Pedagógica Nacional
OFERTA	Es la propuesta presentada a la Universidad por los interesados en ser el contratista del Proceso de Selección objeto de los presentes Términos de Referencia.
TÉRMINOS DE REFERENCIA	Es el conjunto de normas que rigen el proceso de selección y el futuro Contrato, en los que se señalan las condiciones objetivas, plazos y procedimientos dentro de los cuales los Proponentes deben formular su oferta para participar en el Proceso de Selección del contratista y tener la posibilidad de obtener la calidad de adjudicatario del presente Proceso.
PRIMER ORDEN DE ELEGIBILIDAD	Es la posición que ocupa el Proponente según el PUNTAJE OTORGADO.
PROCESO DE SELECCIÓN O CONTRATACIÓN	Es el conjunto de actos y actividades, y su secuencia, adelantadas por la Universidad, desde la planeación hasta el vencimiento de las garantías solicitadas en el proceso.
PROPONENTE	Es la persona natural o jurídica o el grupo de personas jurídicas y/o naturales, nacionales o extranjeras, asociadas entre sí mediante las figuras de consorcio, unión temporal o promesa de sociedad futura que presenta una Oferta para participar en el Proceso de Contratación.
RIESGO	Es un evento que puede generar efectos adversos y de distinta magnitud en el logro de los objetivos del Proceso de Contratación o en la ejecución de un Contrato
RUP	Es el registro único de proponentes que llevan las cámaras de comercio y en el cual los interesados en participar en Procesos de Contratación deben estar inscritos.
SMMLV	Es el salario mínimo mensual legal vigente.

1.8. REGLAS DE SUBSANABILIDAD, EXPLICACIONES Y ACLARACIONES

El Proponente tiene la responsabilidad y deber de presentar su oferta en forma completa e íntegra, esto es, cumpliendo el contenido de los Términos de Referencia y adjuntando los documentos de soporte o prueba de las condiciones que pretenda hacer valer en el proceso.

En caso de ser necesario, la Universidad debe solicitar a los Proponentes durante el proceso de evaluación, y a más tardar en el informe de evaluación, las aclaraciones, precisiones o solicitudes de documentos que puedan ser subsanables. No obstante, los Proponentes no podrán completar, adicionar o mejorar sus propuestas en los aspectos que otorgan puntaje ni tampoco en los factores de desempate, los cuales podrán ser objeto de aclaraciones y explicaciones. Los Proponentes deberán allegar las aclaraciones o documentos requeridos en el momento en el que fueron solicitados y a más tardar en el término señalado en el cronograma del proceso de selección.

En caso de que la Universidad no hubiese advertido durante el proceso de evaluación la ausencia de requisitos o la falta de documentos referentes a la futura contratación o al Proponente, ya sea en relación con los requisitos habilitantes o para aclarar aspectos que otorgan puntaje o relacionados con los factores de desempate, y por ende no los haya requerido, podrá hacerlo posteriormente, otorgándole al Proponente un término igual al establecido para el traslado del informe de evaluación, con el fin de que los allegue. En caso de que sea necesario, la Universidad ajustará el Cronograma. Lo aquí descrito también aplicará cuando la observación a la oferta provenga de otro Proponente y se hubiere realizado en el traslado del informe de evaluación.

Las subsanaciones, explicaciones y aclaraciones se presentarán por cualquier medio: en físico, entre las horas de atención al público o por correo electrónico hasta la hora establecida en el respectivo cronograma para tal fin.

Todos aquellos requisitos de la oferta que afecten la asignación de puntaje, incluyendo los necesarios para acreditar requisitos de desempate, no son subsanables, por lo que los mismos deben ser aportados por los Proponentes desde la presentación de la oferta.

En virtud del principio de buena fe, los Proponentes que presenten observaciones al proceso o a las ofertas y conductas de los demás oferentes deberán justificar y demostrar su procedencia.

1.9. INFORMACIÓN INEXACTA

La Universidad se reserva el derecho de verificar integralmente la información aportada por el Proponente. Para esto, se puede acudir a las autoridades, personas, empresas o instituciones respectivas.

Cuando exista inconsistencia entre la información suministrada por el Proponente y la verificada por la Universidad, la información que se pretende demostrar se entenderá como no acreditada.

La Universidad remitirá copias a las autoridades competentes cuando la información aportada tenga inconsistencias sobre las cuales pueda existir una posible falsedad, sin que el Proponente haya demostrado lo contrario, y rechazará la oferta.

1.10. INFORMACIÓN RESERVADA

Si la propuesta incluye información que, conforme con la ley colombiana, tiene carácter de reservada, el Proponente debe manifestar esta circunstancia con absoluta claridad y precisión en el “Formato 1 – Carta de presentación de la oferta”, identificando el documento o información que considera que goza de reserva, citando expresamente la disposición legal que la ampara. Sin perjuicio de lo anterior, para evaluar las propuestas, la Universidad se reserva el derecho de enseñar esta información a sus funcionarios, empleados, contratistas, agentes o asesores.

En todo caso, la Universidad, sus funcionarios, sus empleados, contratistas, agentes y asesores están obligados a mantener la reserva de la información que, por disposición legal, tenga dicha calidad y que haya sido identificada por el Proponente.

1.11. MONEDA

A. Monedas Extranjeras

La propuesta de precios de las ofertas presentadas, así como la cancelación de las obligaciones pecuniarias del contrato a cargo de la administración, se hará en pesos colombianos, no se acepta propuestas en moneda diferente.

B. Conversión a Salarios Mínimos Mensuales Legales Vigentes (SMMLV):

Cuando los documentos del Proceso de Contratación señalen que un valor debe expresarse en Salarios Mínimos Mensuales Legales Vigentes (SMMLV) se seguirá el siguiente proceso:

- i. Los valores convertidos a Pesos Colombianos, aplicando el procedimiento descrito en el literal anterior, o cuya moneda de origen sea el Peso Colombiano deben convertirse a SMMLV, para lo cual emplearán los valores históricos del SMMLV señalados por el Banco de la República (<http://www.banrep.gov.co/es/mercado-laboral/salarios>), del año correspondiente a la fecha de terminación del Contrato.
- ii. Los valores convertidos a SMMLV deben ajustarse a la unidad más próxima de la siguiente forma: hacia arriba para valores mayores o iguales a cero punto cinco (0.5) y hacia abajo para valores menores a cero punto cinco (0.5).

Si el Proponente aporta certificaciones que no indican el día, sino solamente el mes y el año se procederá así:

Fecha (mes, año) de suscripción y/o inicio del Contrato: se tendrá en cuenta el último día del mes señalado en la certificación.

Fecha (mes, año) de terminación del Contrato: se tendrá en cuenta el primer día del mes señalado en la certificación.

1.12. CONFLICTO DE INTERÉS DE ORIGEN CONSTITUCIONAL O LEGAL

No podrán participar en el Proceso de Contratación y, por tanto, no serán objeto de evaluación, ni podrán ser adjudicatarios, quienes bajo cualquier circunstancia se encuentren en situaciones de Conflicto de

Interés que afecten o pongan en riesgo los principios de la Contratación Pública, de acuerdo con las causales o circunstancias previstas en la Constitución o la ley.

Tampoco podrán participar quienes hayan intervenido directa o indirectamente en la elaboración de los estudios previos y del mercado, ni en la estructuración, en cualquiera de sus etapas del presente proceso de contratación, ni quienes hayan trabajado como asesores o consultores para la elaboración de estos en los últimos dos años contados hasta la fecha de expedición del acto de apertura del presente proceso de contratación, ya sea en calidad de Funcionarios Públicos o Contratistas.

1.13. CAUSALES DE RECHAZO

Son causales de rechazo de las propuestas las siguientes:

- a. El proponente o cualquiera de los integrantes del consorcio o unión temporal, se encuentre incurso en alguna de las prohibiciones, inhabilidades, incompatibilidades o conflicto de intereses para contratar o presentar propuesta, consagradas en la Constitución Nacional o la ley.
- b. Se demuestre la participación del proponente, o de alguno de los miembros que conformen una unión temporal o consorcio, en dos o más propuestas en el mismo proceso. (Nota: se rechazarán todas las propuestas en las que aparezca el mismo participante).
- c. Que la persona jurídica Proponente Individual o integrante del Proponente Plural esté incurso en la situación descrita en el numeral 1 del artículo 38 de la Ley 1116 de 2006.
- d. Cuando al Proponente se le haya requerido con el propósito de subsanar o aclarar o aportar un documento de la propuesta y no lo efectúe dentro del plazo indicado o no lo realice correctamente o de acuerdo con lo solicitado, siempre que la subsanación, aclaración o aporte requerido sea necesario para cumplir un requisito habilitante.
- e. Que la inscripción en el Registro Único de Proponentes (RUP) que realice el Proponente por primera vez o cuando han cesado los efectos y debe volver a inscribirse, no esté en firme en la fecha prevista para el cierre del Proceso de Contratación.
- f. Que el Proponente aporte información inexacta sobre la cual pueda existir una posible falsedad.
- g. Que la Propuesta económica no se aporte firmada y no se subsane dicha omisión.
- h. No entregar la garantía de seriedad de la oferta junto con la propuesta.
- i. La propuesta se presente después de la fecha y hora exacta establecida como límite para el cierre de la presente convocatoria pública.
- j. La propuesta se presente en oficina o dependencia diferente a la indicada expresamente para el efecto, o sea enviada por correo electrónico o vía fax.
- k. Un proponente plural no presente el documento de constitución del consorcio o unión temporal.
- l. No Se presenten las autorizaciones que de conformidad con los estatutos sociales se requieran para representar y comprometer válidamente a la persona jurídica.
- m. Que el objeto social del Proponente, en caso de ser persona jurídica, o el de sus integrantes, tratándose de Proponentes Plurales, no le permita ejecutar el objeto del Contrato.
- n. Que el valor total de la oferta exceda el Presupuesto Oficial estimado para el Proceso de Contratación y no se subsane ese defecto.
- o. Presentar la oferta con tachaduras o enmendaduras en alguno de los documentos que acreditan los requisitos habilitantes o los factores de evaluación de la oferta y no estén convalidadas, sin perjuicio de la posibilidad de subsanar los primeros.

- p. Durante el período del proceso de selección y análisis de propuestas se presenten circunstancias que alteran substancialmente la capacidad operativa del proponente.
- q. Se compruebe el incumplimiento respecto a alguno o algunos de los compromisos anticorrupción relacionados en el acápite correspondiente.
- r. Cuando se presente la propuesta condicionada para la adjudicación del contrato.
- s. Presentar la oferta extemporáneamente.
- t. No presentar oferta económica y no subsanar su entrega.
- u. Cuando se determine que el valor total de la oferta es artificialmente bajo. Por esta razón la Universidad para determinar cuáles propuestas tienen precios artificialmente bajos tendrá en cuenta la “Guía para el Manejo de Propuestas Artificialmente Bajas en Procesos de Contratación” G-MOAB-01 de Colombia Compra Eficiente, que como ente rector del Sistema de Compra Pública, expidió la guía para identificar las principales características de las propuestas artificialmente bajas presentadas en los procesos de contratación y dar pautas para su manejo, en línea con las mejores prácticas internacionales en la materia”, teniendo en cuenta el artículo 25 del acuerdo 27 de 2018 de la Universidad.
- v. Cuando se presenten propuestas parciales y esta posibilidad no haya sido establecida en los Términos de Referencia.
- w. Ofrecer un plazo superior al señalado por la Universidad.
- x. Ofrecer condiciones técnicas distintas a las establecidas por la Universidad en los Términos de Referencia.
- y. Las demás previstas en la ley.

1.14. CAUSALES PARA DECLARAR DESIERTO EL PROCESO DE SELECCIÓN

La Universidad podrá declarar desierto el Proceso de Contratación cuando:

- A. Ninguna de las propuestas cumpla con los requisitos establecidos en los Términos de Referencia.
- B. Cuando no se presente ninguna propuesta.
- C. Por motivos de oportunidad o conveniencia, caso en el cual deberá sustentar las razones de dicha decisión mediante acto administrativo motivado.

1.15. NORMAS DE INTERPRETACIÓN DE LOS TÉRMINOS DE REFERENCIA

Estos Términos de Referencia deben interpretarse como un todo y sus disposiciones no deben entenderse de manera separada de lo que indica su contexto general. Por lo tanto, se considera integrada la información incluida en los documentos del proceso que lo acompañan y las adendas que se expidan.

Además, se seguirán los siguientes criterios para interpretar y entender los Términos de Referencia:

- A. El orden de los numerales, capítulos y cláusulas de estos términos no deben interpretarse como un grado de prelación entre los mismos.
- B. Los títulos de los numerales y capítulos utilizados en estos términos solo sirven como referencia y no afectan la interpretación de su contenido.
- C. Las palabras en singular se entenderán también en plural y viceversa, cuando lo exija el contexto; y las palabras en género femenino, se entenderán en género masculino y viceversa, cuando el contexto lo requiera.

- D. Los plazos en días establecidos en estos términos se entienden como hábiles, salvo que de manera expresa la Universidad indique que se trata de calendario o de meses. Cuando el vencimiento de un plazo corresponda a un día no hábil o no laboral para la Universidad éste se trasladará al día hábil siguiente.
- E. Las palabras definidas en estos Términos deben entenderse en dicho sentido.
- F. La normatividad aplicable al mismo corresponde al Acuerdo 027 de 2018 *“Por el cual se expide el estatuto de contratación de la Universidad Pedagógica Nacional”*, las, y demás normas concordantes o complementarias. Para aquellos aspectos no regulados en las normas anteriores, se aplicarán las normas comerciales y civiles pertinentes.
- G. Estos Términos de Referencia se interpretará, además, en lo pertinente, de conformidad con las reglas del Código Civil definidas en los artículos 1618 a 1624.

1.16. RETIRO DE LA PROPUESTA

Los Proponentes que entreguen su oferta antes de la fecha de cierre del proceso podrán retirarla, siempre y cuando la solicitud, efectuada mediante escrito, sea recibida por la Universidad antes de la fecha y hora del cierre. La oferta se devolverá al Proponente sin abrir, previa expedición de una constancia de recibo firmada por la misma persona que suscribió la oferta o su apoderado.

Si la propuesta es retirada después del cierre del Proceso de Selección, la Universidad debe declarar el siniestro de la Garantía de seriedad de la propuesta.

1.17. CONFIDENCIALIDAD DE LA INFORMACIÓN RELACIONADA CON DATOS SENSIBLES

Conforme el artículo 18 de la Ley 1712 del 2014 o la norma que lo modifique, aclare, adicione o sustituya, la información pública puede exceptuarse de su acceso cuando pueda causar un daño a los siguientes derechos de las personas naturales o jurídicas: el derecho a la intimidad, el derecho de toda a la persona a la vida, la salud o la seguridad y los secretos comerciales, industriales y profesionales. De acuerdo con lo anterior, la Universidad garantizará el derecho a la reserva legal de toda aquella información que acredita el cumplimiento de los factores de desempate de: **i)** mujeres víctima de violencia intrafamiliar, **ii)** personas en proceso de reincorporación y/o reintegración y **iii)** la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitanas.

Por tanto, no se publicará para conocimiento de terceros la información relacionada con los factores de desempate de personas en procesos de reincorporación o reintegración, las mujeres víctimas de violencia intrafamiliar o la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitanas, puesto que su conocimiento público afecta el derecho a la intimidad de los oferentes o de sus trabajadores o socios o accionistas.

Además, de acuerdo con el artículo 6 de Ley 1581 de 2012, o la norma que lo modifique, aclare, adicione o sustituya, se requiere que el titular de la información de estos datos sensibles, como es el caso de las mujeres víctima de violencia intrafamiliar, las personas en proceso de reincorporación o reintegración, o la población indígena, negra, afrocolombiana, raizal, palenquera, Rom o gitanas, diligencie el “Formato 5- Autorización para el tratamiento de datos personales” como requisito para el otorgamiento del criterio de desempate.

1.18. OBSERVACIONES, MODIFICACIONES Y ACLARACIONES AL CONTENIDO DE LOS TÉRMINOS DE REFERENCIA

El interesado indicará en su escrito, el número de página con su correspondiente numeral, subordinal o inciso de los Términos de Referencia sobre el cual efectúa la observación respectiva.

La Universidad analizará las inquietudes presentadas por los interesados y proponentes, y cuando dichas solicitudes impliquen modificaciones a los Términos de Referencia, éstas se harán mediante adendas numeradas que serán firmadas únicamente por el competente contractual y formarán parte os mismos, siendo de obligatorio análisis para la preparación de las propuestas.

La Universidad NO atenderá consultas personales ni telefónicas. Toda solicitud de aclaración debe presentarse por escrito y en los términos señalados en los Términos de Referencia al correo electrónico antes señalado.

La consulta y la respuesta a las observaciones formuladas por el (s) proponente(s), no producirán efecto suspensivo sobre el plazo de presentación de la propuesta.

Las consultas, preguntas y las correspondientes respuestas formarán parte de los documentos del proceso, las cuales tendrán únicamente valor interpretativo.

1.19. CIERRE DEL PROCESO Y ENTREGA DE LA PROPUESTA

En el presente proceso de selección el plazo para la presentación de las propuestas será en la fecha y hora establecida para el cierre, señalada en el correspondiente numeral que indica el “Cronograma” del proceso.

En el plazo indicado, los proponentes presentarán las propuestas, cumpliendo con las exigencias establecidas en los Términos de Referencia.

La verificación de la hora de recepción de la propuesta se efectuará en la página web <http://horalegal.inm.gov.co/>

No se aceptarán propuestas enviadas por correo o fax, o por otro medio diferente al sitio indicado para tal fin, tampoco serán recibidas ni tenidas en cuenta las que lleguen después de la hora prevista para el cierre del proceso de selección.

1.20. ORDEN DE ELEGIBILIDAD

Se establece un orden de elegibilidad de conformidad con la oferta que obtenga el mayor puntaje, siempre que se encuentre en condiciones de mercado y satisfaga las necesidades de la Universidad. De igual manera se procederá si sólo se presenta una oferta.

Si dos o más ofertas obtienen el mismo puntaje, la Universidad llevara a cabo lo establecido en el numeral 5.3. del Capítulo V, de los presentes Términos de Referencia.

1.21. VERIFICACIÓN DE LOS REQUISITOS HABILITANTES

La Universidad, a través del evaluador realizará la verificación de los requisitos mínimos habilitantes establecidos en los Términos de Referencia, para todos los proponentes.

Con base en lo anterior, el evaluador, conceptuará en cuanto al cumplimiento o no de los requisitos habilitantes exigidos en los Términos de Referencia.

1.22. ADJUDICACIÓN

Se adjudicará el proceso al oferente que obtenga el mayor puntaje y cumpla con los requisitos mínimos habilitantes (jurídicos, financieros y técnicos) exigidos en los presentes términos de referencia.

Nota Importante para la adjudicación del proceso de Selección: El proceso se adjudicará con un puntaje mínimo de **800** puntos.

La adjudicación del presente proceso se realizará a través de acto administrativo de adjudicación y se adjudicará por el valor total de la propuesta presentada la cual no podrá exceder el presupuesto oficial.

FIN DEL CAPITULO

CAPÍTULO II ELABORACIÓN, PRESENTACIÓN DE LA OFERTA Y EVALUACIÓN

2.1. ELABORACIÓN Y PRESENTACIÓN DE LA OFERTA

Las propuestas deberán estar escritas en idioma castellano, legajadas y foliadas tanto el original como las copias y deben sujetarse a cada uno de los puntos de los términos de referencia. Las propuestas deben presentarse en sobres separados en original y dos (2) copias y en medio magnético, las cuales contendrán la misma información y copia de los documentos que contenga el original. En caso de presentarse diferencias en los valores expresados en letras y en números, se tomará el valor expresado en letras, así mismo en el evento de presentarse alguna discrepancia entre el original de la propuesta y las copias, prevalecerá el original.

- El original y las dos copias deberán venir cada una dentro de un sobre, paquete o caja cerrado y rotulado con el nombre del proponente. Estos sobres deberán numerarse: original, 1ª copia y 2ª copia y dirigirse así:

UNIVERSIDAD PEDAGÓGICA NACIONAL

Carrera 16 A No. 79-08 – Piso 3 – Grupo de Contratación Bogotá D.C.

CONTRATACIÓN (indicar el objeto)

Nombre, dirección y teléfono del Proponente

- a. La presentación de la propuesta implica que el proponente analizó a cabalidad los diferentes aspectos y requisitos de este documento y las labores que le corresponde desarrollar en el evento en que sea seleccionado y que acepta todas las condiciones y obligaciones establecidas en las normas vigentes y en este documento. De las mismas formas, estarán a cargo del proponente, todos los costos asociados a la preparación, elaboración y presentación de la propuesta. Por lo tanto, la Universidad Pedagógica Nacional no reconocerá ningún reembolso por este concepto.
- b. La validez de la propuesta no podrá ser inferior a noventa (90) días calendario contados a partir de la fecha límite de cierre del proceso de contratación.
- c. No se aceptarán modificaciones con posterioridad a la fecha y hora de cierre de la CONTRATACIÓN. La Universidad podrá solicitar la aclaración de cualquier documento o afirmación efectuada por el proponente en su propuesta, en el evento en que encuentre información equívoca, confusa o aparentemente contradictoria.
- d. Estas aclaraciones se aceptarán siempre que se puedan realizar sin modificar la propuesta. En el evento en que la aclaración implique una modificación de la propuesta, no se tendrá en cuenta, previa solicitud de la Universidad.
- e. En el evento en que no se presenten, o se presenten extemporáneamente, la Universidad podrá rechazar la propuesta.
- f. La Universidad podrá solicitar a los proponentes subsanar los requisitos de la propuesta que no afectan la asignación de puntaje, y recibirlos hasta el momento de la adjudicación. Si el proponente subsana y acredita tales requisitos oportunamente, la Universidad actualizará el informe de evaluación incluyendo en la evaluación la propuesta a la cual se le había suspendido la evaluación por falta de documentos subsanables. Con base en el principio de economía y el objetivo de eficiencia del sistema de compras y contratación pública, la Universidad otorgará un término para la presentación de documentos subsanables de un (1) día, contado a partir de la comunicación mediante correo electrónico.

- g. En el ejercicio de la facultad de presentar información adicional calificada como subsanable, los proponentes no podrán completar, adicionar o modificar sus propuestas.

2.2. CIERRE DEL PROCESO Y APERTURA DE LAS OFERTAS

Se entenderán recibidas por la Universidad las ofertas que a la fecha y hora indicada en el cronograma del Proceso de Contratación se encuentren en el lugar destinado para su recepción.

No serán recibidas las ofertas que hayan sido radicadas o entregadas en otras dependencias de la Universidad.

Una vez vencido el término para presentar ofertas, la Universidad Estatal debe realizar la apertura de las ofertas, para el efecto procederá a la apertura de los sobres que contengan los documentos originales de cada propuesta en presencia de los Proponentes o veedores que deseen asistir y elaborar un acta de cierre en la cual conste:

- a) Calidad del proponente: persona jurídica, persona natural, consorcio o unión temporal
- b) Nombre del proponente.
- c) Nombre de los miembros del consorcio o de la unión temporal
- d) Numero de folios en la propuesta Original
- e) Número de copias de la Propuesta (Primera Copia, Segunda Copia)
- f) Valor Total de la propuesta incluido IVA tomado de la Propuesta Económica
- g) Garantía de seriedad de la Propuesta

En el lugar y fecha señalada, en acto público se realizará la apertura de todas las ofertas y tendrá la responsabilidad de hacerlo el Grupo de Contratación.

De lo anterior se levantará un acta que solo será suscrita por los funcionarios o Contratistas de la Universidad que intervengan en la diligencia de cierre, y los proponentes que hubiesen presenciado la apertura.

La Universidad no será responsable por abrir el Sobre incorrectamente dirigido o sin la identificación adecuada.

2.3. INFORME DE EVALUACIÓN

En la fecha establecida en el Cronograma, la Universidad publicará el informe de evaluación, el cual debe contener la evaluación de los requisitos habilitantes.

El informe de evaluación permanecerá publicado en la página web de la Universidad a disposición de los interesados, durante el término dispuesto en el respectivo cronograma del proceso de selección, término hasta el cual los Proponentes podrán hacer las observaciones que consideren procedentes y entregar los documentos y la información solicitada por la Universidad.

La Universidad debe publicará el informe final de evaluación, en caso de que el inicial hubiere sufrido variaciones, conforme a las subsanaciones a que haya lugar.

2.4. PROPUESTAS PARCIALES

No se admitirá las propuestas parciales, esto es, las presentadas para una parte del objeto o del alcance del contrato.

2.5. PROPUESTAS ALTERNATIVAS

Para este procedimiento de selección no se admite la presentación de ofertas alternativas.

FIN DEL CAPITULO

CAPITULO III DESCRIPCIÓN DEL OBJETO A CONTRATAR

3.1. OBJETO

El objeto del presente proceso de selección es:

“CONTRATAR LA ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UNA NUEVA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL (CLÚSTER DE FIREWALLS) Y DE APLICACIONES (FIREWALLS DE APLICACIONES WEB) PARA LA UNIVERSIDAD PEDAGÓGICA NACIONAL”.

3.2. REFERENTES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS - (PROFORMA No. 4 - Especificaciones Técnicas)

El oferente deberá diligenciar la **PROFORMA No. 4** en su totalidad deberá indicar **SI CUMPLE el REQUERIMIENTO, so pena de INHABILITARSE** en caso de incumplimiento y deberá indicar cómo la Universidad podrá **VERIFICAR y/o COMPROBAR** el cumplimiento de los ítems referenciados. (Folios No. Desde a hasta, ficha técnica, certificaciones, etc.).

3.3. PRESUPUESTO OFICIAL

El valor del presupuesto oficial máximo dispuesto para el presente proceso corresponde a la suma de **MIL CIENTO OCHENTA Y OCHO MILLONES CIENTO SESENTA Y SEIS MIL NOVECIENTOS NOVENTA Y UN PESOS M/CTE (\$ 1.188.166.991) M/Cte.**, incluidos todos los costos, gastos, tributos, IVA e impuestos nacionales y distritales a que haya lugar.

NOTA 1: El valor de la propuesta económica presentada por el proponente en ningún caso podrá superar el presupuesto oficial del presente proceso, so pena de rechazo de la oferta.

NOTA 2: Los oferentes son responsables de informarse e incluir en su propuesta toda tasa, retribución, impuesto o gravamen que corresponda y/o del cual sea responsable y, la Universidad, no aceptará reclamación alguna por estos conceptos.

NOTA 3: La adjudicación del presente proceso de selección se efectuará de forma **GLOBAL** y **POR EL VALOR TOTAL DE LA OFERTA ECONÓMICA PRESENTADA POR EL OFERENTE SELECCIONADO** y se ejecutará de acuerdo con los **precios unitarios fijos sin fórmula de reajuste ofertados por quien resulte seleccionado.**

NOTA 4: La propuesta económica deberá ser presentada antes de IVA, sin decimales y el valor unitario y total utilizando número entero si de acuerdo a las regulaciones tributarias colombianas aplica el IVA.

3.4. CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL

Presupuesto oficial dispuesto, se encuentran amparados con certificados de disponibilidad presupuestal que se relacionan a continuación:

CDP No.	1829	VALOR DEL CDP:	\$ 1.188.166.991
FECHA DE EXPEDICION	12 de noviembre de 2021	FECHA VIGENCIA	2021

3.5. FORMA DE PAGO

La Universidad pagará el valor de los contratos que resulten del presente proceso de selección, de la forma que a continuación se dispone, previo cumplimiento de los trámites administrativos y financieros a que haya lugar y de los siguientes requisitos, y disponibilidad PAC -Programa Anual Mensualizado de Caja:

- La Universidad efectuará un único pago al contratista de acuerdo con el lleno de los requisitos legales, entrega a satisfacción del proyecto y aprobada por el supervisor del contrato. (Los pagos se realizarán de acuerdo con la disponibilidad del PAC). Aunado a lo anterior, deberá constar la entrega del total de los equipos adquiridos objeto del presente contrato y expedición del acta de entrega y recibo a satisfacción expedido el supervisor designado por la Universidad.
- El pago igualmente requerirá de presentación de factura por el 100% del valor contratado, constancia de cumplimiento expedida por el supervisor y certificación en que conste que el PROVEEDOR se encuentra al día en el pago de aportes a seguridad social y a parafiscales, conforme a lo dispuesto en la Ley 789 de 2002
- Cobro del IVA: El Impuesto al Valor Agregado IVA debe ser calculado conforme al Estatuto Tributario vigente de acuerdo con la naturaleza de actividades a realizar en desarrollo de este contrato.

Para la procedencia del respectivo pago, el contratista deberá cumplir los siguientes requisitos:

- Formato de abono a cuenta debidamente diligenciado.
- Certificación Bancaria, con fecha de expedición no mayor a treinta (30) días, que contenga los siguientes datos:
 - Nombre o Razón Social

- Número de Nit.
 - Universidad Financiera
 - Número de cuenta
 - Tipo de cuenta (Ahorros o corriente)
3. Factura Electrónica con el cumplimiento de los requisitos señalados en los Artículos 621 y 774 del Código de Comercio y Artículo 617 del Estatuto Tributario Nacional, y demás normas específicas que rijan la materia.
 4. Certificación de paz y salvo del pago de seguridad social integral y parafiscales y obligaciones laborales. Si es U.T o Consorcio se deben anexar igualmente por cada miembro. Tratándose de personas jurídicas, se deberá acreditar el pago de los aportes de sus empleados, a los sistemas mencionados mediante certificación expedida por el revisor fiscal, cuando este exista de acuerdo con los requerimientos de ley, o en su defecto por el representante legal.
 5. Si es persona natural, aportar planilla de pago seguridad social y parafiscales; por parte del contratista de las obligaciones frente al sistema de salud, riesgos profesionales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, cuando a ello haya lugar.

NOTA 1. La Universidad no se hace responsable por las demoras presentadas en el trámite para el pago al Contratista cuando ellas fueren ocasionadas por encontrarse incompleta la documentación de soporte o no ajustarse a cualquiera de las condiciones establecidas en el presente Contrato. En atención a lo anterior, la Universidad no pagará intereses moratorios bajo ninguna circunstancia.

NOTA 2. La Universidad hará las retenciones a que haya lugar sobre cada pago, de acuerdo con las disposiciones legales vigentes sobre la materia.

NOTA 3. El futuro contratista para la acreditación del pago de seguridad social integral y parafiscales, deberá atender lo dispuesto por la Resolución No. 209 del 12 febrero de 2020, expedida por la Unidad Administrativa de Gestión Pensional y Contribuciones Parafiscales de la Protección Social – UGPP- , *Por la cual se adopta el esquema de presunción de costos para los trabajadores independientes con contratos diferentes a prestación de servicios personales, conforme a su actividad económica.*

3.6. PLAZO DE EJECUCIÓN

El plazo de ejecución de los contratos que resulten del presente proceso de selección será de **CUATRO (4) MESES**, contados a partir de la suscripción de la respectiva acta de inicio, previo cumplimiento de los requisitos de ejecución del contrato, establecidos en el Artículo 34 del Acuerdo 027 de 2018 - *Estatuto de Contratación de la Universidad Pedagógica Nacional* –

3.7. LUGAR DE EJECUCIÓN

La entrega de los bienes objeto del presente proceso, deberá efectuarse en:

INSTALACIONES	DIRECCIÓN
Subdirección de Gestión de Sistemas de Información.	Calle 72 No. 11 – 86, Bloque B - 101

3.8. OBLIGACIONES

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C. www.pedagogica.edu.co

3.8.1. Obligaciones Específicas:

1. Firmar el acta de inicio una vez se haya perfeccionado y reunido los requisitos para la ejecución del contrato de compraventa.
2. Cumplir a cabalidad con las condiciones técnicas y económicas ofertadas.
3. Efectuar la entrega de los bienes y/o elementos, de conformidad con lo establecido en las especificaciones técnicas contenidas en los Estudios y documentos previos y términos de referencia.
4. Efectuar la entrega de bienes y/o elementos nuevos, no remanufacturados y de alta calidad.
5. Contar con la logística necesaria para la entrega de los bienes
6. Garantizar la calidad de los bienes a suministrar.
7. Entregar los bienes objeto de contratación única y exclusivamente al supervisor del contrato y/o quien haga sus veces, o a quien este indique, y en el lugar indicado por este.
8. Garantizar la idoneidad de los bienes, comprometiéndose a suministrarlos en óptimas condiciones.
9. Disponer de una garantía comercial no inferior a un (1) año, contada a partir del recibo a satisfacción de los bienes.
10. Reponer, cambiar o sustituir los bienes defectuosos y los elementos que no cumplan con las especificaciones de calidad o funcionamiento requerido en un término no mayor a cuarenta y ocho (48) horas, contados a partir de la comunicación que le dirija el supervisor.
11. Entregar el manual de uso, mantenimiento y condiciones de garantía de cada uno de los elementos, dentro de los 15 primeros días después de perfeccionado el contrato.
12. Acordar de manera mancomunada con el supervisor del contrato, dentro de los cinco (5) días siguientes a la firma del acta de inicio, un cronograma de entrega de los bienes adquiridos.
13. Obrar con lealtad y buena fe, evitando dilataciones y trabas.

3.8.2. Obligaciones Generales:

1. Entregar a la Universidad la información que requieran para verificar el cumplimiento de las obligaciones laborales, de seguridad industrial y de salud ocupacional del personal empleado para cumplimiento del objeto contractual.
2. Acatar y cumplir las instrucciones que el supervisor le imparta en relación con el objeto contractual.
3. Acatar y cumplir lo dispuesto en cuanto a Normas de Seguridad y Salud en el trabajo, según lo dispuesto en, el Decreto 1072 de 2015, la Resolución 0312 de 2019, Resolución 4502 del 2012, Resolución 2404 y demás normas concordantes establecidas en la presente política.
4. Dar cumplimiento a las obligaciones con los sistemas de seguridad social, salud, pensiones y aportes parafiscales cuando haya lugar, y presentar los documentos respectivos que así lo acrediten.
5. Pagar los salarios, prestaciones sociales e indemnizaciones de todo el personal que ocupe en la ejecución del contrato, igualmente la elaboración de los subcontratos necesarios, quedando claro que no existe ningún tipo de vínculo laboral del personal con la Universidad.
6. Cumplir con todos los requisitos establecidos para pago, quedando bajo su responsabilidad el no trámite de pago de la respectiva (s) factura (s), por falta de cumplimiento total de los mismos.
7. Actualizar y/o modificar las garantías cuando a ello hay lugar.
8. Responder en los plazos que la Universidad establezca en cada caso, los requerimientos de aclaración o de información que le formule.
9. Mantener indemne a la Universidad de cualquier tipo de reclamación por parte del personal que utilice para la prestación del servicio.

10. Responder por todos los gastos, contribuciones y demás deducciones que genere la suscripción y ejecución del contrato.
11. Asistir a las reuniones que sea convocado por parte del contratante
12. Atender en forma permanente la dirección de la ejecución del objeto contractual.
13. Reportar de manera inmediata cualquier novedad o anomalía al supervisor del contrato.
14. Guardar total reserva de la información que por razón del servicio y desarrollo de sus actividades obtenga, esta es propiedad de la Universidad y está cobijada de reserva legal.
15. Constituir la garantía de cumplimiento y responsabilidad civil extracontractual dentro de un plazo no mayor de dos (02) días hábiles siguientes a la fecha de perfeccionamiento del presente contrato.

3.8.3. OBLIGACIONES DEL CONTRATISTA SEGÚN EL OBJETO DEL CONTRATO

Una vez se suscriba el contrato, el contratista estará obligado a:

- a) Suministrar dos (2) firewalls perimetrales y un (1) firewall de aplicaciones web (según especificaciones técnicas) con licenciamiento a un año.
- b) Realizar la implementación y configuración de dos firewalls perimetrales y un firewall de aplicaciones web, según la información que suministre la Universidad Pedagógica Nacional.
- c) Realizar la entrega de la documentación de toda la solución implementada y configurada.
- d) Realizar la transferencia de conocimiento y capacitación de la infraestructura implementada y configurada a los ingenieros administradores de la solución por parte de la universidad (5 Ingenieros).
- e) Realizar una visita de mantenimiento preventivo a la infraestructura implementada y configurada durante la vigencia del contrato.
- f) Realizar la entrega de la documentación referente al mantenimiento preventivo realizado.
- g) Prestar todos los servicios de mantenimiento correctivo 7x24 a que haya lugar durante la vigencia del contrato.
- h) Suministrar la matriz de escalamiento donde se indiquen como mínimo (Niveles, Roles, Áreas, Contactos, Teléfonos, Correos Electrónicos, Tiempos de Atención).
- i) Colaborar con los ingenieros administradores de seguridad de la UPN en el escalamiento y seguimiento de casos al fabricante durante la duración del contrato en caso de presentarse alguna falla de hardware, configuración y/o evaluación en la implementación de alguna nueva funcionalidad.
- j) Ejecutar el objeto del contrato en los términos acordados, incluido la, instalación, configuración y puesta en marcha de la infraestructura de seguridad perimetral (Clúster de Firewalls) y de aplicaciones (Firewalls de Aplicaciones WEB) suministrada; de todas formas, la propuesta aceptada por la Universidad hará parte integral de las obligaciones contractuales.
- k) Entregar las garantías y certificados de todos los licenciamientos de los equipos y software suministrados.
- l) Cumplir, entregar, Instalar, configurar, poner en marcha, certificar y garantizar todo lo relacionado en el numeral 3.1. REFERENTES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS de los pliegos de la presente convocatoria pública.
- m) El contratista está obligado a prestar los Servicios de Soportes, Mantenimientos o Cambios de Equipos durante el periodo de la garantía con base en lo señalado y relacionado en el ítem 3.1.

REFERENTES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS de los pliegos de la presente convocatoria pública.

NOTA: La propuesta presentada por el Contratista hará parte integral de este contrato a suscribir.

3.8.4. OBLIGACIONES EN MATERIA DE SOPORTE

Para la atención de solicitudes de soporte, el proponente deberá contar con un sistema para la gestión de incidentes y una Mesa de Ayuda para la atención de los incidentes que se puedan presentar. Se entiende por incidente cualquier solicitud de soporte que haga la UPN en relación con la prestación del servicio. A cada incidente deberá asignarle una identificación única, para realizar la gestión y trazabilidad en la atención correspondiente. Esta identificación deberá ser suministrada a la UPN al momento de la apertura del incidente.

El proveedor entregará a la UPN en medio magnético y en papel impreso una matriz de escalamiento de incidentes, indicando los nombres, cargos y teléfonos de contacto de las personas encargadas de la atención de los incidentes. Se deberá especificar en la matriz de escalamiento los tiempos de atención de los Acuerdos de Niveles de Servicio.

El proponente se compromete durante la vigencia del contrato a brindar soporte, en las siguientes modalidades:

Soporte Remoto.

Garantizar disponibilidad con respuesta inferior a cuatro (4) horas para dar soporte remoto para la solución de incidentes. Esta figura de soporte debe cubrir 7*12, es decir, siete (7) días a la semana, doce (12) horas al día.

Soporte Presencial.

Cuando la solución del incidente que se atienda por Soporte Remoto, no sea posible, cuando se presente daño físico, el Contratista enviará sus colaboradores calificados al sitio donde se encuentre alojada la solución, para atender la solicitud. Esta atención se realizará dentro de las cuatro (4) horas siguientes al reporte de la falla, reporte que podrá ser hecho telefónicamente.

El servicio de soporte y mantenimiento de incidentes con prioridad¹ 1 se deberá prestarlos siete (7) días de la semana las 24 horas.

El servicio de soporte y mantenimiento para los incidentes de prioridad 2, 3 y 4, se deberá prestar de lunes a viernes entre las ocho (8:00) horas y las dieciocho (18:00) horas, excluyendo festivos.

El servicio de atención para movimientos, adiciones y cambios (MACs) se deberá prestar de lunes a viernes entre las ocho (8:00) horas y las dieciocho (18:00) horas, para lo cual se excluyen los días festivos.

Los Acuerdos de Niveles de Servicio (ANS) se establecen de acuerdo con el impacto y la criticidad de los incidentes que se presenten con el sistema, para lo cual a continuación se realiza la siguiente clasificación:

Definición de prioridades para los incidentes

El nivel de prioridad de las incidencias se basa en los siguientes parámetros:

- Impacto: Determina la importancia del incidente dependiendo de cómo éste afecta a los



procesos de negocio de la UPN y/o del número de usuarios afectados.

- Urgencia: Rapidez con la cual debe resolverse el incidente.

De acuerdo con los eventos ocurridos se definen las prioridades tal como se muestra en la tabla siguiente:

IMPACTO	URGENCIA	PRIORIDAD
A	A	1
A	M	1
A	B	2

¹ Las definiciones de las prioridades se establecen de acuerdo con el impacto y la urgencia, esto se define más adelante.

A	S	3
M	A	1
M	M	2
M	B	2
M	S	3
B	A	1
B	M	2
B	B	3
B	S	3
S	A	2
S	M	3
S	B	4
S	S	4

Dónde:

A: Alto Impacto o Alta Urgencia

M: Medio Impacto o Media Urgencia B: Bajo Impacto o Baja Urgencia

S: Sin Impacto o Sin urgencia

La Clasificación de las prioridades se definen de Mayor a Menor, donde 1 es la más alta prioridad y 4 la más baja. A continuación, se describen los eventos que se clasifican en cada nivel de Impacto y/o Urgencia:

1. Impacto Alto

- Caída total de la Plataforma
- Indisponibilidad de la totalidad de las funcionalidades del servicio, para más del 50% de los usuarios.
- Degradación de los servicios hasta el punto de que no pueden ser utilizados.
- Intermitencias en los servicios con intervalos mayores a 1 minuto durante un periodo de 4 horas.

2. Impacto Medio

- Indisponibilidad de la totalidad de las funcionalidades del sistema para un porcentaje entre el 5% y el 49% de los usuarios.
- Degradación de los servicios, pero con disponibilidad de estos.
- Intermitencias en los servicios con intervalos menores a 5 minutos durante un periodo de 4 horas.
- Caída de la gestión de la plataforma.

3. Impacto Bajo

- a. Caída de una funcionalidad de la plataforma central sin que afecte los servicios.
- b. Indisponibilidad total o parcial de las funcionalidades que afecte menos del 5% del total de usuarios.
- c. Intermitencias en los servicios con intervalos menores a 20 minutos.

4. Sin Impacto

- a. Ningún impacto sobre el servicio de la UPN.
- b. Fallas recurrentes para las cuales es necesario programar pruebas o monitoreo a las horas en las cuales se presenta el suceso.
- c. Monitoreo sobre los servicios.
- d. Pruebas Programadas.
- e. Riesgos Potenciales. - Mantenimientos Programados.

5. Urgencia Alta

- a. Caída total o parcial de la Plataforma
- b. Caída de la conexión física entre la UPN y la plataforma Central
- c. Indisponibilidad de la totalidad de las funcionalidades del servicio para el 5% o más de los usuarios.

6. Urgencia Media

- a. Indisponibilidad para el 100% de los usuarios de por lo menos una de las funcionalidades del sistema.
- b. Indisponibilidad de la totalidad de las funcionalidades del sistema para al menos el 5% del total de los usuarios.
- c. Fallas recurrentes pero momentáneas (menores a 30 segundos) que afectan el servicio.
- d. Caída de la gestión de la plataforma.

7. Urgencia Baja

- a. Caída de una funcionalidad de la plataforma central sin que afecte los servicios.
- b. Fallas recurrentes para las cuales es necesario programar pruebas o monitoreo a las horas en las cuales se presenta el suceso.
- c. Riesgos.

8. Sin Urgencia

9. Pruebas Programadas.

10. Mantenimientos Programados.

Cuando sucedan eventos que no estén contemplados dentro de esta clasificación serán revisados entre la UPN y el Contratista para establecer el impacto y la urgencia asociados.

Tiempos De Solución

De acuerdo a las prioridades descritas en el numeral anterior se definen los siguientes tiempos de tiempo promedio de resolución de fallas:

NIVEL	TIEMPO (horas)
Prioridad 1	4
Prioridad 2	6
Prioridad 3	60
Prioridad 4	168

Mantenimientos preventivos y correctivos

Se entiende por mantenimiento preventivo cualquier actividad de mantenimiento programada por el proveedor, en la plataforma del servicio, para lo cual el proveedor notificará a la entidad con una anticipación de setenta y dos (72) horas y se llevarán a cabo, ya sea:

- en ventana de tiempo de mantenimiento preventivo de 1:00 AM a 5:00 AM de los días sábados, domingos o festivos; o,
- que sea notificada a la UPN con una anticipación de veinticuatro (24) horas y se llevarán a cabo durante una (1) hora en una ventana de tiempo de mantenimiento preventivo de 3:00 AM a 5:00 AM entre los días de lunes a viernes.

Mantenimientos preventivos y correctivos:

Se entiende por mantenimiento preventivo cualquier actividad de mantenimiento programada por el proveedor, en la plataforma del servicio, para lo cual el proveedor notificará a la entidad con una anticipación de setenta y dos (72) horas y se llevarán a cabo, ya sea: en ventana de tiempo de mantenimiento preventivo de 1:00 AM a 5:00 AM de los días sábados, domingos o festivos; y/o que sea notificada a la UPN con una anticipación de veinticuatro (24) horas y se llevarán a cabo durante una (1) hora en una ventana de tiempo de mantenimiento preventivo de 3:00 AM a 5:00 AM entre los días de lunes a viernes.

Se entiende por mantenimientos correctivos aquellos que deben ser llevados a cabo de manera inmediata y por los cuales no se notifica previamente a la UPN.

La solución ofertada por el proveedor deberá incluir soporte técnico o atención de resolución de problemas durante la vigencia del contrato y de las licencias, contado a partir de la firma del acta de inicio. Tiempo durante el cual el proveedor se obliga a suministrar ó, indicarla URL o sitio Web desde el cual se pueden descargar, los parches (patches) y actualizaciones (upgrades y updates) que el fabricante del software genere para la solución y/o sus componentes y a los cuales la UPN tendrá acceso sin costo adicional para la entidad. Manteniendo las personalizaciones que en su momento tenga la UPN. Igualmente, el proveedor realizará la(s) migración(es) correspondientes a que hubiere lugar, si la Universidad así lo aprueba.

Todos los costos generados por soporte y mantenimiento durante la ejecución del contrato estarán a cargo del contratista.

3.8.5. OBLIGACIONES EN MATERIA DE TRANSFERENCIA DE CONOCIMIENTO

El proveedor deberá realizar la transferencia de conocimiento a los colaboradores de la UPN, para lo cual deberá entregar en medio magnético e impreso un plan de transferencia de conocimiento. El Plan de Transferencia de conocimiento estará orientado de acuerdo con el perfil de usuarios así:

- a. Usuarios de infraestructura: La transferencia de conocimiento deberá realizarse para Cinco (5) Usuarios colaboradores de la Subdirección de Gestión de Sistemas de Información de la UPN.
- b. Colaboradores de la Mesa de Ayuda de la Subdirección de Gestión de Sistemas de Información: Para los colaboradores de la Mesa de Ayuda de la Subdirección de Gestión de Sistemas de Información se deberá realizar la transferencia de conocimiento para estar en capacidad de atender los requerimientos de soporte de primer nivel hechos por los usuarios de la Universidad.

Medios Digitales

Una versión en video completa y por módulos de las transferencias de conocimiento que realice el proveedor deberán ser entregados en medio magnético y formato digital de forma que puedan ser dispuestos por la UPN (según su discrecionalidad) en alguno de sus portales internos/externos para que puedan ser utilizados con posterioridad por los colaboradores de la UPN. Igualmente, se deben generar manuales de usuario final en formato digital para ser publicados por la UPN en los sitios que establezca según su discrecionalidad.

3.9. LIQUIDACIÓN DEL CONTRATO

La liquidación de mutuo acuerdo de los contratos que resulten del presente proceso de selección, se efectuará dentro de los cuatro (4) meses siguientes a la expiración del término previsto para la ejecución del contrato.

En la eventualidad que el contratista no se presente en el término antes señalado, habiéndosele requerido, o las partes no lleguen a un acuerdo sobre la misma, la Universidad procederá a liquidar unilateralmente el respectivo contrato, dentro de los dos (2) meses siguientes.

Lo anterior, en concordancia con lo dispuesto en los artículos 50 y 53 del Acuerdo 027 de 2018 - *Estatuto de Contratación de la Universidad Pedagógica Nacional* -.

3.10. SUPERVISIÓN DEL CONTRATO

La supervisión de los contratos que resulten del presente proceso de selección estará a cargo del **SUBDIRECTOR DE GESTIÓN DE SISTEMAS DE INFORMACIÓN**; quien deberá desarrollar la misma, de conformidad con lo dispuesto en el Artículo 47 del Acuerdo 027 de 2018 - *Estatuto de Contratación de la Universidad Pedagógica Nacional* -.

3.11. TIPOLOGÍA CONTRACTUAL

De conformidad con las especificaciones establecidas en el proceso y los objetos contractuales determinados, se concluye que los contratos que resulten del presente proceso de selección, se tratarán

de **CONTRATOS DE COMPRAVENTA**, por tratarse de un contrato bilateral en el que una de las partes (vendedor) se obliga a la entrega de una cosa determinada y la otra (comprador) a pagar por ella un precio cierto en dinero, no obstante que la entrega se extienda en el tiempo y los pagos se hagan conforme dicha entrega, no desnaturaliza la figura contractual, de conformidad con la definición establecida en el artículo 905 del Código de Comercio. Determinación que es concordante con lo dispuesto en el Artículo 33º del Acuerdo 027 de 2018 - *Estatuto de Contratación de la Universidad Pedagógica Nacional* -.

FIN DEL CAPITULO

CAPÍTULO IV REQUISITOS HABILITANTES Y SU VERIFICACIÓN

Los integrantes del comité evaluador realizarán la verificación de los requisitos habilitantes de capacidad jurídica, condiciones de experiencia, capacidad financiera y capacidad de organización de los proponentes de acuerdo con las competencias que les correspondan.

LA UNIVERSIDAD PEDAGÓGICA NACIONAL, verificará con el Registro Único de Proponentes el cumplimiento de los requisitos habilitantes, además se verificará con los documentos que se solicitan para aquella información adicional que no reposa en el RUP. Esta verificación se hará de acuerdo con los artículos 2.2.1.1.1.5.2 y 2.2.1.1.1.5.3 del Decreto 1082 de 2015 para determinar y verificar los requisitos habilitantes en Procesos de Contratación expedido por Colombia Compra Eficiente.

La capacidad jurídica, las condiciones de experiencia, la capacidad financiera y de organización de los proponentes serán objeto de verificación de cumplimiento como requisitos habilitantes para la participación en el proceso de selección conforme a lo señalado en el artículo 5 de la ley 1150 de 2007, en concordancia con el artículo 2.2.1.1.1.3 del decreto 1082 de 2015:

FACTOR DE EVALUACIÓN	VALORACIÓN
CAPACIDAD JURÍDICA	<i>Habilitado / No Habilitado</i>
CAPACIDAD FINANCIERA	<i>Habilitado / No Habilitado</i>
CAPACIDAD TÉCNICA Y EXPERIENCIA MÍNIMA	<i>Cumple / No Cumple</i>

NOTA: La Universidad, se reserva el derecho de corroborar la autenticidad de los datos suministrados en la propuesta, y el oferente autoriza a todas las Universidades, personas o empresas que de una u otra forma se mencionen en los documentos presentados, a suministrar la información que se requiera, a visitar sus instalaciones o a solicitar información de cualquiera de sus empleados en caso de considerarlo necesario.

4.1. REQUISITOS JURÍDICOS HABILITANTES:

Los requisitos y/o documentos de carácter jurídico que el oferente deberá allegar con su propuesta son los que se relacionan a continuación:

a. Carta de Presentación de la Oferta (FORMATO No. 1)	La Carta de Presentación de la Propuesta (Formato No. 1) deberá estar debidamente diligenciada según la información del modelo suministrado por la Universidad, <u>discriminando adecuadamente si se actúa en calidad de persona natural o como representante de la persona jurídica o representante de consorcio o unión temporal</u>, y firmada por el oferente. En caso de ser una persona jurídica, unión temporal o consorcio, deberá venir firmada por el representante legal, debidamente facultado en los términos de la ley. En la carta el oferente deberá manifestar bajo la gravedad de juramento que él o sus integrantes si el mismo es un consorcio o una unión temporal no se encuentra(n)
---	--



	incurso(s) en las causales de inhabilidades o incompatibilidades, prohibiciones o conflictos de intereses, establecidos en la Constitución Política, la Ley 80 de 1993, el artículo 18 de la Ley 1150 de 2007, Ley 1296 de 2009 y las demás normas pertinentes. La carta de presentación debe suscribirse. Con la firma de este documento se entiende que el proponente conoce y acepta el Pacto de Transparencia y, por lo tanto, no será necesaria la entrega de este documento al momento de presentar la oferta. Si la carta de presentación de la propuesta no se encuentra suscrita por el proponente, o se presenta incompleta o su contenido no está conforme a lo exigido en el Formato No. 1 anexo a los términos de referencia, la Universidad solicitará aclaración al proponente, para que dentro del plazo señale para el efecto la aporte o subsane lo pertinente. Se tendrán por no escritas las manifestaciones o condicionamientos dentro de la carta de presentación o cualquier parte de la propuesta que sean contrarias al objeto, alcance, obligaciones o especificaciones técnicas del presente proceso, no obstante, la Universidad se reserva el derecho de solicitar que se aclaren los aspectos que considere pertinentes.
b. Poder	Cuando el oferente actúe a través de apoderado deberá acreditar mediante documento legalmente expedido, con anterioridad a la presentación de la oferta, que su apoderado se encuentra facultado para presentar la oferta y, en el caso que así se considere, firmar el respectivo contrato. Si el oferente no anexa el respectivo poder o anexándolo no se ajusta a los términos legales para el efecto, la Universidad solicitará aclaración para que dentro del plazo que señale para el efecto lo aporte o subsane lo pertinente. El poder especial para representar al oferente deberá estar con nota de presentación personal, de conformidad con lo señalado en el inciso 3º del Artículo 25 del Decreto Ley 019 de 2012 y la Circular No. 17 de Colombia Compra Eficiente.
c. Autorización para Presentar Propuesta y Suscribir el Contrato	Si el representante legal del oferente o algunos de los integrantes de un consorcio, unión temporal o promesa de sociedad futura requiere autorización de sus órganos de dirección para presentar oferta y para suscribir el contrato, anexarán los documentos que acrediten dicha autorización, la cual será previa a la presentación de la oferta. Cuando el valor de la propuesta supere el monto de la autorización prevista en los estatutos para que el representante legal pueda presentar propuesta o contratar, anexará el respectivo documento donde previamente a la presentación de la



	propuesta se le faculte contratar, mínimo con el presupuesto oficial del proceso de selección. En el caso de consorcios o promesas de sociedad futura, cada uno de los representantes legales de sus miembros deberá estar facultado para contratar mínimo por la proporción en la relación con la cantidad de sus integrantes frente al presupuesto oficial. Para las uniones temporales los representantes legales deberán estar facultados para contratar mínimo en proporción a su participación en dicha unión frente al valor de la propuesta. En el evento en que no se aporte con la oferta la autorización prevista anteriormente, la Universidad solicitará al oferente allegue el documento dentro del plazo que se señale para el efecto, dicha autorización deberá ser expedida con anterioridad a la presentación de la oferta.
d. Certificado De Existencia y Representación Legal (Persona Jurídica) Expedido Por la Cámara de Comercio	El proponente PERSONA JURÍDICA, debe anexar a la propuesta, certificado de existencia y representación legal vigente, que cumpla con los siguientes requisitos: Debe ser expedido por la Cámara de Comercio o la autoridad competente. El objeto social del proponente debe permitir la actividad, gestión y operación que se solicita en este proceso. La persona jurídica proponente debe demostrar que su duración no será inferior al plazo de ejecución del contrato y treinta (30) meses más. La fecha de expedición del certificado de existencia y representación legal no podrá ser superior a treinta (30) días calendario anteriores a la fecha del cierre del proceso. Cuando el certificado de existencia y representación legal sea expedido por una Universidad diferente a la Cámara de Comercio, el proponente deberá presentar el certificado de existencia y representación legal expedido por la autoridad competente, con una fecha de expedición no superior a noventa (90) días calendario anteriores a la fecha de cierre del proceso o el que establezca el organismo regulador. Cuando el representante legal de la persona jurídica tenga restricciones para contraer obligaciones en nombre de la misma, debe anexar a la propuesta, autorización expresa del órgano social competente (Asamblea, Junta Directiva, etc.), en la que conste que el representante legal está plenamente facultado para presentar la propuesta y para comprometer la Universidad hasta por el valor de la propuesta. El documento de autorización deberá presentarse debidamente suscrito y expedido con anterioridad a la presentación de la propuesta. En el evento que el proponente sea una PERSONA NATURAL, deberá acreditar que se encuentra inscrito en el registro mercantil de la Cámara de Comercio del



	respectivo domicilio, en el cual conste que su actividad mercantil registrada es directamente relacionada con el objeto del contrato. En caso de CONSORCIOS, UNIONES TEMPORALES O PROMESA DE SOCIEDAD FUTURA conformados por personas jurídicas, cada uno de los integrantes debe presentar certificado de existencia y representación legal que cumpla con los requisitos aquí señalados. Los consorcios o uniones temporales conformados por personas naturales cada uno de los integrantes deberá acreditar que se encuentra inscrito en el registro mercantil de la Cámara de Comercio del respectivo domicilio que cumpla con los requisitos señalados en el presente numeral. Cuando el proponente sea una PERSONA JURÍDICA EXTRANJERA sin domicilio en Colombia y no tenga establecida sucursal en Colombia, debe presentar el documento que acredite la inscripción de la personería jurídica en el Registro correspondiente del país donde tenga su domicilio principal, así como los documentos que acrediten su existencia y representación legal debidamente apostillados, en la forma como lo establece la Ley 455 de 1998. Adicionalmente, deberá acreditar un apoderado domiciliado en Colombia, debidamente facultado para presentar la propuesta y celebrar el contrato, así como para representarla judicial o extrajudicialmente. En el evento de resultar favorecido un proponente extranjero sin domicilio ni sucursal en Colombia, para poder ejecutar el contrato deberá previamente constituir una sucursal en Colombia. A través de este se verificará, según sea el caso: 1.VIGENCIA DE LA SOCIEDAD 2.FACULTADES DEL REPRESENTANTE LEGAL. 3.OBJETO SOCIAL NOTA: La fecha de expedición del certificado de existencia y representación legal o del Registro Mercantil si es el caso, no podrá ser superior a treinta (30) días calendario
e. Fotocopia De La Cedula de Ciudadanía	En caso de que la propuesta sea presentada por persona jurídica o persona natural se debe anexar la fotocopia legible de la cédula de ciudadanía del Representante Legal, de la persona natural o apoderado, según corresponda.
f. Documento de Conformación de Proponente Plural (FORMATO No. 2)	En el evento que la propuesta sea presentada en Consorcio o Unión Temporal deberá adjuntar con su propuesta debidamente diligenciado para cada caso en particular el documento de conformación del Consorcio o la Unión Temporal.



	Para lo cual el proponente plural deberá allegar debidamente diligenciado el FORMATO No. 2 NOTA: En la eventualidad de allegarse de manera incompleta, confusa, sin el lleno de los requisitos aquí establecidos, se requerirá al proponente para que lo complete, adiciones y/o observe la totalidad de los aspectos allí señalados.
g. Certifica do de Pago de Seguridad Social y Aportes Legales (FORMATO No. 3)	1. PERSONAS JURÍDICAS El Proponente persona jurídica debe presentar el “Formato 3 – Pagos de seguridad social y aportes legales” suscrito por el revisor fiscal, de acuerdo con los requerimientos de ley, o por el representante legal, bajo la gravedad del juramento, cuando no se requiera revisor fiscal, en el que conste el pago de los aportes de sus empleados a los sistemas de salud, riesgos laborales, pensiones y aportes a las cajas de compensación familiar, al Instituto Colombiano de Bienestar Familiar y al Servicio Nacional de Aprendizaje, cuando a ello haya lugar. La Universidad no exigirá las planillas de pago. Bastará el certificado suscrito por el revisor fiscal, en los casos requeridos por la ley, o por el representante legal que así lo acredite. Cuando la persona jurídica esté exonerada de estas obligaciones en los términos previstos en el artículo 65 de la Ley 1819 de 2016, debe indicarlo en el “Formato 5 – Pagos de seguridad social y aportes legales”. Esta misma previsión aplica para las personas jurídicas extranjeras con domicilio o sucursal en Colombia las cuales deben acreditar este requisito respecto del personal vinculado en Colombia. 2. PERSONAS NATURALES El Proponente persona natural debe acreditar la afiliación a los sistemas de seguridad social en salud y pensiones, aportando los certificados de afiliación respectivos acompañados de las planillas de pago de los últimos seis (06) meses anteriores a la fecha de cierre del proceso. Los certificados de afiliación a salud y pensión deben presentarse con fecha de expedición no mayor a treinta (30) días calendario anteriores a la fecha de cierre del Proceso de Contratación. En caso de modificarse la fecha de cierre del Proceso de Contratación, se tendrá como referencia para establecer el plazo de vigencia de los certificados de afiliación la originalmente fijada en los términos de referencia. La persona natural que reúna los requisitos para acceder a la pensión de vejez, o se pensione por invalidez o anticipadamente, presentará el certificado que lo acredite y además la afiliación al sistema de salud.



	Esta misma previsión aplica para las personas naturales extranjeras con domicilio en Colombia las cuales deberán acreditar este requisito respecto del personal vinculado en Colombia. 3. PROPONENTES PLURALES Cada uno de los integrantes del Proponente Plural debe cumplir con la acreditación del requisito según aplique a su naturaleza jurídica.
h. Verificación De No Inclusión en el boletín de responsables Fiscales	En cumplimiento a lo previsto en el Artículo 60 de la Ley 610 de 2000, las Resoluciones Orgánicas No. 5149 de 2000 y 5677 de 2005, y a la Circular No.05 del 25 de febrero de 2008 de la Contraloría General de la República, la Universidad verificará que los proponentes no se encuentren reportados en el último boletín de responsables fiscales que expide la Contraloría General de la República. El artículo 60 de la Ley 610 de 2000, por medio del cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías, exige como requisito indispensable para nombrar, dar posesión o celebrar cualquier tipo de contrato con el Estado, verificar que la correspondiente persona natural o jurídica, según se trate, no se encuentra reportada en el boletín de responsables fiscales que publica la Contraloría General de la República con periodicidad trimestral.
i. Verificación del SIRI (Sistema de Registro de Sanciones e Inhabilidades)	De conformidad con lo previsto en el Artículo 1 de la Ley 1238 de 2008, y con el fin de verificar los antecedentes disciplinarios, la Universidad, realizará la consulta de los antecedentes disciplinarios del oferente o de cada uno de los miembros del consorcio o unión temporal, según sea el caso.
j. Verificación De Antecedentes Judiciales – Policía Nacional	De conformidad con lo previsto en el artículo 94 del Decreto Ley 0019 de 2012 y con el fin de verificar los antecedentes judiciales del oferente (persona natural o representante legal de persona jurídica o consorcio o unión temporal), la Universidad, accederá a los mismos a través de la página web de la Policía Nacional. En caso de que el oferente persona natural o representante legal de la persona jurídica o del consorcio o unión temporal, según el caso, registre antecedentes judiciales consistentes en sentencia judicial condenatoria con pena accesorias de interdicción de derechos y funciones públicas, la propuesta será rechazada.
k. Verificación del Registro Nacional de Medidas Correctivas	De conformidad con lo previsto en los Artículos 183 y 184 de la Ley 1801 del 29 de julio de 2016 (Código Nacional de Policía y Convivencia) y con el fin de verificar el pago de las multas establecidas en la mencionada Ley, la Universidad realizará e imprimirá la consulta en línea que genere el Registro Nacional de Medidas Correctivas para el efecto.
	El proponente deberá aportar su identificación tributaria e información sobre el régimen de impuestos al que pertenece, adjuntando para tal efecto, copia del



I. Registro Único Tributario – RUT	Registro Único Tributario – RUT ACTUALIZADO con el código QR, de conformidad con el nuevo formato de la DIAN. Las personas jurídicas directamente, o como integrantes de un consorcio o unión temporal, deberán acreditar este requisito (RUT), cuando intervengan como responsables del Impuesto sobre las Ventas (IVA), por realizar directamente la prestación de servicios gravados con dicho impuesto Lo anterior, de conformidad con lo dispuesto en los artículos 368 y siguientes, 555-2 y siguientes del Estatuto Tributario, en concordancia con el artículo 66 de la Ley 488 de 1998, que adicionó el artículo 437 del mismo Estatuto y el Decreto Reglamentario N.º 2788 de 2004 y Resolución 139 de 2012 de la DIAN. Para las sociedades extranjeras sin domicilio en Colombia, deberán anexar el documento equivalente en su país de residencia haciendo mención clara y expresa de la norma que para tal efecto los rige.
m. Certificación Vigente de su Inscripción y Clasificación en el Registro Único De Proponentes de la Cámara de Comercio – RUP	El proponente (Personas naturales o jurídicas nacionales o extranjeras naturales con domicilio en Colombia o extranjeras jurídicas con sucursal en Colombia) deberá presentar con su oferta el Certificado de Inscripción y Clasificación en el Registro Único de proponentes expedido por la respectiva Cámara de Comercio. Este certificado no deberá tener una fecha de expedición superior a noventa (90) días calendario. En el certificado se verificará, que el Proponente no tenga reportes sobre multas o sanciones en relación con contratos de compraventa suscritos con Universidades oficiales o privadas que lo inhabiliten para celebrar el contrato que se deriva del presente proceso de contratación. NOTA 1. La inscripción del proponente debe encontrarse en firme y vigente para el momento de la adjudicación del proceso. <i>Si a la fecha de presentación de la oferta, el RUP del proponente no se encuentra en firme, deberá acreditar que solicitó su renovación oportunamente, sin perjuicio que al vencimiento del término de traslado de los informes de evaluación y consolidado, el RUP, deba encontrarse en firme.</i> NOTA 2: La firmeza de la inscripción se adquiere pasados diez (10) días hábiles siguientes a la publicación sin que se haya presentado recurso de reposición en contra de la información inscrita.



n. Garantía
de Seriedad de la
Propuesta y
Recibo de Pago

El Proponente debe presentar con la propuesta una **Garantía de seriedad** de la propuesta que cumpla con los siguientes parámetros, condiciones y requisitos:

Cualquier error o imprecisión en el texto de la Garantía presentada será susceptible de aclaración por el Proponente hasta el término de traslado del informe de evaluación.

Las características de las Garantías son las siguientes:

Característica	Condición
Clase	Contrato de seguro contenido en una póliza
Asegurado/ beneficiario	UNIVERSIDAD PEDAGÓGICA NACIONAL, Universidad pública con régimen privado de contratación, identificada con NIT. 899.999.124- 4
Objeto	La garantía deberá señalar expresamente el objeto del presente proceso de selección.
Amparos	La sanción derivada del incumplimiento del ofrecimiento en los eventos señalados en el numeral 3 del Artículo 45° del Acuerdo 027 de 2018 - Estatuto de Contratación de la Universidad Pedagógica Nacional -
Vigencia	Tres (3) meses contados a partir de la fecha de cierre del Proceso de Contratación.
Valor Asegurado	Diez por ciento (10 %) del presupuesto oficial.
Tomador	• Para las personas jurídicas: la Garantía deberá tomarse con el nombre o razón social y tipo societario que figura en el certificado de existencia y representación legal expedido por la Cámara de Comercio respectiva, y no sólo con su sigla, a no ser que en el referido documento se exprese que la sociedad podrá denominarse de esa manera. • Para los Proponentes Plurales: la Garantía deberá ser otorgada por todos los integrantes del Proponente Plural, para lo cual se deberá relacionar claramente los integrantes, su identificación y porcentaje de participación, quienes para todos los efectos serán los otorgantes de esta.

Si en desarrollo del Proceso de Contratación se modifica el Cronograma, el Proponente deberá ampliar la vigencia de la Garantía de seriedad de la oferta hasta tanto no se haya perfeccionado y cumplido los requisitos de ejecución del respectivo Contrato.



La propuesta tendrá una validez igual al término de vigencia establecido para la Garantía de seriedad de la propuesta. Durante este período la propuesta será irrevocable, de tal manera que el Proponente no podrá retirar ni modificar los términos o condiciones de la misma, so pena de que la Universidad pueda hacer efectiva la Garantía de seriedad de la oferta.

Sin perjuicio de la correspondiente verificación que podrá, en uso de sus facultades, efectuar la Universidad.

Alcance del Amparo y Contenido Obligatorio de la Garantía de seriedad de la Propuesta.

De conformidad con lo establecido en el numeral 3 del artículo 45 del Acuerdo 027 de 2018 - *Estatuto de Contratación de la Universidad Pedagógica Nacional* -, la garantía de seriedad de las propuestas amparará a la Universidad de las sanciones imputables al proponente derivadas del incumplimiento de las obligaciones establecidas en los términos de referencia y/o estudios previos.

Esta garantía la hará efectiva, cuando ocurra alguno de los siguientes eventos:

La no ampliación de la vigencia de la garantía de seriedad de la oferta cuando el plazo para la Adjudicación o para suscribir el contrato es prorrogado, siempre que tal prórroga sea inferior a tres (3) meses.

El retiro de la oferta después de vencido el plazo fijado para la presentación de las ofertas.

La no suscripción del contrato sin justa causa por parte del adjudicatario.

La falta de otorgamiento por parte del proponente seleccionado de la garantía de cumplimiento del contrato.

4.2. REQUISITOS HABILITANTES FINANCIEROS:

CAPACIDAD FINANCIERA	1. IDENTIFICACIÓN TRIBUTARIA ACTUALIZADA El proponente deberá indicar su identificación tributaria e información sobre el régimen de impuestos al que pertenece, adjuntando para tal efecto, copia del Registro Único Tributario – RUT ACTUALIZADO con el código QR, de conformidad con el nuevo formato de la DIAN. Las personas jurídicas directamente, o como integrantes de un consorcio o unión temporal, deberán acreditar este requisito (RUT), cuando intervengan como responsables del Impuesto sobre las Ventas (IVA), por realizar directamente la prestación de servicios gravados con dicho impuesto Lo anterior, de conformidad con lo dispuesto en los artículos 368 y siguientes, 555-2 y siguientes del Estatuto Tributario, en concordancia con el artículo 66 de la Ley 488 de 1998, que adicionó el artículo 437 del mismo Estatuto y el Decreto Reglamentario N.º 2788 de 2004 y Resolución 139 de 2012 de la DIAN. Para las sociedades extranjeras sin domicilio en Colombia, deberán anexar el documento equivalente en su país de residencia haciendo mención clara y expresa de la norma que para tal efecto los rige. 2. REGISTRO ÚNICO DE PROPONENTES- CAPACIDAD FINANCIERA El proponente deberá presentar el Certificado de Registro Único de Proponentes actualizado con información de estados financieros y con información en firme, con una fecha de expedición máxima de noventa (90) días calendario a la fecha de presentación de la propuesta y conforme a lo establecido en el Decreto 579 del 2021. En el certificado se verificará (ítem de la capacidad financiera) que el proponente cumpla con los indicadores financieros requeridos en los presentes términos de referencia. Únicamente las sociedades extranjeras sin domicilio en Colombia, deben presentar para registro la información contable y financiera de su casa matriz. Los estados financieros de las sociedades extranjeras deben ser presentados de conformidad con las normas aplicables en el país en el que son emitidos. Estos Estados Financieros deben ser del corte anual más reciente según lo dispongan las normas de origen. Estos estados deben estar acompañados de sus notas y del informe de auditor externo dependiendo el país. Nota: Cuando la propuesta sea presentada por Consorcio o Unión Temporal deberán adjuntarse los documentos financieros de cada uno de sus integrantes, como si se fuera a presentar en forma independiente.
------------------------------------	--

	Índice de liquidez El proponente debe tener una liquidez mayor o igual a 1.24. En caso contrario, la propuesta será calificada como NO HABILITADA. Se evaluará con la siguiente fórmula: $LIQ. = AC / PC > 0 = (1,24)$ Donde, LIQ. = Índice de liquidez. AC= Activo corriente. PC= Pasivo corriente. Para los consorcios o uniones temporales la liquidez de cada socio se afectará por el porcentaje de participación de cada socio. Para las sociedades extranjeras sin domicilio en Colombia, se tendrá en cuenta la información de los EEFF con el corte anual más reciente según lo dispongan las normas de origen. Estos estados deben estar acompañados de sus notas y del informe de auditor externo dependiendo el país. Índice de endeudamiento El nivel de endeudamiento debe ser menor o igual al 70 %. En caso contrario la propuesta será calificada como NO HABILITADA. Para calcular este índice se aplicará la siguiente fórmula: $E = Pasivo Total / Activo Total \leq 70\%$ Para los consorcios o uniones temporales el capital de trabajo de cada socio se afectará por el porcentaje de participación de cada socio. Para las sociedades extranjeras sin domicilio en Colombia, se tendrá en cuenta la información de los EEFF con el corte anual más reciente según lo dispongan las normas de origen. Estos estados deben estar acompañados de sus notas y del informe de auditor externo dependiendo el país.
--	---

4.3. REQUISITOS TÉCNICOS HABILITANTES:

Los requisitos y/o documentos de carácter técnico y experiencia, que el oferente deberá allegar con su propuesta son los que se relacionan a continuación, los cuales deberán aportarse en su totalidad para valorarse como CUMPLE.



a. Verificación de Especificaciones Técnicas Mínimas Exigidas (Formato No. 4)	El oferente acreditará que los bienes y/o servicios ofrecidos cumplen con las especificaciones técnicas exigidas, para cual DEBERÁ DILIGENCIAR Y PRESENTAR CON SU OFERTA EL FORMATO DENOMINADO “ESPECIFICACIONES TÉCNICAS”. La información contenida en este Formulario o formato, NO DEBERÁ SER MODIFICADA por el oferente, debido a que corresponden a las especificaciones técnicas exigidas por la Universidad, y, por ende, SON DE OBLIGATORIO CUMPLIMIENTO. Si el oferente no presenta el formato con su propuesta, o si incluyéndolo, no contiene la totalidad de la información solicitada, la Universidad requerirá al proponente a fin de que subsane lo correspondiente dentro del plazo que se señale para el efecto.								
b. Experiencia (FORMATO No.7)	Se verificará la experiencia del proponente en la celebración y ejecución de máximo tres (3) contratos cuyo objeto corresponda o esté relacionado con el de esta convocatoria, ejecutados en los últimos 4 años anteriores a la fecha del cierre del presente proceso de selección cuya sumatoria sea igual o superior al 100% del presupuesto oficial representado en SMMLV. Además, el respectivo contrato, deberá contemplar todos los códigos del Clasificador de Bienes y Servicios (UNSPSC) en el tercer nivel, que se relacionan a continuación: <table border="1" data-bbox="610 1075 1341 1266"><thead><tr><th>CODIGO UNSPC</th><th>CLASE</th></tr></thead><tbody><tr><td>43233200</td><td>SOFTWARE DE SEGURIDAD Y PROTECCIÓN</td></tr><tr><td>43222500</td><td>EQUIPO DE SEGURIDAD DE RED</td></tr><tr><td>43222600</td><td>EQUIPO DE SERVICIO DE RED</td></tr></tbody></table> REGLAS PARA LA VALORACIÓN DE LA EXPERIENCIA DE CONSORCIOS, UNIONES TEMPORALES O PROMESA DE SOCIEDAD FUTURA: Los proponentes plurales deberán tenerse en cuenta los siguientes criterios: Regla de Proporcionalidad: Cuando la propuesta se presente en consorcio o unión temporal, o promesa de sociedad futura, deberá acreditar la experiencia de acuerdo con el porcentaje de participación en la figura asociativa (expresada en SMLMV).	CODIGO UNSPC	CLASE	43233200	SOFTWARE DE SEGURIDAD Y PROTECCIÓN	43222500	EQUIPO DE SEGURIDAD DE RED	43222600	EQUIPO DE SERVICIO DE RED
CODIGO UNSPC	CLASE								
43233200	SOFTWARE DE SEGURIDAD Y PROTECCIÓN								
43222500	EQUIPO DE SEGURIDAD DE RED								
43222600	EQUIPO DE SERVICIO DE RED								



NOTA 1: El proponente plural debe cumplir con el 100% de los requisitos exigidos en la experiencia del proponente, es decir es obligatorio que cada uno de los integrantes acredite experiencia.

JUSTIFICACIÓN DE LA REGLA DE PROPORCIONALIDAD:

Se justifica la regla de proporcionalidad establecida por la Universidad, en consideración a que todos los integrantes de una figura asociativa deberán ostentar experiencia que permita verificar la idoneidad del futuro contratista en la ejecución de proyectos con alcances similares al contratado. Lo anterior, tiene con fundamento legal responsabilidad solidaria de todas y cada una de las obligaciones derivadas de la propuesta y del contrato, consagrada en el artículo 7 de la Ley 80 de 1993.

Así mismo, conforme lo prevé el artículo 5 de la ley 1150 de 2007, la exigencia de tales condiciones debe ser adecuada y proporcional a la naturaleza del contrato a suscribir y a su valor, pues como se expresó, es necesario contar con proponentes que acrediten experticia en la ejecución de contratos como el requerido por la UPN situación que conllevó a establecer la regla de proporcionalidad, a efectos que de forma equitativa y conforme a cada figura asociativa que se cree, atendiendo a un criterio objetivo de participación los integrantes de las mismas aúnen esfuerzos y garanticen en la ejecución del contrato el conocimiento y la experticia de cualquiera de los mismos para lograr su éxito en los tiempos y las condiciones técnicas previstas.

La anterior regla tiene como sustento jurisprudencial en la posibilidad de fijar límites al número de participantes o de fijar reglas para determinar su capacidad real o material, SALA DE LO CONTENCIOSO ADMINISTRATIVO, SECCIÓN TERCERA, consejera Ponente: MARÍA ELENA GIRALDO GÓMEZ, Radicación N° 73001-23-31-000-1997-04707- 02(15188).

Nota 1: Para el caso de contratos que sean aportados por socios de empresas que no cuentan con más de tres (3) años de constituidas, en caso de ser necesario se deberá aportar adicional a los documentos válidos para la acreditación de experiencia, un documento debidamente suscrito por el representante legal y el revisor fiscal o contador público (según corresponda), donde se indique la conformación societaria de la empresa, y los respectivos contratos acreditados, los cuales deben estar inscritos en el RUP de cada socio.

LA Universidad se reserva el derecho de verificar durante la evaluación y hasta la adjudicación la información aportada por el



	proponente, así como la información que reposa en la cámara de comercio u otras plataformas públicas y solicitar los soportes que considere convenientes tales como: certificaciones, copias de los contratos, facturas de venta, copia de los medios de pago, actas suscritas, actas de liquidación, estados financieros, copia de pago de impuestos o cualquier otro documento. La verificación de esta experiencia, se efectuará de conformidad con la información relacionada en el FORMATO No. 6.
c. Otros requisitos técnicos habilitantes	La oferta presentada por el proponente deberá cumplir con las especificaciones técnicas mínimas exigidas, por lo tanto, el proponente deberá entregar CERTIFICACIÓN DE ACEPTACIÓN Y CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS, mediante la cual acredita el cumplimiento de lo mínimo exigido en cada uno de los ítems relacionado en el numeral 3.1, REFERENTES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS - (PROFORMA No. 4 - Especificaciones Técnicas) . Sin embargo, las respuestas deberán ser soportadas para su comprobación en la columna ¿Cómo se Verifica?, cuando el requerimiento del ítem lo exija. El proponente deberá entregar la FICHA TÉCNICA DEL FABRICANTE de todos y cada uno de los equipos y productos suministrados.

FIN DEL CAPITULO

CAPITULO V

CRITERIOS DE EVALUACIÓN DE LAS OFERTAS Y CRITERIOS DE DESEMPATE

LA UNIVERSIDAD debe evaluar únicamente las Ofertas de los Proponentes que hayan acreditado los requisitos habilitantes solicitados.

La Universidad asignará el siguiente puntaje:

ITEM	CRITERIO DE EVALUACIÓN	MÁXIMO PUNTAJE
1	FACTOR ECONÓMICO – VALOR DE LA PROPUESTA	400
2	FACTOR TECNICO – VALORES AGREGADOS	600
	TOTAL	1000

5.1 FACTOR ECONÓMICO – VALOR DE LA OFERTA – PUNTAJE (400 PUNTOS)

La Universidad otorgará el máximo puntaje por este concepto (hasta 400 puntos), a la propuesta que, cumpliendo con la totalidad de requisitos habilitantes exigidos, ofrezca el menor precio total.

Sobre esta base se calificarán a las demás ofertas en forma proporcional, aplicando regla de tres inversas. Solo para este ítem.

Los proponentes deberán diligenciar la Proforma No. 7. Los valores de la propuesta deberán presentarse en pesos colombianos que deben cubrir todos los costos directos e indirectos derivados de la prestación del servicio. El IVA se deberá detallar de manera tal que refleje los productos que están o no exentos de este impuesto

Los proponentes deberán presentar como parte de su propuesta, una Propuesta Económica en los términos y condiciones descritos en los presentes Términos de Referencia. Para este fin, el proponente deberá diligenciar y adjuntar el formato “Propuesta Económica”.

Deberá diligenciar y adjuntar el valor de los precios unitarios ofertados (Antes de IVA) para cada uno de los ítems establecidos y las cantidades ofertadas, en el formato Excel “PROPUESTA OFERTA ECONÓMICA” fijado por LA UNIVERSIDAD.

A partir del Valor de la SUMATORIA DE UNITARIOS de la Pregunta “OFERTA ECONÓMICA” de los oferentes habilitados, se aplicará una de las metodologías establecidas por la UNIVERSIDAD (ver 5.3.2) escogida aleatoriamente a partir de los primeros dos dígitos decimales de la TRM que rija el día hábil posterior a la fecha en que se adelante el cierre del proceso, la cual será el parámetro de asignación del puntaje de acuerdo con el procedimiento establecido para cada metodología.

5.3.1. Verificación

Previo a la aplicación de la metodología seleccionada, la “OFERTA ECONÓMICA” presentada por los proponentes será objeto de verificación por el equipo evaluador del cumplimiento de los siguientes requisitos:

- Deben presentarse en moneda legal colombiana.
- El formato “Oferta Económica” debe estar totalmente diligenciado con el Valor Unitario Ofertado para todos los ítems que ofrece.
- La sumatoria de los Valores unitarios ofertados para cada uno de los ítems no pueden exceder el presupuesto oficial para el presente proceso y deben ser mayor a cero pesos (\$0).

Nota 1. La Universidad no aceptará ofertas parciales, por lo tanto, los proponentes deberán diligenciar completamente la totalidad de los ítems que ofrece.

Nota 2. No se aceptarán ofertar con ítems con un valor de cero “\$0”.

Nota 3. Para la presentación de la “PROPUESTA ECONÓMICA” no se deben utilizar centavos; por lo tanto, los valores unitarios y el valor total Ofertado deben presentarse en números enteros. En el evento en que la Oferta cuente con valores que contengan centavos, se aproximará al siguiente peso si los centavos son iguales o superiores a 50, o en caso contrario se mantendrá el mismo entero.

Nota 4. La presentación de la propuesta constituye una manifestación explícita de que el Proponente ha efectuado un estudio completo de la documentación que compone el presente proceso de contratación,

el objeto a contratar, precios, plazos, especificaciones técnicas, económicas y/o financieras, condiciones de ejecución del contrato y demás elementos que influyan directa e indirectamente durante la ejecución del contrato sobre el valor de su oferta; por lo tanto, el Proponente debe proyectar el Valor de su “PROPUESTA ECONÓMICA” de forma responsable y serán de la exclusiva responsabilidad del Proponente, los errores en que incurra al indicar los valores unitarios y totales en su propuesta debiendo asumir los mayores costos o pérdidas que se deriven de dichos errores.

Nota 5. Cualquier error en la determinación de los valores unitarios ofertados no dará lugar a su modificación, con excepción de las aproximaciones por uso de centavos (redondeo) que realice LA UNIVERSIDAD. El Proponente deberá asumir los valores unitarios y totales corregidos por la entidad, los cuales harán parte del contrato que se suscriba.

Nota 6. La(s) propuesta(s) económica(s) deberá(n) contemplar todos los costos directos e indirectos, impuestos, tasas y contribuciones de ley y cualquier otra erogación necesaria para la correcta suscripción y ejecución del objeto de la presente contratación y por ningún motivo se considerarán costos adicionales.

Nota 7. (Los) precio(s) ofertado(s), no estará(n) sujeto(s) a ajuste alguno, razón por la cual, el proponente deberá prever en su oferta que debe asumir los posibles incrementos que se ocasionen, inclusive aquellos que se presenten en la ejecución del contrato por cambio de año.

Nota 8. El valor de la Sumatoria de los precios Unitarios Ofertados resultado del diligenciamiento del Formato “PROPUESTA ECONÓMICA”, debe ser igual que el valor diligenciado en la CARTA DE PRESENTACIÓN DE LA PROPUESTA. En caso de que estos valores no coincidan, la UNIVERSIDAD tomará para efectos de la evaluación económica el valor contenido en el Formato “PROPUESTA ECONÓMICA”.

5.2 FACTOR TÉCNICO – VALORES AGREGADOS – PUNTAJE (600 PUNTOS)

La Universidad otorgará el máximo puntaje por este concepto (hasta 600 puntos), a la propuesta que, cumpliendo con la totalidad de requisitos exigidos, ofrezca mayor valor agregado en el suministro de los Bienes con los estándares de calidad reconocidos en el sector.

PUNTAJES ASIGNADOS A LOS VALORES AGREGADOS (Proforma No. 6)

ITEM	CRITERIOS DE EVALUACIÓN PARA VALORES AGREGADOS	PUNTOS ASIGNADOS
1	Ofrecer una solución de administración de los firewalls por aparte con un appliance dedicado. Por mejores prácticas de implementación es siempre mejor tener la capa de protección separada de la capa de administración lo cual mejorara notablemente el rendimiento y performance de las comunicaciones, y segundo permitirá la continuidad de negocio, es decir, en caso de que la consola de administración falle, no se interrumpen las comunicaciones; si falla la consola de administración los firewalls siguen trabajando normalmente.	200
2	Ofrecer una solución de SOC, donde se realice un monitoreo	150

	en tiempo real de los equipos implementados durante la duración del contrato, para de esta manera ser lo más proactivo posibles ante cualquier fallo y/o error que se pueda presentar en la infraestructura ofertada	
3	Dar curso para dos personas de certificación de la solución dictado directamente por el fabricante, incluido el Voucher para la presentación del examen de certificación	150
4	Dar curso de la solución para cinco (5) personas de la entidad dictado fuera de las instalaciones de la universidad por un ente certificado por el fabricante con entrega de certificado de asistencia	50
5	Transferencia de conocimiento y sensibilización de la norma ISO27000 y ISO27001 a los funcionarios de la unidad de sistemas de la UPN realizado en las instalaciones de la universidad (Aproximadamente 20 personas)	50
NOTA	Si no ofrece valor agregado el puntaje será de Cero (0) en el ítem correspondiente	0
	TOTAL	600

En la evaluación se tendrán en cuenta los aspectos anteriormente definidos y se asignarán los puntajes respectivos según ofrecimiento.

5.1. PROPUESTA ECONÓMICA

El oferente debe presentar su propuesta, conforme se indica en la Proforma No. 7 “**PROPUESTA ECONOMICA**”, de los presentes términos de referencia, proforma que es de obligatorio diligenciamiento, por lo que el proponente que no diligencie será calificado como **rechazado**.

Dentro del valor de la oferta el proponente debe contemplar todos los gastos necesarios para la ejecución del contrato, todos los gastos e impuestos a que hay lugar (salvo el IVA que se calcula automáticamente), servicios agregados del oferente y demás gastos que deba incurrir para el desempeño del objeto del contrato.

LA SUMATORIA DE LOS PRECIOS UNITARIOS Y SU CORRESPONDIENTE CANTIDAD NO PODRÁN SUPERAR EL PRESUPUESTO OFICIAL DETERMINANDO POR LA UNIVERSIDAD SO PENA DE RECHAZO DE LA OFERTA.

La oferta no podrá estar condicionada, ni ser adicionada, modificada o completada después de haber sido presentada.

5.2. ÚNICO OFERENTE

Si sólo se presenta una oferta para, se le adjudicará el contrato siempre y cuando la misma cumpla con los requisitos habilitantes y la propuesta económica se ajuste a los valores unitarios y/o presupuesto oficial, según aplique.

5.3. CRITERIOS DE DESEMPATE

La Universidad Estatal debe utilizar las siguientes reglas de forma sucesiva y excluyente para seleccionar el oferente favorecido de conformidad con lo establecido en el artículo 35 de la Ley 2069 de 2020 así:

1. Preferir la oferta de bienes o servicios nacionales frente a la oferta de bienes o servicios extranjeros.

Este requisito se acreditará con la presentación del formato de Apoyo a la Industria Nacional.

2. Preferir la propuesta de la mujer cabeza de familia, mujeres víctimas de la violencia intrafamiliar o de la persona jurídica en la cual participe o participen mayoritariamente; o, la de un proponente plural constituido por mujeres cabeza de familia, mujeres víctimas de violencia intrafamiliar y/o personas jurídicas en las cuales participe o participen mayoritariamente.

El proponente deberá acreditar dicha condición mediante, según corresponda:

- Declaración juramentada ante notario de la mujer que acredite su condición de cabeza de familia, junto con la copia de los documentos de idUniversidad de la mujer que acredite alguna de las condiciones referidas.
- Medida de protección expedida por el Comisario de Familia, o el Juez (en caso de que en el lugar no exista comisario), o la autoridad indígena – en los casos de violencia intrafamiliar en las comunidades de esta naturaleza –, junto con la copia de los documentos de Universidad de la mujer que acredite alguna de las condiciones referidas.
- Certificación del representante legal y/o revisor fiscal en los casos en que la sociedad esté obligada a tenerlo, en la que conste que más del 50% de la participación accionaria o cuota parte son de titularidad de género femenino. Adicionalmente, deberá acreditar la condición indicada de cada una de las mujeres que participen en la sociedad, aportando copia de los documentos de Universidad de cada una de ellas.

Finalmente, en el caso de los Proponentes plurales, se preferirá la oferta cuando cada uno de los integrantes, si se trata de persona natural, acredite que más del 50% son mujeres sobre las cuales recaiga alguna de las condiciones arriba señaladas; si se trata de integrante persona jurídica este debe acreditar que se encuentra constituida mayoritariamente por mujeres sobre las cuales recaiga alguna de las condiciones ya mencionadas. La Universidad Estatal compradora deberá solicitarle al proponente la autorización expresa del titular de la información, relacionada con el tratamiento de datos sensibles de conformidad con lo establecido en artículo 6 de la Ley 1581 de 2012.

3. Preferir la propuesta presentada por el oferente que acredite en las condiciones establecidas en la ley que por lo menos el diez por ciento (10%) de su nómina está en condición de discapacidad a la que se refiere la Ley 361 de 1997. Si la oferta es presentada por un proponente plural, el integrante del oferente que acredite que el diez por ciento (10%) de su nómina está en condición de discapacidad en los términos del presente numeral, debe tener una participación de por lo

menos el veinticinco por ciento (25%) en el consorcio, unión temporal o promesa de sociedad futura y aportar mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta.

El proponente deberá acreditar que en su nómina se encuentra al menos el diez por ciento (10%) de trabajadores en situación de discapacidad de la siguiente manera:

Anexar el certificado expedido por el Ministerio de Trabajo, el cual deberá estar vigente a la fecha de cierre del proceso de contratación. Si la propuesta es presentada por un consorcio o unión temporal, el integrante del proveedor plural deberá acreditar que el diez por ciento (10%) de su nómina está en condición de discapacidad en los términos del presente numeral, y tener una participación de por lo menos el veinticinco por ciento (25%) en el consorcio o unión temporal y aportar mínimo el veinticinco por ciento (25%) de la experiencia habilitante.

Para efectos de lo anterior, deberá revisarse el documento de constitución en el SECOP II con el fin de verificar el porcentaje de participación de sus integrantes.

En este caso el proponente, en los términos del párrafo 2 del artículo 35 de la Ley 2069 de 2020, deberá adicionalmente acreditar mediante certificación suscrita por el representante legal y/o revisor fiscal que el personal referido ha sido contratado por lo menos con un (1) año de anterioridad a la fecha de cierre del proceso de contratación o desde el momento de la constitución de la persona jurídica y que certifique adicionalmente que mantendrá dicho personal por un lapso igual al término de ejecución de la orden de compra.

4. Preferir la propuesta presentada por el oferente que acredite la vinculación en mayor proporción de personas mayores que no sean beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de edad de pensión establecido en la Ley.

El Proponente a través del representante legal y/o revisor fiscal deberá certificar bajo la gravedad de juramento el número de personas mayores que hayan cumplido el requisito de edad de pensión y que no sean beneficiarios de la pensión de vejez que se encuentren vinculadas por contrato laboral o contrato de prestación de servicios. Solo se tendrá en cuenta la acreditación de aquellas personas mayores que hayan cumplido el requisito de edad de pensión, y que hayan estado vinculadas con una anterioridad igual o mayor a un año de la fecha de cierre del proceso de contratación.

Para los casos de constitución inferior a un año se tendrá en cuenta a aquellos que hayan estado vinculados desde el momento de la constitución de la persona jurídica.

En el caso de los proponentes plurales, el representante del mismo deberá certificar el número de personas mayores que no sean beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de edad de pensión establecido en la Ley, vinculadas por cada uno de sus integrantes, o por la unión temporal o consorcio; junto con los documentos de identificación de cada uno de las personas vinculadas.

La mayor proporción se definirá en relación con el número total de personas mayores que no sean beneficiarios de la pensión de vejez vinculadas por contrato laboral o contrato de prestación de servicios, por lo que se preferirá al Proponente que acredite un porcentaje mayor.

5. Preferir la propuesta presentada por el oferente que acredite, en las condiciones establecidas en la ley, que por lo menos diez por ciento (10%) de su nómina pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitanas.

El Proponente deberá anexar la copia de la certificación expedida por el Ministerio del Interior en la cual acredite que el trabajador pertenece a la comunidad indígena, comunidades negras, afrocolombianas, raizales, palenqueras, Rrom o gitanas en los términos del Decreto 2893 de 2011, o la norma que lo modifique, sustituya o complemente.

Adicionalmente, se deberá adjuntar el certificado expedido por el representante legal y/o el revisor fiscal de la persona jurídica según corresponda, o el proponente persona natural acredite que al menos el 10% de su nómina pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rom o gitanas. Y la copia de los documentos de identificación de población indígena, negra, afrocolombiana, raizal, palanquera, Rom o gitanas con la cual se pretende acreditar esta condición.

En el caso de los proponentes plurales, el representante legal del mismo certificará que por lo menos diez por ciento (10%) del total de la nómina de sus integrantes pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rom o gitanas. Este porcentaje se definirá de acuerdo con la sumatoria de la nómina de cada uno de los integrantes del Proponente plural. En todo caso, deberá aportar la copia de la certificación expedida por el Ministerio del Interior en la cual acredite que el trabajador pertenece a la comunidad indígena, comunidades negras, afrocolombianas, raizales, palenqueras, Rom o gitanas en los términos del Decreto 2893 de 2011, o la norma que lo modifique, sustituya o complemente.

Debido a que, para el otorgamiento de este criterio de desempate se entregan certificados que contienen datos sensibles, de acuerdo con el artículo 6 de la Ley 1581 de 2012, se requiere autorización por parte del titular del dato como es el caso de las personas que pertenecen a la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitanas; el proveedor deberá anexar la autorización para el tratamiento de datos personales como requisito para el otorgamiento del criterio de desempate.

6. Preferir la propuesta de personas en proceso de reintegración o reincorporación o de la persona jurídica en la cual participe o participen mayoritariamente; o, la de un proponente plural constituido por personas en proceso de reincorporación, y/o personas jurídicas en las cuales participe o participen mayoritariamente.

El Proponente deberá acreditar copia de alguno de los siguientes documentos:

1. La certificación en las desmovilizaciones colectivas que expide la Oficina de Alto Comisionado para la Paz,
2. El certificado que expida el Comité Operativo para la Dejación de las Armas respecto de las personas desmovilizadas en forma individual. Además, se entregará el documento de identificación de la persona en proceso de reintegración o reincorporación.
3. U otro documento que para el efecto determine las autoridades competentes.

En el caso de las personas jurídicas, el representante legal y/o revisor fiscal certificará bajo la gravedad de juramento que más del 50% de la composición accionaria o cuotas partes de la persona jurídica está constituida por personas en proceso de reintegración o reincorporación. Además, deberá aportar alguno

de los certificados del inciso anterior, junto con los documentos de identificación de cada una de las personas que están en proceso de reincorporación o reintegración.

Debido a que, para el otorgamiento de este criterio de desempate se entregan certificados que contienen datos sensibles, de acuerdo con el artículo 6 de la Ley 1581 de 2012, se requiere autorización por parte del titular del dato. El proveedor deberá anexar autorización para el tratamiento de datos personales como requisito para el otorgamiento del criterio de desempate.

Tratándose de proveedores plurales, se preferirá la oferta cuando cada uno de los integrantes acredite alguna de las condiciones señaladas en los incisos anteriores de este numeral.

7. Preferir la oferta presentada por un proponente plural siempre que: (a) esté conformado por al menos una madre cabeza de familia y/o una persona en proceso de reincorporación o reintegración, o una persona jurídica en la cual participe o participen mayoritariamente, y, que tenga una participación de por lo menos el veinticinco por ciento (25%) en el proponente plural; (b) la madre cabeza de familia, la persona en proceso de reincorporación o reintegración, o la persona jurídica aporte mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta; y (c) ni la madre cabeza de familia o persona en proceso de reincorporación o reintegración, ni la persona jurídica, ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural.

El proponente plural deberá acreditar la condición de madre cabeza de familia y/o persona en proceso o situación de reintegración o reincorporación o que ostenten esta condición para lo cual deberá tener en cuenta la totalidad de las siguientes condiciones:

En todos los casos, la mujer cabeza de familia, o, la persona reincorporada o reinsertada, no podrá ejercer u ostentar la calidad de accionista, socio, empleado o representante legal en más de uno de los integrantes de la figura asociativa oferente.

Adicionalmente, deberá adjuntar declaración juramentada de la mujer que invoque la condición de cabeza de familia; y/o la persona en proceso de reintegración o reincorporación deberá anexar certificación expedida por el Comité Operativo para la Operación de las Armas -CODA, o la Oficina del Alto Comisionado para la Paz, conforme el Registro Nacional de Reincorporación, a través de la cual se acredite su inclusión en los programas de reincorporación, conforme lo establecido en el Decreto 1081 de 2015.

Una vez lo anterior, el Proponente podrá optar por las siguientes alternativas según corresponda:

- a) O, adjuntar certificación del representante legal y/o revisor fiscal en los casos en que la sociedad esté obligado a tenerlo, en la que conste que al menos el 25% de participación accionaria en la respectiva sociedad son de titularidad de género femenino y/o persona en proceso de reincorporación o reintegración o que ostente tal calidad.
- b) O, mediante documento de conformación de la figura asociativa, con fundamento en el cual, según el porcentaje de participación del integrante, se evidencie que la experiencia aportada por la madre cabeza de familia o la persona en proceso de reincorporación o reintegración o calidad de tal, sea no inferior al 25% del total acreditado en la oferta.

8. Preferir la oferta presentada por una Mipyme o cooperativas o asociaciones mutuales; o un proponente plural constituido por Mipymes, cooperativas o asociaciones mutuales.

El Proponente deberá acreditar en la forma indicada a continuación, según corresponda:

- a) Mipymes: El proveedor deberá acreditarlo mediante el Certificado de Existencia y Representación Legal,
- b) Cooperativas o Asociaciones se acreditará mediante el certificado de existencia y representación legal expedido por la Cámara de Comercio.

Tratándose de proveedores plurales, se preferirá la oferta cuando cada uno de los integrantes acredite alguna de las condiciones señaladas en el inciso anterior de este numeral.

9. Preferir la oferta presentada por el proponente plural constituido por micro y/o pequeñas empresas, cooperativas o asociaciones mutuales.

El Proponente plural deberá acreditar en la forma indicada a continuación, según corresponda:

- a) Para las empresas micro y/o pequeñas empresas: El proponente deberá acreditarlo mediante el Certificado de Existencia y Representación Legal,
- b) Cooperativas o Asociaciones se acreditará mediante el certificado de existencia y representación legal expedido por la Cámara de Comercio.

Tratándose de proponentes plurales, se preferirá la oferta cuando cada uno de los integrantes acredite alguna de las condiciones señaladas en el inciso anterior de este numeral.

10. Preferir al oferente que acredite de acuerdo con sus estados financieros o información contable con corte a 31 de diciembre del año anterior, por lo menos el veinticinco por ciento (25%) del total de pagos realizados a MIPYMES, cooperativas o asociaciones mutuales por concepto de proveeduría del oferente, realizados durante el año anterior; o, la oferta presentada por un proponente plural siempre que: (a) esté conformado por al menos una MIPYME, cooperativa o asociación mutual que tenga una participación de por lo menos el veinticinco por ciento (25%); (b) la MIPYME, cooperativa o asociación mutual aporte mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta; y (c) ni la MIPYME, cooperativa o asociación mutual ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural.

El proponente deberá acreditar los pagos con corte a 31 de diciembre del año inmediatamente anterior realizados a MIPYMES para lo cual, el Proponente deberá tener en cuenta la totalidad de las siguientes condiciones:

En todos los casos, la MIPYME, cooperativa o asociación mutual, sus accionistas, socios o representantes legales, no podrán ejercer u ostentar la calidad de accionista, socio, empleado o representante legal en más de uno de los integrantes de la figura asociativa oferente. Para acreditar la calidad de MIPYME, Cooperativa o Asociación Mutual:

Si se trata de Mipymes: El Proponente deberá acreditarlo mediante: el Certificado de Existencia y Representación Legal, y o Si se trata de Cooperativas o Asociaciones se acreditará mediante el certificado de existencia y representación legal expedido por la Cámara de Comercio.

Una vez lo anterior, el Proponente podrá optar por las siguientes alternativas en orden de precedencia para lograr el desempate:

- a) O, adjuntar certificación del representante legal y/o revisor fiscal en los casos en que la sociedad esté obligado a tenerlo, en la que conste, con corte a 31 de diciembre del año anterior, los pagos en al menos un 25% en favor de Cooperativas, Mipymes o Asociaciones Mutuales por concepto de ejecución de contratos celebrados en el marco del orden legal.

Para el efecto anterior, el oferente deberá allegar sus estados financieros o información contable con fundamento en la cual se evidencia la información requerida. Adicionalmente, deberá aportar el documento que acredite que el receptor del pago es en efecto una cooperativa, Mipymes o Asociaciones Mutuales. Este requisito podrá ser sustituido por la consulta que hagan las Universidades en las correspondientes bases de datos, de lo cual, deberán dejar constancia.

- b) O, mediante documento de conformación de la figura asociativa y sus modificaciones, con fundamento en el cual, según el porcentaje de participación del integrante, se evidencie el que la experiencia aportada por la Cooperativas, Mipymes o Asociaciones Mutuales, sea no inferior al 25% del total acreditado en la oferta.

- 11. Preferir las empresas reconocidas y establecidas como Sociedad de Beneficio e Interés Colectivo o Sociedad BIC, del segmento MIPYMES.

El Proponente del segmento Mipymes deberá acreditar mediante el certificado de existencia y representación legal de la sociedad, en el cual conste que reúne los requisitos del artículo 2 de la Ley 1901 de 2018, conforme el cual: "Tendrán la denominación de sociedades BIC todas aquellas compañías que sean constituidas de conformidad con la legislación vigente, las cuales además del beneficio e interés de sus accionistas, actuarán en procura del interés de la colectividad y del medio ambiente".

- 12. El Proponente Utilizar un método aleatorio para seleccionar el oferente, método que deberá haber sido previsto previamente en los Documentos del Proceso:

Si el empate se mantiene, se procederá a adjudicar al que haya presentado la oferta en primer lugar entre los empatados y que no haya tenido lugar a subsanaciones, según el orden de presentación reportado en el acta de cierre. En caso de que todas las propuestas hayan tenido lugar a subsanación, se adjudicará a la que haya subsanado en primer lugar.

Este resultado es aceptado de antemano por los interesados involucrados en el empate sin lugar a reclamación alguna.

Nota: Para efectos de la aplicación de los criterios de desempate, los proponentes deberán aportar con su propuesta, los documentos que de acuerdo con las disposiciones legales acrediten dichas circunstancias. Por tal razón, para efectos de dar aplicación de los factores de desempate se efectuará la verificación con base en los documentos aportados dentro de la propuesta y hasta el cierre del proceso.

NOTA 1. La acreditación de cumplimiento de cualquiera de las reglas de desempate deberá aportarse con la presentación de la propuesta, junto con los requisitos para acreditar la capacidad técnica.

FIN DEL CAPITULO

CAPITULO VI RIESGOS ASOCIADOS AL PROCESO DE SELECCIÓN Y EL CONTRATO

La Universidad efectúa la evaluación de los riesgos previsible, de conformidad con lineamientos y directrices efectuadas por Colombia Compra Eficiente mediante manual para la identificación y cobertura del riesgo (Versión M-ICR-01), en concordancia con lo dispuesto en el parágrafo del Artículo 13° del Estatuto de Contratación de la Universidad Pedagógica Nacional, así:

N	Clase	Fuente	Etapas	Tipo	Descripción	Consecuencia De La Ocurrencia Del Evento	Probabilidad	Impacto	Valoración del Riesgo	Categoría	¿A Quién Se Le Asigna?	Tratamiento/Control A Ser Implementado	Impacto Después Del Tratamiento				¿Afecta La Ejecución Del Responsable Por	Fecha Estimada En Que Se Inicia El Tratamiento	Fecha Estimada En Que Se Completa El Tratamiento	Monitoreo Y Revisión		
													Probabilidad	Impacto	Valoración	Categoría				¿Cómo Se Realiza El Monitoreo?	Periodicidad	
1	General	Interno	Planeación	Económico	Falta de experiencia necesaria para la prestación del servicio	Incumplimiento de las obligaciones del contrato	3	5	8	Extremo	Universidad -Contratista	Solicitar los requisitos necesarios que acrediten experiencia en la prestación del servicio	1	1	2	Bajo	No	Universidad	En la estructuración del proceso	Con la suscripción del contrato	Establecer los requisitos idóneos que demuestren la capacidad financiera del contratista	Durante la estructuración del proceso
2	General	Interno	Selección	Operacional	No existen oferentes habilitados para el proceso de selección	Declaratoria del desierto del proceso de selección	3	5	8	Extremo	Universidad	Desarrollar un adecuado análisis de la oferta del sector	2	5	7	Alto	Si	Universidad	En la estructuración del proceso	Con la aceptación de la oferta	Analizando adecuadamente el mercado, de modo que se identifique claramente los posibles	Durante la estructuración del proceso

6	Externo	Externo	Ejecución	Operacional	Modificación de las especificaciones técnicas	Deficiente calidad de los bienes parte del objeto contractual	1	1	2	Bajo	Contratista	Solicitud de Garantía de calidad de los bienes	1	1	2	Bajo	Si	Supervisor	A Partir De La Suscripción Del Contrato	Plazo de ejecución del contrato	Informe de supervisión	Mensual	
5	General	Externo	Ejecución	Operacional	Incumplimiento Total o Parcial de las Obligaciones	Incumplimiento del Objeto Contractual	2	2	4	Bajo	Contratista	Solicitud de Garantía De Cumplimiento	2	2	4	Bajo	Si	Supervisor	A Partir De La Suscripción Del Contrato	Plazo de ejecución del contrato	Informe De Supervisión	Mensual	
4	Específico	Externa	Ejecución	Financiero	Falta de fluidez económica para cumplir con el objeto contractual	Incumplimiento del Objeto Contractual	3	4	7	Alto	Contratista	Solicitud de capital de Trabajo	1	2	3	Bajo	Si	Universidad	En la estructuración del proceso	Plazo de ejecución del contrato	Con la verificación de los requisitos habilitantes	Durante la estructuración y evaluación del proceso	
3	Específico	Externo	Ejecución	Operacional	Suministros de mala calidad	Inadecuada atención de la necesidad	3	5	8	Extremo	Contratista	Verificación de los bienes por parte del supervisor y solicitud de garantía que ampare la calidad de los bienes	3	5	8	Extremo	Si	Contratista – Universidad	A Partir De La Suscripción Del Contrato	Plazo de ejecución del contrato	Solicitud o y aprobando la garantía que ampare el riesgo	Una única vez a la suscripción del contrato	

CAPÍTULO VII GARANTÍAS QUE SE EXIGIRÁN EN EL PROCESO DE CONTRATACIÓN

7.1. GARANTÍA DE SERIEDAD DE LA PROPUESTA

El Proponente debe presentar con la propuesta una Garantía de seriedad de la oferta que cumpla con los parámetros, condiciones y requisitos que se indican en este numeral.

Cualquier error o imprecisión en el texto de la Garantía presentada será susceptible de aclaración por el Proponente durante el término que establece el cronograma del proceso de selección.

Las características de las Garantías son las siguientes:

Característica	Condición
Clase	Contrato de seguro contenido en una póliza
Asegurado/ beneficiario	UNIVERSIDAD PEDAGÓGICA NACIONAL, Universidad pública con régimen privado de contratación, identificada con NIT. 899.999.124-4
Objeto	La garantía deberá señalar expresamente el objeto del presente proceso de selección.
Amparos	La sanción derivada del incumplimiento del ofrecimiento en los eventos señalados en el numeral 3 del Artículo 45º del Acuerdo 027 de 2018 - Estatuto de Contratación de la Universidad Pedagógica Nacional -
Vigencia	Tres (3) meses contados a partir de la fecha de cierre del Proceso de Contratación.
Valor Asegurado	Diez por ciento (10 %) del presupuesto oficial.
Tomador	• Para las personas jurídicas: la Garantía deberá tomarse con el nombre o razón social y tipo societario que figura en el certificado de existencia y representación legal expedido por la Cámara de Comercio respectiva, y no sólo con su sigla, a no ser que en el referido documento se exprese que la sociedad podrá denominarse de esa manera. • Para los Proponentes Plurales: la Garantía deberá ser otorgada por todos los integrantes del Proponente Plural, para lo cual se deberá relacionar claramente los integrantes, su identificación y porcentaje de participación, quienes para todos los efectos serán los otorgantes de esta.

Si en desarrollo del Proceso de Contratación se modifica el Cronograma, el Proponente deberá ampliar la vigencia de la Garantía de seriedad de la oferta hasta tanto no se haya perfeccionado y cumplido los requisitos de ejecución del respectivo Contrato.

La propuesta tendrá una validez igual al término de vigencia establecido para la Garantía de seriedad de la oferta. Durante este período la propuesta será irrevocable, de tal manera que el Proponente no podrá retirar ni modificar los términos o condiciones de la misma, so pena de que la Universidad pueda hacer efectiva la Garantía de seriedad de la oferta.

7.2. GARANTÍAS DEL CONTRATO

Para cubrir cualquier hecho constitutivo de incumplimiento, el contratista deberá presentar la Garantía de cumplimiento en original a la Universidad dentro de los tres (03) días hábiles siguientes contados a partir de la firma del Contrato y requerirá la aprobación de la Universidad. Esta garantía tendrá las siguientes características:

Características	Condición		
Clase	Contrato de seguro contenido en una póliza		
Asegurado/ beneficiario	UNIVERSIDAD PEDAGÓGICA NACIONAL, Universidad pública con régimen privado de contratación, identificada con NIT. 899.999.124-4		
Objeto	La garantía deberá señalar expresamente el objeto del presente proceso de selección.		
Amparos, vigencia y valores asegurados	Amparo	Vigencia	Valor Asegurado
	pago de salarios, prestaciones sociales e indemnizaciones laborales	Por el termino de ejecución del contrato y tres años más	diez por ciento (10%) sobre el valor del contrato
	Cumplimiento del Contrato	Plazo del contrato y seis (6) meses más	Treinta por ciento (30%) sobre el valor total del contrato
	Calidad y Correcto Funcionamiento de los Bienes y Equipos Suministrados	Plazo del Contrato y UN (1) año más	Veinte por ciento (20%) del valor total contrato
	Calidad del servicio	Plazo del contrato y seis (6) meses más	Treinta por ciento (30%) sobre el valor total del contrato
Tomador	• Para las personas jurídicas: la Garantía deberá tomarse con el nombre o razón social y tipo societario que figura en el Certificado de Existencia y Representación Legal expedido por la Cámara de Comercio respectiva, y no sólo con su sigla, a no ser que en el referido documento se exprese que la sociedad podrá denominarse de esa manera. • No se aceptan Garantías a nombre del representante legal o de alguno de los integrantes del Consorcio o la Unión Temporal. Cuando el Contratista sea una Unión Temporal o Consorcio, se debe incluir la razón social, el NIT y el porcentaje de participación de cada uno de los integrantes. • Para el Contratista conformado por una estructura plural (Unión temporal, Consorcio), la Garantía deberá ser otorgada por todos los integrantes del Contratista, para lo cual se deberá relacionar claramente los integrantes, su identificación y porcentaje de participación, quienes para todos los efectos serán los otorgantes de la misma.		

Características	Condición
Información necesaria dentro de la póliza	• Número y año del Contrato • Objeto del Contrato • Firma del representante legal del Contratista • En caso de no usar centavos, los valores deben aproximarse al mayor Ej. cumplimiento si el valor a asegurar es \$14.980.420,20 aproximar a \$14.980.421

FIN DEL CAPITULO

CAPÍTULO VIII LISTADO DE ANEXOS, FORMATOS

8.1. ANEXOS

1. Anexo 1 –Cronograma
2. Anexo 2 –Pacto de Transparencia

8.2. FORMATOS

1. PROFORMA No.1 – MODELO DE CARTA DE PRESENTACIÓN DE LA PROPUESTA (junto con sus anexos)
2. PROFORMA No.2 – Conformación de proponente plural
3. PROFORMA No.3 – Pagos de seguridad social y aportes legales
4. PROFORMA No.4 – Especificaciones Técnicas
5. PROFORMA No.5 – Experiencia
6. PROFORMA No.6 – Valores Agregados
7. PROFORMA No.7 - Propuesta Económica

ANEXO No. 1 CRONOGRAMA DEL PROCESO

ACTIVIDAD	Fecha y hora	LUGAR
Expedición de Resolución de Apertura de la convocatoria pública.	Viernes 26 de noviembre de 2021	Página web de la Universidad Pedagógica Nacional
Publicación de los términos de referencia de la Convocatoria Pública en la página Web de la	Viernes 26 de noviembre de 2021	Página web de la Universidad Pedagógica Nacional



Universidad.		
Publicación de los Términos de Referencia de la Convocatoria Pública en un diario de circulación nacional	Viernes 27 de noviembre de 2021	Diario de alta circulación
Envío de autorización para la Audiencia de Aclaración de los Términos de Referencia	Lunes 29 de noviembre de 2021 Hasta las 3:00 pm El representante legal debe enviar mediante correo electrónico la autorización para participar máximo dos apoderados de la empresa en la audiencia virtual. La carta de autorización debe relacionar nombres completos, número de cédula, número de celular, nombre de la empresa proponente, sea consorcio, unión temporal, persona jurídica o persona natural y correo electrónico al cual se realizará la citación de la audiencia virtual.	Estas deben enviarse al correo electrónico: procesosdeseleccion@pedagogica.edu.co
Audiencia de Aclaración de los Términos de Referencia	Fecha: miércoles 1 de diciembre de 2021 Hora: 4:00 pm Organizar por la aplicación Microsoft Teams	Virtual a través de la plataforma Microsoft Teams
Fecha límite para presentación de observaciones	viernes 3 de diciembre de 2021 hasta las 3:00 pm	Estas deben enviarse al correo electrónico: procesosdeseleccion@pedagogica.edu.co
Respuestas a las observaciones de los términos de referencia,	Lunes 6 de diciembre de 2021	Página web de la Universidad Pedagógica Nacional
Plazo de presentación de las ofertas	La recepción de ofertas será únicamente el jueves 9 de diciembre de 2021 en horario de 10:00 am a 2:00 p.m. Nota: Solo se recibirán las propuestas que estén completas, <u>es decir Un original, dos (2) copias y un CD.</u>	Carrera 16 A No.79- 08 Primer Piso, Administrativa UPNBogotá..

	Nota: El CD debe contener toda la propuesta presentada en medio físico, así mismo los archivos del CD deben tener seguridad para evitar la edición	
Apertura de Urna	Jueves 9 de diciembre de 2021 a 2:15 p.m. Únicamente podrá asistir una persona por proponente y debe cumplir con el protocolo de bioseguridad para el ingreso a las instalaciones el cual se puede consultar en: http://protocolodebioseguridad.upn.edu.co/	Lugar: Grupo de Contratación (Carrera 16 A No.79-08 Piso Tercero).
Informe de evaluación de propuestas. Publicado en la página web de la Universidad.	martes 14 de diciembre de 2021	Página web de la Universidad Pedagógica Nacional
Plazo para presentar observaciones al informe de evaluación. procesosdeseleccion@pedagogica.edu.co	Jueves 16 de diciembre de 2021 Hasta: las 3:00 pm	Estas deben enviarse al correo electrónico: procesosdeseleccion@pedagogica.edu.co
Respuestas a observaciones de las evaluaciones, en la página Web de la Universidad.	lunes 20 de diciembre de 2021	Página web de la Universidad Pedagógica Nacional
Expedición y publicación del acto de administrativo adjudicación	martes 21 de diciembre de 2021	Página web de la Universidad Pedagógica Nacional
Firma del Contrato	Dentro de los tres (3) días hábiles siguientes a la adjudicación	Por medio de correo electrónico

Cuadro No. 4 cronograma

Nota 1. Los términos antes señalados podrán prorrogarse, antes de su vencimiento, siempre que las necesidades de la Universidad lo exijan. Esto a través del correo electrónico.

Nota 2. En caso de requerirse expedir adendas, éstas se enviarán al correo electrónico hasta el día hábil anterior a la fecha programada para efectuar el cierre del proceso.

ANEXO No. 2

PACTO DE TRANSPARENCIA

Este documento hace parte integral de los documentos del proceso y con la firma de la carta de presentación de la propuesta el Proponente se compromete a:

- a. Cumplir estrictamente la ley aplicable.
- b. Interpretar de buena fe las normas aplicables a los Procesos de Contratación de manera que siempre produzcan los efectos buscados por las mismas.
- c. No incurrir en faltas a la verdad o adulteración en los documentos o requisitos exigidos en el Proceso de Contratación.
- d. Aceptar que durante la evaluación de las propuestas del Proceso de Contratación primen los aspectos de fondo por encima de la forma, buscando siempre favorecer la libre competencia.
- e. Hacer un estudio completo del proyecto y de los documentos del Proceso de Contratación, así como realizar estudios y análisis propios con la debida diligencia y responsabilidad, a fin de contar con los elementos de juicio e información económica, comercial, jurídica y técnica relevante y necesaria para tomar una decisión sustentada para presentar la propuesta. Lo anterior, con el propósito de que la misma sea seria y honesta, de tal manera que me permita participar en el Proceso de Contratación y en caso de resultar adjudicatario cumplir todas las obligaciones contenidas en el contrato y asumir los riesgos asociados a la ejecución de este.
- f. No hacer arreglos previos, concomitantes o posteriores al Proceso de Contratación con los encargados de planear el proceso para tratar de conocer, influenciar o manipular la información del proyecto y presentar la respectiva propuesta.
- g. No hacer arreglos previos, concomitantes o posteriores al Proceso de Contratación, con otros Proponentes para tratar de influenciar o manipular los resultados de la adjudicación.
- h. Enviar por escrito a la Universidad todas las preguntas o inquietudes que surjan durante el Proceso de Contratación y no hacerlo de manera oral por ningún medio, salvo que se realicen dentro de las audiencias públicas.
- i. Actuar con lealtad hacia los demás Proponentes y con la Universidad y abstenernos de utilizar herramientas para dilatar o sabotear el Proceso de Contratación. Igualmente, las observaciones al Proceso de Contratación o a las Propuestas de los otros interesados serán presentadas oportunamente, en los plazos y términos fijados estrictamente en el Pliego de Condiciones.
- j. Abstenerse de hacer manifestaciones orales o escritas en contra de los demás Proponentes y sus propuestas sin contar con evidencia, material probatorio o indicios sólidos, que razonablemente permitan considerar que existe un acto irregular, de competencia desleal o de corrupción por parte

- de ellos. En caso de tener las pruebas, material probatorio o indicios, estos se dejarán a inmediata disposición de la Universidad o de las autoridades competentes para corroborar tales afirmaciones.
- k. En las audiencias guardar compostura, no levantar la voz y hacer uso de la palabra únicamente cuando sea concedida y por el tiempo establecido y acatar las decisiones de la Universidad. En caso de desacuerdo interponer los recursos o acciones que se consideren pertinentes en los términos de la ley aplicable.
 - l. En las audiencias, abstenerse de proferir juicios de valor contra personas naturales o jurídicas, ni referirse a asuntos personales de otros Proponentes. Por lo tanto, en las audiencias solamente se debatirán asuntos relacionados con el Proceso de Contratación.
 - m. Solicitar o remitir a la Universidad o a sus funcionarios y contratistas cualquier información utilizando solamente los procedimientos y canales previstos en el Proceso de Contratación.
 - n. No ofrecer trabajo, contratos o algún tipo de beneficio económico o de cualquier otra naturaleza a ningún funcionario público, contratista o estructurador, vinculado a la Universidad ni a sus familiares en primer grado de consanguinidad, segundo de afinidad o primero civil, a partir de la adjudicación o con ocasión de la misma y hasta dos (2) años siguientes a la suscripción del Contrato, sin perjuicio del régimen de conflictos de intereses y de inhabilidades e incompatibilidades previsto en la Constitución y en la ley.
 - o. Exigir a nuestros empleados, proveedores y subcontratistas relacionados con el proyecto, suscribir un pacto ético de conducta que garantice la probidad y transparencia de las actuaciones de todos los involucrados en la preparación de la propuesta y en la ejecución del Contrato.
 - p. No ofrecer gratificaciones o atenciones en dinero o en especie, ni financiar, patrocinar, auspiciar o promover directa o indirectamente fiestas, recepciones, homenajes o cualquier tipo de atenciones sociales a funcionarios públicos o contratistas del Estado, durante el Proceso de Contratación ni durante la ejecución o liquidación del Contrato.
 - q. No contratar, ni ofrecer dádivas, regalos o gratificaciones a personas con alta capacidad de influencia política o mediática, con el objeto de obtener citas o influir o presionar las decisiones que la Universidad tome respecto de Procesos de Contratación Estatal, bien sea en su adjudicación, supervisión o terminación.
 - r. Manifestar las inquietudes relacionadas con el Proceso de Contratación por los canales definidos en los documentos del proceso.
 - s. No contratar ni ofrecer dádivas, regalos, gratificaciones, contratos o cualquier tipo de beneficio económico o de cualquier naturaleza, a servidores de la Universidad o sus asesores, o del equipo estructurador, con el fin de tener asesoramiento o acceso a información privilegiada, relacionada con el Proceso de Contratación.
 - t. Dar a conocer a la Universidad, a la Secretaría de Transparencia del Departamento Administrativo de la Presidencia de la República y a las autoridades competentes en caso de presentarse alguna queja o denuncia sobre la ocurrencia de un acto de corrupción durante el Proceso de Contratación o con cargo al Contrato, y del conocimiento que tenga sobre posibles pagos o beneficios ofrecidos u otorgados.
 - u. Denunciar de manera inmediata ante las autoridades competentes, con copia a la Secretaría de Transparencia del Departamento Administrativo de la Presidencia de la República, cualquier solicitud, ofrecimiento, favor, dádiva, prerrogativa, recompensa, gratificación o atención social, efectuada por Proponentes o cualquiera de sus empleados, administradores, consultores o contratistas, a funcionarios públicos o a sus asesores que estén directa o indirectamente involucrados en la estructuración, manejo y decisiones del Proceso de Contratación, de manera previa, concomitante o posterior al mismo, que tengan la intención de inducir o direccionar alguna decisión relacionada con la adjudicación.

PROFORMA No. 1

MODELO DE CARTA DE PRESENTACIÓN DE LA PROPUESTA

Bogotá, D.C.,

Señores
UNIVERSIDAD PEDAGÓGICA NACIONAL
Oficina de Contratación
Carrera 16 A No. 79-08
Bogotá D. C.

Asunto: **CONVOCATORIA PÚBLICA No. 05 DE 2021**

Por medio de los documentos adjuntos me permito presentar propuesta para participar en el proceso de selección tendiente a:

CONTRATAR LA ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UNA NUEVA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL (CLÚSTER DE FIREWALLS) Y DE APLICACIONES (FIREWALLS DE APLICACIONES WEB) PARA LA UNIVERSIDAD PEDAGÓGICA NACIONAL

En el evento de resultar favorecido con la adjudicación me comprometo a notificarme, perfeccionar el contrato, a legalizarlo dentro de los plazos establecidos en el cronograma del proceso y a ejecutar el objeto contractual de acuerdo con lo previsto en la invitación y el contrato.

En mi calidad de proponente declaro:

- a) Que conozco los términos de la Invitación del proceso de selección e informaciones sobre preguntas y respuestas, así como los demás documentos relacionados con el objeto a desarrollar y acepto cumplir todos los requisitos en ellos exigidos.
- b) De igual forma manifiesto que acepto las consecuencias que se deriven del incumplimiento de los requisitos a que se refiere el numeral anterior.
- c) Igualmente declaro bajo la gravedad del juramento que toda la información aportada y contenida en mi propuesta es veraz y susceptible de verificación.
- d) Que acepto las condiciones y demás exigencias para la ejecución del contrato.
- e) Que en caso de que se me adjudique el contrato me comprometo a suscribir el acta de iniciación con la Universidad Pedagógica Nacional y a terminar el contrato dentro de los plazos contractuales, de acuerdo con lo establecido en los documentos del proceso de selección y el contrato.
- f) Que conozco y acepto en un todo las leyes generales y especiales aplicables a este proceso contractual.
- g) Que con la firma de la presente carta manifiesto bajo la gravedad de juramento que ni yo ni la(s) persona(s) natural(es) y/o jurídicas por mi representada, nos encontramos incurso(s) en inhabilidades, incompatibilidades o prohibiciones consagradas en la Ley.
- h) Que leí cuidadosamente los Términos de Referencia y elaboré mi propuesta ajustada a los mismos. Por tanto, conocí y tuve las oportunidades establecidas para solicitar aclaraciones, formular objeciones, efectuar preguntas y obtener respuestas a mis inquietudes.
- i) Que me he enterado debidamente de adendas, aclaraciones y respuestas logrando claridad en el proceso.
- j) Que me comprometo a mantener la validez de la propuesta por el término de tres meses.

Que mi propuesta se resume así:

Nombre completo del proponente:	
Cédula de Ciudadanía o NIT:	
Representante legal	
País de origen del proponente	
Valor total de la propuesta incluido IVA:	
Plazo para ejecutar el contrato: (NO PODRÁ SER SUPERIOR AL PLAZO INDICADO EN LOS TÉRMINOS REFERENCIA)	
Validez de la garantía de seriedad de la propuesta:	
Garantía de seriedad:	
Aseguradora: _____	_____ \$
Valor :	Desde: () Hasta: ()
Vigencia :	(Día/ mes/año) (Día/ mes/ año)

Me permito informar que las comunicaciones relativas a este proceso de selección las recibiré en la siguiente dirección:

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C. www.pedagogica.edu.co



UNIVERSIDAD PEDAGOGICA
NACIONAL
Educadora de educadores

Dirección: _____

Ciudad: _____

Teléfono(s): _____

Correo electrónico _____ donde recibiré comunicaciones,
notificaciones y requerimientos durante el proceso de selección

Atentamente,

Firma _____

Representante Legal: _____

Nombre _____

Representante Legal: _____

C.C.: _____

ANEXO No. 1 A LA CARTA DE PRESENTACIÓN DE LA PROPUESTA

(Ciudad), (fecha)

Autorizo a la Universidad Pedagógica Nacional en forma permanente e irrevocable, para que exclusivamente con fines estadísticos y de información interbancaria y en especial los relativos al funcionamiento de las Centrales de Riesgo, informe todo lo referente a mi comportamiento como CONTRATISTA de la Universidad Pedagógica Nacional en general y en especial sobre los saldos que a su favor resulten de todas las operaciones que bajo cualquier modalidad me hubiese otorgado o me otorgue en el futuro, especialmente en lo que respecta a los pagos por concepto del contrato resultante de la presente Invitación cerrada

Igualmente autorizo a la Universidad Pedagógica Nacional con carácter permanente e irrevocable y mientras subsista alguna relación comercial u obligación insoluta, para consultar ante la Asociación Bancaria o cualquiera otra Central de Información legalmente constituida mi endeudamiento con el sector financiero, así como la información comercial disponible sobre el cumplimiento y manejo dado a los compromisos adquiridos con dicho sector, especialmente para la evaluación financiera de la propuesta presentada dentro de esta invitación.

Lo anterior implica que la información reportada permanecerá en la base de datos de la Asociación Bancaria o de la Central de Información autorizada por la ley, durante el tiempo que la misma ley establezca de acuerdo con el momento y las condiciones en que se efectúe el pago de las obligaciones.

En consecuencia, las Universidades del sector financiero afiliadas a la Central de Información del Sector Financiero (CIFIN), o a cualquier otra Central de Información legalmente constituida, conocerán mi comportamiento presente y pasado relacionado con el cumplimiento e incumplimiento de mis obligaciones financieras, derivadas del contrato que llegare a suscribir con la Universidad Pedagógica Nacional.

Nombre y Firma del Representante Legal

ANEXO No. 2 A LA CARTA DE PRESENTACIÓN DE LA PROPUESTA¹

¿PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES TRIBUTARIAS, EN QUE REGIMEN ENCUENTRA CLASIFICADO COMO PROPONENTE, CONTRATISTA?		
	SI	NO
• GRAN CONTRIBUYENTE		
• REGIMEN COMUN		
• REGIMEN SIMPLIFICADO		
RENTA		
1. Es usted Sujeto Pasivo de Retención en la Fuente		
2. Tiene usted la calidad de Autorretenedor		
Si tiene la calidad de “Autorretenedor”, anexar fotocopia de la Resolución expedida por la DIAN.		
IMPUESTO AL VALOR AGREGADO – IVA		
1. A qué Régimen Impositivo pertenece usted como CONTRATISTA		
2. Es usted responsable del Impuesto al Valor agregado-IVA		
3.IMPUESTO DE INDUSTRIA Y COMERCIO - ICA		
1. De acuerdo a las actividades sujetas al Impuesto, en cual se considera clasificado y cuál es el porcentaje: • Industrial • Comercial • Servicios		

Firma del Representante Legal _____
Nombre _____

¹Deberá tramitarse uno por cada integrante del consorcio o unión temporal.

PROFORMA No. 2
DOCUMENTOS CONSORCIAL Y COMPROMISO DE UNIÓN TEMPORAL

A. FORMATO CONSORCIO

Entre los suscritos a saber: _____, mayor de edad, vecino de esta ciudad, identificado con cédula de ciudadanía N° _____, expedida en _____, quien obra en nombre y representación legal de (escribir el nombre completo incluyendo el tipo de sociedad y en su defecto indicar que se trata de una persona natural.), legalmente constituida, con domicilio principal en _____, con NIT N° _____, y debidamente facultado por la junta de socios, y _____ mayor de edad, vecino de esta ciudad, identificado con cédula de ciudadanía N° _____, expedida en _____, quien obra en nombre y representación legal de (escribir el nombre completo incluyendo el tipo de sociedad y en su defecto indicar que se trata de una persona natural.), legalmente constituida, con domicilio principal en _____, con NIT N° _____, debidamente facultado por los estatutos sociales, _____, manifestamos que mediante el presente documento hemos acordado integrar un Consorcio cuya integración, conformación y reglamentación se regirá por las siguientes cláusulas:

PRIMERA. – OBJETO: El objeto del presente documento es la integración de un Consorcio entre _____ y _____, con el propósito de complementar las capacidades técnicas, operativas, administrativas y financieras de las partes que constituyen el presente Consorcio, para la presentación de la propuesta, adjudicación, celebración y ejecución del contrato, dentro de **LA CONVOCATORIA PÚBLICA NO. 05 DE 2021**, por la Universidad, cuyo objeto es: *“CONTRATAR LA ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UNA NUEVA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL (CLÚSTER DE FIREWALLS) Y DE APLICACIONES (FIREWALLS DE APLICACIONES WEB) PARA LA UNIVERSIDAD PEDAGÓGICA NACIONAL”*. Nuestra responsabilidad será solidaria, mancomunada e ilimitada en todas y cada una de las obligaciones derivadas de la propuesta y el contrato. En consecuencia, las actuaciones hechas y omisiones que se presenten en desarrollo de la propuesta y del contrato, afectarán a todos los miembros que lo conforman.

SEGUNDA. – DENOMINACIÓN: El presente consorcio se denominará _____.

TERCERA. – DOMICILIO: El domicilio del consorcio será la (dirección, teléfono y/o fax) de la ciudad de _____.

CUARTA. – REPRESENTANTE DEL CONSORCIO: Se designa como representante del presente Consorcio al(a) señor(a) _____, identificado con cédula de ciudadanía N° _____, expedida en _____, cargo este que se entiende aceptado con la firma del presente documento y quien está do para contratar, comprometer, negociar y representar al consorcio. Igualmente se nombra como suplente del representante del consorcio al señor _____. Identificado con cédula de ciudadanía N° _____.

QUINTA. – DURACIÓN: La duración del presente Consorcio, en caso de salir favorecido con la adjudicación, será el tiempo comprendido entre la fecha de presentación de la propuesta y treinta (30) meses más contado desde la finalización del término de ejecución del objeto contractual. En todo caso el consorcio durará todo el término necesario para atender las garantías prestadas.

sexta. – condiciones y extensión de la participación de acuerdo con la ley: La participación de cada una de las partes que conforman el cien por ciento (100%), del consorcio no podrá ser modificada sin el consentimiento previo de la Universidad, y será distribuida de la siguiente forma:

Integrantes	%	Labor a desarrollar en la propuesta (administrativos, jurídicos, técnicos y económicos)

SEPTIMA. PROHIBICIÓN DE CESIÓN DEL CONTRATO No se podrá ceder en todo o en parte la participación de alguno de los integrantes del Consorcio, entre ellos. Cuando se trate de cesión a un tercero se requerirá aprobación escrita previa de la Universidad contratante.

CLÁUSULAS OPCIONALES: El documento podrá contener las demás cláusulas opcionales: que los asociados consideren pertinentes, siempre y cuando no contravengan lo dispuesto en la ley 80/93 o incluyan limitaciones o exclusiones de los consorciados frente a la Universidad. (Aspectos financieros, Arbitramento, Reglas básicas que regulan la relaciones entre los integrantes del consorcio, entre otras).

En constancia de lo anterior, se firma por quienes intervinieron en el presente documento a los _____ días del mes de _____ del año _____.

Acepto:

C.C:

Representante Legal de:

O persona natural del consorcio:

NIT:

Dirección:

Tel: y/o fax:

Acepto:

C.C:

Representante Legal de:

O persona natural del consorcio:

NIT:

Dirección:

Tel: y/o fax:

NOTA 1: Señor Proponente Recuerde que el presente Anexo solo deberá diligenciarse y presentarse en el caso en el que su propuesta sea en calidad de CONSORCIO. En tal sentido en el caso de no aplicar NO DEBERA ANEXARSE NI DILIGENCIARSE.

B. FORMATO DOCUMENTO UNIÓN TEMPORAL

En la ciudad de _____ a los _____ días del mes de _____ del año _____, entre quienes suscriben este documento, de una parte _____, sociedad de responsabilidad (escribir el nombre completo, incluyendo el tipo de sociedad y en su defecto indicar si se trata de persona natural) legalmente constituida y con domicilio principal en la ciudad de _____, representada legalmente por _____ mayor de edad, domiciliado en _____, identificado con cédula de ciudadanía número _____, expedida en _____, en su condición de _____, y representante legal de la misma, por una parte, y por la otra _____, sociedad de responsabilidad (escribir el nombre completo, incluyendo el tipo de sociedad y en su defecto indicar si se trata de persona natural), legalmente constituida y con domicilio principal en _____, representada legalmente por _____, mayor de edad, domiciliado en _____, identificado con la cédula de ciudadanía número _____, expedida en _____, quien obra en su calidad de gerente y representante legal de la misma. Han decidido conformar una Unión Temporal, la cual se denominará _____ y se registrará por las siguientes cláusulas:

PRIMERA. - OBJETO Y ALCANCE: El objeto de la Unión Temporal consiste en la presentación conjunta a la Universidad, de una propuesta para la adjudicación, celebración y ejecución del contrato “*CONTRATAR LA ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UNA NUEVA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL (CLÚSTER DE FIREWALLS) Y DE APLICACIONES (FIREWALLS DE APLICACIONES WEB) PARA LA UNIVERSIDAD PEDAGÓGICA NACIONAL*”, producto **DE LA CONVOCATORIA PÚBLICA NO. 05 DE 2021**. La Unión Temporal se compromete en caso de adjudicación, a la realización a cabalidad de los trabajos objeto del contrato dentro de las normas exigidas por la Universidad y en general al cumplimiento de las obligaciones que se deriven de su ejecución. Las partes se encargarán de elaborar la propuesta técnica y económica, suministrarán el mutuo apoyo técnico, logístico y administrativo que se requiera para dicha presentación.

SEGUNDA. - NOMBRE Y DOMICILIO: La Unión Temporal se denominará _____, y su domicilio será la ciudad de _____, con dirección en _____, oficina, _____, fax _____, teléfono _____.

TERCERA. – CONDICIONES Y EXTENSIÓN DE LA PARTICIPACIÓN DE ACUERDO CON LA LEY: La participación de cada una de las partes que conforman el cien por ciento (100%), de la Unión Temporal no podrá ser modificada sin el consentimiento previo de la Universidad, y será distribuida de la siguiente forma:

Integrantes	%	Labor a desarrollar en la propuesta (administrativos, jurídicos, técnicos y económicos)

CUARTA. - OBLIGACIONES Y SANCIONES: Los miembros de la Unión Temporal responderán solidariamente en cada uno de los compromisos que esta celebre con la Universidad. Las sanciones por el incumplimiento de las obligaciones derivadas de la propuesta y del contrato se impondrán de acuerdo con la participación en la ejecución de cada uno de los miembros de la unión temporal, (numeral 2, del artículo 7º de la ley 80 de 1993).

QUINTA. – DURACIÓN: La duración de la Unión Temporal en caso de salir favorecida con la adjudicación será el tiempo comprendido entre la fecha de presentación de la propuesta y treinta (30) meses más contado desde la finalización del término de ejecución del objeto contractual. En todo caso la Unión Temporal durará todo el término necesario para atender las garantías prestadas.

SEXTA. – CESIÓN: No se podrá ceder en todo o en parte la participación de alguno de los integrantes de la Unión Temporal, entre ellos. Cuando se trate de cesión a un tercero se requerirá aprobación escrita previa de la Universidad contratante.

SÉPTIMA. - REPRESENTANTE DE LA UNIÓN TEMPORAL: La Unión Temporal designa como representante legal de ésta, al señor(a) _____ domiciliado en _____, identificada(o) con la cédula de ciudadanía número _____ de _____, el cual está facultado para contratar, comprometer, negociar, y representar a la unión temporal, igualmente se nombra como suplente del representante legal al señor(a) _____, domiciliado en _____, con cédula de ciudadanía número _____ de _____.

OCTAVA. CLÁUSULAS OPCIONALES: El documento podrá contener las cláusulas opcionales que los asociados consideren pertinentes, siempre y cuando no contravengan lo dispuesto en la ley 80/93.

Para constancia y aprobación, el presente documento se firma en la ciudad de _____ a los _____ días del mes de _____ de _____, por quienes intervinieron.

Nombre
CC
Representante legal
NIT:
Dirección:
Teléfono:
Acepto

Nombre
CC
Representante legal
NIT:
Dirección:
Teléfono:
Acepto

Nombre
CC
Representante legal
NIT:
Dirección:
Teléfono:

Nombre
CC
Representante legal
NIT:
Dirección:
Teléfono:

NOTA 1 Señor Proponente Recuerde que el presente Anexo solo deberá diligenciarse y presentarse en el caso en el que su propuesta sea en calidad de UNIÓN TEMPORAL. En tal sentido en el caso de no aplicar NO DEBERA ANEXARSE NI DILIGENCIARSE.

PROFORMA No. 3
PAGOS DE SEGURIDAD SOCIAL Y APORTES LEGALES

ARTÍCULO 50 LEY 789 DE 2002
(PERSONAS JURÍDICAS)

[Este Formato debe ser diligenciado por las personas jurídicas nacionales y las extranjeras con domicilio o sucursal en Colombia las cuales deberán acreditar este requisito respecto del personal vinculado en Colombia].

[Cuando la persona jurídica no esté exonerada en el pago al sistema de aportes parafiscales, deberá incluir el siguiente texto y ajustar el Formato en lo correspondiente:]

[Incluir el nombre del representante legal de la persona jurídica], identificado con [Incluir el número de identificación], en mi condición de representante legal de [Incluir la razón social de la persona jurídica] identificada con el NIT [Incluir el NIT], bajo la gravedad de juramento certifico el pago de los aportes de salud, riesgos laborales, pensiones y aportes a las Cajas de Compensación Familiar, al Instituto Colombiano de Bienestar Familiar y al Servicio Nacional de Aprendizaje, (artículo 65 Ley 1819 de 2016), pagados por la compañía durante los últimos seis (6) meses contados a partir de la fecha de cierre del presente Proceso de Contratación. Lo anterior, en cumplimiento de lo dispuesto en el artículo 50 de la Ley 789 de 2002.

[Incluir el nombre del revisor fiscal, según corresponda], identificado con [Incluir el número de identificación], y con tarjeta profesional [Incluir número de tarjeta profesional] de la Junta Central de Contadores de Colombia, en mi condición de revisor fiscal de [Incluir la razón social de la compañía] identificada con el NIT [Incluir el NIT], debidamente inscrito en la Cámara de Comercio de _____, luego de examinar los estados financieros de la compañía, de acuerdo con las normas de auditoría generalmente aceptadas en Colombia, bajo la gravedad de juramento certifico el pago de los aportes de salud, riesgos laborales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, (artículo 65 Ley 1819 de 2016), pagados por la compañía durante los últimos seis (6) meses contados a partir de la fecha de cierre del presente Proceso de Contratación. Lo anterior, en cumplimiento de lo dispuesto en el artículo 50 de la Ley 789 de 2002.

[En el evento en que la sociedad no tenga más de seis (6) meses de constituida, deberá acreditar los pagos a partir de la fecha de su constitución como sigue:]

[Incluir el nombre del representante legal de la persona jurídica] identificado con [Incluir el número de identificación] en mi condición de representante legal de [Incluir la razón social de la persona jurídica] identificada con el NIT [Incluir el NIT], bajo la gravedad de juramento certifico el pago de los aportes de salud, riesgos laborales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto

Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, (artículo 65 Ley 1819 de 2016), pagados por la compañía a partir de [fecha de constitución]. Lo anterior, en cumplimiento de lo dispuesto en el artículo 50 de la Ley 789 de 2002.

[Incluir el nombre del revisor fiscal, según corresponda] identificado con [Incluir el número de identificación], y con tarjeta profesional [Incluir número de tarjeta profesional] de la Junta Central de Contadores de Colombia, en mi condición de revisor fiscal de [Incluir la razón social de la persona jurídica] identificada con el NIT [Incluir el NIT], debidamente inscrito en la Cámara de Comercio de _____, luego de examinar los estados financieros de la compañía, de acuerdo con las normas de auditoría generalmente aceptadas en Colombia, bajo la gravedad de juramento certifico el pago de los aportes de salud, riesgos laborales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, (artículo 65 Ley 1819 de 2016), pagados por la compañía a partir de [fecha de constitución]. Lo anterior, en cumplimiento de lo dispuesto en el artículo 50 de la Ley 789 de 2002.

[En caso de presentar acuerdo de pago con alguna de las Universidades anteriormente mencionadas, se deberá precisar el valor y el plazo previsto para el acuerdo de pago, con indicación del cumplimiento de esta obligación, caso en el cual tendrá que anexar copia del acuerdo de pago correspondiente y el comprobante de pago soporte del mes anterior al cierre del proceso de contratación].

[Cuando la persona jurídica esté exonerada de aportes parafiscales de acuerdo con el artículo 114-1 del Estatuto Tributario modificado por el artículo 65 de la Ley 1918 de 2016, deberá incluir el siguiente texto y ajustar el Formato en lo correspondiente:]

Conforme el artículo 65 de la Ley 1819 de 2016, bajo la gravedad de juramento manifiesto que me encuentro exonerado del pago de los aportes parafiscales a favor del Servicio Nacional del Aprendizaje (SENA), del Instituto Colombiano de Bienestar Familiar (ICBF) y las cotizaciones al Régimen Contributivo de Salud, las sociedades y personas jurídicas y asimiladas contribuyentes declarantes del impuesto sobre la renta y complementarios, correspondientes a los trabajadores que devenguen, individualmente considerados, menos de diez (10) salarios mínimos mensuales legales vigentes.

[Cuando la persona jurídica no haya tenido personal a cargo dentro de los seis (6) meses anteriores a la presentación de la propuesta deberá manifestarlo de la siguiente manera:]

[Incluir el nombre del representante legal de la persona jurídica o el revisor fiscal, según corresponda] identificado con [Incluir el número de identificación], en mi condición de [Indicar si actúa como representante legal o revisor fiscal] de [Incluir la razón social de la persona jurídica] identificada con el NIT [Incluir el NIT], bajo la gravedad de juramento, manifiesto que dentro de los seis (6) meses anteriores a la fecha de firma del contrato no tuve personal a cargo y, por ende, no estoy obligado a efectuar el pago de aportes legales y seguridad social.

En constancia, se firma en _____, a los _____ días del mes de _____ de 20__.

[Nombre y firma del representante legal de la persona jurídica o el revisor fiscal, según corresponda]

Nota: Para los Proponentes Plurales cada uno de los integrantes debe acreditar por separado los requisitos señalados. Adicionalmente, la persona jurídica adjudicataria debe presentar, para la suscripción del Contrato, ante la dependencia respectiva, la declaración donde acredite el pago correspondiente a seguridad social integral y aportes legales cuando a ello haya lugar.

PROFORMA No. 4

ACEPTACIÓN DE ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO

La entrega de los bienes objeto del proceso, se efectuará en observancia a las siguientes especificaciones y requerimientos de carácter técnico:

A. Especificaciones Generales

La entrega de los bienes objeto del proceso, se efectuará en observancia a las siguientes especificaciones y requerimientos de carácter técnico:

B. Ficha Técnica:

Observaré especificaciones técnicas detalladas en las fichas técnicas adjuntas, en todos los aspectos allí relacionados, al momento de confeccionar su oferta; y en la ejecución del contrato cumpliré a cabalidad los requerimientos allí efectuados.

C. Garantía Técnica

Responderé y/o cambiaré aquellos bienes y/o elementos deteriorados, incompletos, en aparente mal estado y que no cumplan con las especificaciones técnicas establecidas en el contrato y documentos previos, en un término **no superior a 48 horas** una vez comunicada la eventualidad, quedando los costos que genere esta actuación, a mi cargo.

D. Transporte y Entrega:

Asumiré y dispondré de los medios logísticos necesarios (medio de transporte y personal idóneo) para efectuar las entregas e instalaciones en el sitio dispuesto por el supervisor.

E. Instalación

El futuro contratista deberá Instalar los equipos en el sitio indicado por el supervisor, con los respectivos requerimientos técnicos y funcionales especificados, sin que ello genere un costo adicional a la Universidad.

F. Calidad y Presentación de los Bienes y/o Elementos:

Durante el término de ejecución del respectivo contrato, suministraré bienes y/o elementos que atiendan a los siguientes condicionamientos de calidad y presentación:

1. Suministraré una garantía comercial, no inferior a un (1) año, término en el cual responderá por la calidad de los bienes, por causas imputables a su fabricación, efectuando los mantenimientos o cambios que se hagan necesarios, asumiendo los costos que generen tales requerimientos.
2. Los bienes y/o elementos a suministrar serán de óptimas condiciones, y de buena calidad.
3. Los bienes y/o elementos se entregarán nuevos, en óptima presentación, según corresponda para cada caso, con los sellos y cintas de seguridad de fábrica según corresponda y aplique, y no re manufacturados.

**REFERENTES, ESPECIFICACIONES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS
(PROFORMA No. 4 – Especificaciones Técnicas)**

MODERNIZACIÓN TECNOLÓGICA DEL SISTEMA DE SEGURIDAD PERIMETRAL DE LA UNIVERSIDAD PEDAGÓGICA			
REFERENTES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS			
ITEM	REQUERIMIENTOS FIREWALL	Cumple (SI)	¿Cómo se Verifica?
A	1. Requisitos generales		
1	La UNIVERSIDAD PEDAGÓGICA NACIONAL desea una solución de seguridad perimetral para alrededor de 15.000 usuarios y 120 servidores, que tenga las capacidades de una solución de Prevención de Amenazas, el cual incluya los componentes de Firewall, Control de Aplicaciones, Control de Navegación, IPS, Control de Malware Conocido, Control de Malware Avanzado, VPN IPSec /SSL, Manejo de Identidades. La solución Ofertada debe proporcionarnos en Alta disponibilidad		
2	Esta solución debe estar reconocida por Gartner como una solución líder en su cuadrante en los últimos 3 años		
3	Los registros (logs) de la solución de seguridad perimetral descritas, deben centralizarse en una única consola central de gestión, que permita generar reportes y correlacionar eventos según el impacto de seguridad		
4	La entidad requiere, que las capas de Plano de Control (Gestión) y Plano de Datos (Componentes de Protección) estén completamente separados tal como lo sugiere el modelo Zero Trust (http://go.forrester.com)		
5	Los gateway deben estar en alta disponibilidad		
6	La solución debe incluir el licenciamiento full de NGFW		
7	La solución debe incluir el licenciamiento o uso de vpn tipo IPSec y SSL para usuarios ilimitados		
8	El año de lanzamiento de los Appliances Gateway debe ser mínimo 2020 en adelante.		
9	El soporte, licenciamiento y garantía del fabricante ofertado deberá ser por 1 año y debe incluir soporte de fabrica 7x24 y del proveedor 7x24.		

10	El Gateway de próxima generación debe ser capaz de soportar estas aplicaciones de seguridad de próxima generación en una plataforma unificada.		
11	Stateful Inspection Firewall		
12	Sistema de Prevención de Intrusión		
13	Adquisición de identidad de usuarios		
14	Control de aplicaciones y filtrado de URL		
15	Control de Bots & Botnets, actualización periódica desde servicio en la nube propio		
16	Anti - Virus		
17	Emulación de amenazas (Sandboxing)		
18	Extracción de amenazas (Depuración)		
19	Data Scrubbing – Limpieza de Datos/Archivos		
20	Inspección de HTTPS		
21	Reconocimiento de identidad de usuarios		
22	Anti - Spam		
23	VPN IPSec		
24	Acceso Seguro para dispositivos móviles Android y IOS mediante el uso de agentes para VPN, para usuarios ilimitados de la entidad		
25	Gestión de políticas de seguridad		
26	Monitoreo y registro de logs		
27	Almacenamiento de logs y estados de la plataforma		
28	Correlación de logs, eventos, generación de acciones automáticas de respuesta ante incidentes e informe		
29	Virtualización de firewalls (sistemas virtuales)		
30	Si requieren appliance adicionales para la administración de la solución o almacenamiento de logs para la solución estos deberán ser físicos propios del fabricante		
31	La plataforma debe incluir sistema operativo de 64 bits		
32	Los equipos gateway debe soportar más de 32 GB de memoria RAM.		
33	Los equipos gateway deben soportar como mínimo 8 interfaces 1G en cobre y/o fibra y 8 interfaces 10G en fibra, deben tener la posibilidad de realizar agregación entre las interfaces (LACP). Se deben incluir los diferentes SFP		
34	Debe tener la opción de contar con una interfaz de administración (out-of-band) que permita las siguientes acciones sobre el equipo: a. Encender la caja de manera remota b. Acceso remoto a través de consola virtual KVM c. Instalación remota utilizando una media virtual. d. Para solución de problemas debe permitir el conocer el último estado de la caja antes de reiniciarse e. Monitoreo de estado a través del protocolo SNMP		
35	Los componentes de la solución deben ser accesibles a través de SSH y de interfaz Web usando SSL.		

36	La solución debe tener soporte IPv6 como mínimo para IPS, Control de Aplicaciones, Firewall, Modulo de Adquisición de Identidades, Filtrado URL, Antivirus and Control de Bots.		
37	Debe soportar la integración con Active Directory sin importar si es IPv4 o IPv6		
38	La solución debe soportar de forma mínima y oficial, las siguientes características /RFC. Que permitirán un perfecto acoplamiento de la entidad con el decreto 2710 del Ministerio de Tecnologías de la Información y las comunicaciones, que habla de la implementación de IPv6 en el Gobierno de Colombia. a. RFC 1981 - Path Maximum Transmission Unit Discovery for IPv6 b. RFC 2460 - IPv6 Basic specification c. RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks d. RFC 3596 - DNS Extensions to support IPv6 e. RFC 4007 - IPv6 Scoped Address Architecture f. RFC 4193 - Unique Local IPv6 Unicast Addresses g. RFC 4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers – 6in4 tunnel is supported. h. RFC 4291 IPv6 Addressing Architecture (which replaced RFC1884) i. RFC 4443 ICMPv6 j. RFC 4861 Neighbor Discovery		
39	La herramienta debe ser capaz de realizar backup/restores de la configuración, permitiendo al administrador programar la realización de los backups en el tiempo deseado.		
40	Los Backups pueden ser almacenados localmente y/o remotamente		
41	2. Requisitos para el Firewall de próxima generación		
42	El gateway de seguridad debe usar Stateful inspection basado en el análisis granular de la comunicación y el estado de las aplicaciones para rastrear y controlar el flujo de la red.		
43	La solución debe ser basada en Stateful Inspection, permitiendo crear reglas por puerto, protocolo y aplicación.		
44	La solución debe admitir el control de acceso para al menos 150 servicios / protocolos / predefinidos		
45	Debe proporcionar estadísticas de recuento de aciertos en las reglas de seguridad a la aplicación de administración de la plataforma.		
46	Debe permitir que las reglas de seguridad se apliquen en intervalos de tiempo que se configurarán con una fecha / hora de caducidad. Debe tener la posibilidad de definir expiración de reglas de forma automática, por fecha & hora.		
47	El firewall debe admitir los métodos de autenticación de usuario, cliente y sesión.		
48	Los siguientes esquemas de autenticación de usuario deben ser compatibles con el gateway de seguridad y el módulo VPN: tokens (ejemplo, SecureID), TACACS, RADIUS y certificados digitales		
49	La solución debe incluir una base de datos de usuarios local, para permitir la autenticación y autorización de usuarios sin la necesidad de un dispositivo externo		
50	La solución debe soportar protocolo DHCP, tanto servidor, como relay		
51	La solución debe soportar ser proxy de HTTP y HTTPS		
52	La solución debe incluir la capacidad de trabajar en modo Transparente / modo bridge		
53	La solución debe admitir alta disponibilidad de los dispositivos en modo activo pasivo y en modo compartición de carga. Ambos con sincronización de estados.		

54	Soporte IPv6		
55	La solución debe soportar la configuración de doble stack (IPv4 e IPv6) en cualquier interfaz, sub interfaz o bond de las mismas.		
56	La solución debe admitir el manejo del tráfico IPv6 como mínimo en los módulo IPS y APP, firewall, reconocimiento de identidad, filtrado de URL, antivirus y anti-Bot		
57	La solución debe admitir NAT 6 a 4 NAT o tuneles 6 a 4.		
58	La solución debe ser compatible con la integración de AD usando el tráfico ipv6		
59	La plataforma deberá admitir la capacidad de mostrar la tabla de enrutamiento IPv6		
60	La solución debe soportar los siguientes RFC de IPv6:		
61	RFC 1981 Path Maximum Transmission Unit Discovery for IPv6		
62	RFC 2460 IPv6 Basic specification		
63	RFC 2464 Transmission of IPv6 Packets over Ethernet Networks		
64	RFC 3596 DNS Extensions to support IPv6		
65	RFC 4007 IPv6 Scoped Address Architecture		
66	RFC 4193 Unique Local IPv6 Unicast Addresses		
67	RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – 6in4 tunnel is supported.		
68	RFC 4291 IPv6 Addressing Architecture (which replaced RFC1884)		
69	RFC 4443 ICMPv6		
70	RFC 4861 Neighbor Discovery		
71	RFC 4862 IPv6 Stateless Address Auto-configuration		
B	Sistema de Prevención de Intrusión		
1	El proveedor debe proporcionar evidencia de la posición de liderazgo en los últimos 3 años del Cuadrante Mágico de Gartner para las soluciones de Prevención de Intrusión y / o el Cuadrante Mágico Gartner de firewall de red empresarial.		
2	El módulo de Prevención de Intrusiones 'IPS' debe estar integrado en la plataforma de Firewall de nueva Generación.		
3	El IPS debe basarse en los siguientes mecanismos de detección: firmas de explotación, anomalías de protocolo, controles de aplicaciones y detección basada en el comportamiento		
4	IPS y el módulo de firewall deben integrarse en una plataforma.		
5	El módulo de Prevención de Intrusiones 'IPS', debe ser capaz de tener una opción para proteger solo los activos internos, en caso de ser requerido.		
6	IPS debe tener opciones para crear perfiles para las protecciones basadas en el cliente o servidor, o una combinación de ambos		
7	IPS debe proporcionar al menos dos perfiles / políticas predefinidos que se puedan usar de inmediato		
8	IPS debe tener un mecanismo de apertura de fallas basado en software, configurable basado en umbrales de CPU de puertas de enlace de seguridad y uso de memoria		
9	IPS debe proporcionar un mecanismo automatizado para activar o administrar nuevas firmas a partir de actualizaciones		

10	IPS debe admitir excepciones de red basadas en la fuente, el destino, el servicio o una combinación de los tres		
11	IPS debe incluir un modo de solución de problemas que establece el perfil en uso en modo de detección (sin bloquear tráfico), con un click sin modificar las protecciones individuales		
12	La aplicación IPS debe tener un mecanismo centralizado de correlación e informe de eventos		
13	El IPS debe proveer de un mecanismo automático, para activar o administrar nuevas firmas de protección, desde el proceso de actualización de este componente.		
14	El administrador debe poder activar automáticamente nuevas protecciones, en función de parámetros configurables (impacto en el rendimiento, gravedad de la amenaza, nivel de confianza, protecciones del cliente, protecciones del servidor)		
15	IPS debe ser capaz de detectar y prevenir las siguientes amenazas: uso indebido de protocolos, comunicaciones de malware, intentos de tunelización y tipos de ataques genéricos sin firmas predefinidas.		
16	Para cada protección, la solución debe incluir el tipo de protección (relacionada con el servidor o con el cliente), la gravedad de la amenaza, el impacto en el rendimiento, el nivel de confianza y la referencia de la industria.		
17	El IPS deberá contar con una guía visual para el administrador, que le permita categorizar la severidad de las firmas, si la seguridad protege la comunicación del lado del cliente o del servidor al que se accede.		
18	IPS debe ser capaz de recopilar una captura de paquetes para protecciones específicas		
19	El IPS debe tener un mecanismo de Fail-Open basado en Software, que permita el funcionamiento del appliance en caso de consumos altos de CPU y/o Memoria RAM.		
20	IPS debe poder detectar y bloquear los ataques a la red y a la capa de aplicaciones, protegiendo al menos los siguientes servicios: servicios de correo electrónico, DNS, FTP, servicios de Windows (redes de Microsoft)		
21	El proveedor debe proporcionar evidencia de liderazgo para proteger las vulnerabilidades de Microsoft		
22	IPS y / o Application Control deben incluir la capacidad de detectar y bloquear aplicaciones P2P y evasivas		
23	El administrador debe ser capaz de definir exclusiones de red y host de la inspección de IPS		
24	La solución debe proteger contra el envenenamiento de caché de DNS e impide que los usuarios accedan a las direcciones de dominio bloqueadas		
25	La solución debe proporcionar protecciones de protocolos VOIP		
26	IPS y / o Application Control deben detectar y bloquear las aplicaciones de controles remotos, incluidas aquellas que son capaces de crear túneles a través del tráfico HTTP.		
27	IPS debe tener protecciones SCADA		
28	IPS debe tener un mecanismo para convertir firmas SNORT		
29	La solución debe hacer cumplir la aplicación del protocolo Citrix		
30	La solución debe permitir al administrador bloquear fácilmente el tráfico entrante y / o saliente en función de los países, sin la necesidad de administrar manualmente los rangos de IP correspondientes al país.		
31	El IPS debe permitir la captura de paquetes, para propósitos forenses, para firmas específicas.		
32	Adquisición de identidad de usuario		

33	Debe poder adquirir la identidad del usuario al consultar Microsoft Active Directory en función de los eventos de seguridad		
34	La Solución debe ser capaz de adquirir la identidad de los usuarios, desde un directorio activo, sin la necesidad de instalar software/agentes en los controladores de dominio, basado en la lectura de los eventos de seguridad de Microsoft.		
35	Debe tener un método de autenticación de identidad de usuario basado en navegador para usuarios o activos que no sean de dominio		
36	Debe tener un agente de cliente dedicado que pueda instalarse por política en las computadoras de los usuarios que puedan adquirir e informar identidades a la pasarela de seguridad.		
37	Debe tener soporte de Kerberos (Principalmente en Directorio Activo), para poder realizar procesos de autenticación transparente y garantizar Single Sign-On.		
38	Debe soportar grupos anidados dentro del directorio activo		
39	Debe admitir entornos de servidor de terminal		
40	La solución debe integrarse sin problemas con los servicios de directorio, IF-MAP y Radius		
41	La solución de identidad debe admitir servidores de terminal y citrix		
42	La solución debe permitir la identificación a través de un proxy (por ejemplo: encabezados X-forward)		
43	Debe poder adquirir la identidad del usuario de Microsoft Active Directory sin ningún tipo de agente instalado en los controladores de dominio		
44	Debe admitir la autenticación transparente de Kerberos para el inicio de sesión único		
45	Debe admitir el uso de grupos anidados LDAP		
46	Debe poder compartir o propagar identidades de usuario entre múltiples puertas de enlace de seguridad		
47	Debe poder crear roles de identidad para usar en todas las aplicaciones de seguridad		
48	Control de aplicaciones y filtrado de URL		
49	La base de datos de control de aplicaciones debe contener más de 8000 aplicaciones conocidas.		
50	La solución debe ser capaz de crear una regla de filtrado con múltiples categorías		
51	La solución debe ser capaz de crear un filtro para un solo sitio que sea compatible con múltiples categorías.		
52	La solución debe tener granularidad de usuarios y grupos con reglas de seguridad		
53	La solución debe tener una interfaz de búsqueda fácil de usar para aplicaciones y URL		
54	La solución debe categorizar aplicaciones y URL y aplicaciones por Factor de riesgo		
55	El control de la aplicación y la política de seguridad URLF deben poder definirse por las identidades del usuario		
56	El control de la aplicación y la base de datos URLF deben ser actualizados por un servicio basado en la nube		
57	La solución debe tener control unificado de la aplicación y reglas de seguridad URLF		
58	La solución debe proporcionar un mecanismo para informar o pedir a los usuarios en tiempo real que los eduquen o confirmen acciones basadas en la política de seguridad.		

59	La solución debe proporcionar un mecanismo para limitar el uso de la aplicación en función del consumo de ancho de banda		
60	La solución debe permitir excepciones de red basadas en objetos de red definidos		
61	La solución debe proporcionar la opción de modificar la Notificación de bloqueo y redirigir al usuario a una página de corrección.		
62	La solución debe incluir un mecanismo de listas en blanco y negro que permita al administrador denegar o permitir URL específicas independientemente de la categoría		
63	La solución debe tener un mecanismo de bypass configurable		
64	La solución debe proporcionar un mecanismo de anulación en la categorización de la base de datos de URL		
65	El control de la aplicación y la política de seguridad URLF deben informar sobre el recuento de aciertos de la regla		
66	La Solución debe proveer un mecanismo que permita re-categorizar los sitios WEB.		
C	Anti-Bot y Anti-Virus		
1	El proveedor debe tener una aplicación integrada Anti-Bot y Anti-Virus en el firewall de próxima generación		
2	La aplicación anti-bot debe ser capaz de detectar y detener el comportamiento anormal sospechoso de la red		
3	La aplicación Anti-Bot debe usar un motor de detección de múltiples niveles, que incluye la reputación de direcciones IP, URL y DNS, y detectar patrones de comunicaciones de bots.		
4	Las protecciones anti-Bot deben poder escanear en busca de acciones de bots		
5	La solución debe ser compatible con la detección y prevención de virus y variantes de Cryptors y ransomware (p. Ej., Wannacry, Cryptlocker, CryptoWall ...) mediante el uso de análisis estáticos y / o dinámicos.		
6	La solución debe tener mecanismos para proteger contra los ataques de spear phishing		
7	El componente de control de Bots, debe ser capaz de detectar y prevenir ataques tipo ransomware y sus variantes (ej. Wannacry, Cryptolocker, CryptoWall) a través de análisis estático o dinámico.		
8	Ataques basados en DNS:		
D	La solución debe tener capacidades de detección y prevención para los escondites DNS de C & C.		
1	Búsqueda de patrones de tráfico C & C, no solo en su destino DNS		
2	Ingeniería reversa del malware para descubrir su DGA (domain name generation)		
3	Característica de captura DNS como parte de la prevención de amenazas, ayudando a descubrir hosts infectados generando comunicación C & C		
4	La solución debe detectar comunicaciones hacia sitios de comando & control, basados entre otros en direcciones IP, URL & Reputación de Dominios.		
5	La solución debe contar con la capacidad de detectar & prevenir ataques encapsulados en túneles DNS.		
6	La política de Anti-Bot y Anti-Virus debe administrarse desde una consola central		
7	La aplicación Anti-Bot y Anti-Virus debe tener un mecanismo centralizado de correlación e informe de eventos		
8	La aplicación antivirus debe poder evitar el acceso a sitios web maliciosos		

9	La aplicación antivirus debe poder inspeccionar el tráfico cifrado SSL		
10	Anti-Bot y Anti-Virus deben tener actualizaciones en tiempo real de servicios de reputación basados en la nube		
11	Anti-Virus debe ser capaz de detener los archivos maliciosos entrantes		
12	El antivirus debe ser capaz de escanear archivos descargados.		
13	El antivirus será capaz de inspeccionar tráfico pasando por el protocolo CIFS (carpetas compartidas), entre vians de servidores y usuarios.		
14	Anti-Virus debe poder escanear archivos de almacenamiento		
15	Las políticas de antivirus y anti-Bot se deben administrar de forma centralizada con la configuración de políticas granulares y la aplicación		
16	El Anti-Virus debería ser compatible con el escaneo de enlaces dentro de correos electrónicos		
17	El Anti-Virus debe Escanear archivos que están pasando el protocolo CIFS		
E	Inspección SSL (entrante / saliente)		
1	La solución ofrece soporte para la inspección / descifrado SSL con un rendimiento líder en todas las tecnologías de mitigación de amenazas		
2	La solución debería ser compatible con Perfect Forward Secrecy (PFS)		
3	La solución debe ser compatible con AES-NI, AES-GCM para mejorar el rendimiento		
4	La emulación de amenazas / sandboxing debe integrarse con SSL Inspection		
5	La solución debe aprovechar la base de datos de filtrado de URL para permitir al administrador crear una política de inspección https granular		
6	La solución puede inspeccionar el filtrado de URL basado en HTTPS sin necesidad de descifrado SSL		
F	Emulación de amenazas (sandboxing)		
1	La solución debe proporcionar la capacidad de proteger contra ataques de malware desconocidos y de día cero antes de que se hayan creado protecciones de firmas estáticas.		
2	1 Real-Time Prevention-unknown malware patient-0 en la navegación web		
3	1 Real-Time Prevention-unknown malware patient-0 en el correo electrónico		
4	La solución debe actuar en modo prevención, en caso de malware de "paciente-0" (cero) en los procesos de navegación.		
5	La solución debe tener la capacidad de emular archivos Office (doc, docx, ppt, pptx, dot, xls,) archivos de empaquetamiento (tar, 7z, zip, gz)		
G	Protocolos		
1	La solución debería ser capaz de emular ejecutable, archivar archivos, documentos, JAVA y flashear específicamente dentro de varios protocolos:		
2	HTTP		
3	HTTPS		
4	SMTP		
5	SMTP TLS		
6	PO3		

7	FTP		
8	CIFS (SMB)		
H	Tecnología Sandboxing:		
1	El motor de emulación debería poder inspeccionar, emular, prevenir y compartir los resultados del evento de sandboxing en la infraestructura antimalware		
2	La solución debería poder realizar un filtrado estático previo a la emulación		
3	la solución permitiría la emulación de archivos con un tamaño superior a 10 Mb en todos los tipos que admita		
4	Las soluciones deberían ser compatibles con los motores de detección basados en el aprendizaje automático de máquinas		
5	La solución debe detectar el ataque en la etapa de explotación, es decir, antes de que se ejecute el código de shell y antes de que se descargue / ejecute el malware.		
6	La solución debe ser capaz de detectar ROP y otras técnicas de explotación (por ejemplo, escalada de privilegios) mediante el control del flujo de la CPU		
7	La solución debe ser capaz de admitir enlaces de escaneo dentro de correos electrónicos de 0 días y malware desconocido.		
8	La solución de emulación de amenazas debe permitir la 'Restricción geográfica' que permite que las emulaciones se restrinjan a un país específico.		
9	La solución debe proporcionar la capacidad de Incrementar la seguridad con el intercambio automático de nueva información de ataque con otras pasarelas en forma de actualizaciones de firmas, etc.		
10	El motor de emulación debe superar el 90% de tasa de captura en las pruebas de Virus Total donde los archivos PDF y exe maliciosos conocidos se modifican con encabezados "no utilizados" para demostrar la capacidad de las soluciones para detectar malware nuevo y desconocido		
11	La solución debe detectar el tráfico de C & C de acuerdo con la reputación dinámica de ip / url		
12	La solución debería ser capaz de emular y extraer archivos incrustados en documentos		
13	La solución debe poder escanear documentos que contienen URL		
I	Detección de actividad del sistema:		
1	La solución debe monitorear la actividad sospechosa en:		
2	Llamadas API		
3	Cambios del sistema de archivos		
4	Registro del sistema		
5	Conexiones de red		
6	Procesos del sistema		
7	Creación y eliminación de archivos		
8	Modificación de archivo		
9	Inyección de código Kernel		
10	Detectar intentos de escalamiento de privilegios		



11	Modificaciones del núcleo (cambios en la memoria realizados por el código del kernel, no el hecho de que se cargue un controlador; esto está cubierto por el elemento anterior)		
12	Comportamiento del código del kernel (monitoriza la actividad del código no del modo de usuario)		
13	Interacción física directa de la CPU		
14	Detección de derivación UAC (control de acceso de usuario)		
J	Tecnología anti evasión:		
1	La solución debe tener capacidades anti evasión que detecten la ejecución de sandbox		
2	La solución debe ser resistente a los casos en los que el código de shell o el malware no se ejecutarían si detectan la existencia de un entorno virtual. (hipervisor propietario)		
3	retrasos		
4	La solución debe ser resistente a las demoras implementadas en el código del shell o en las etapas de malware.		
5	apagado, reinicio		
6	La solución debe ser resistente a los casos en los que el código de shell o el malware se ejecutan solo al reiniciarse o al apagarse el punto final.		
7	La interacción del usuario		
8	Emulación humana: la solución debe emular las actividades reales del usuario, como los clics del mouse, las teclas, etc.		
9	Similitud de icono: la solución debería ser capaz de identificar íconos que son similares a los documentos de aplicaciones populares		
10	evasión dentro de archivo flash (swf)		
K	Gestión e informes		
1	Tras la detección de archivos maliciosos, se debe generar un informe detallado para cada uno de los archivos maliciosos.		
2	El informe detallado debe incluir:		
3	video de la emulación		
4	líneas de tiempo		
5	creación / modificaciones de clave de registro,		
6	creación de archivos y procesos		
7	Actividad de red detectada.		
L	Extracción de amenazas (depuración / aplanamiento de archivos)		
1	la solución debería eliminar amenazas y eliminar contenido explotable, incluido contenido activo y objetos incrustados		
2	la solución debería poder Reconstruir archivos con elementos seguros conocidos		
3	la solución debe proporcionar la capacidad de convertir archivos reconstruidos a formato PDF		
4	la solución debe mantener flexibilidad con opciones para mantener el formato de archivo original y especificar el tipo de contenido que se eliminará		
M	IPsec VPN		

1	Se debe admitir la CA interna y la CA externa de terceros.		
2	La solución debe admitir cifrado 3DES y AES-256 para IKE Phase I y II IKEv2 más "Suite-B-GCM-128" y "Suite-B-GCM-256" para Fase II		
3	La solución debe admitir al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 y Grupo 20		
4	La solución debe ser compatible con la integridad de los datos con md5, sha1 SHA-256, SHA-384 y AES-XCBC		
5	La solución debe incluir soporte para VPN de sitio a sitio en las siguientes topologías:		
6	Full Mesh (todos para todos),		
7	Estrella (oficinas remotas al sitio central)		
8	Hub and Spoke (sitio remoto a través del sitio central a otro sitio remoto)		
9	La solución debe ser compatible con la configuración de VPN con una GUI mediante la adición de objetos de arrastrar y soltar a las comunidades de VPN		
10	La solución debe admitir VPN SSL sin cliente para el acceso remoto.		
11	La solución debe ser compatible con VPN L2TP, incluida la compatibilidad con el cliente de iPhone L2TP		
12	La solución debe permitir que el administrador aplique reglas de seguridad para controlar el tráfico dentro de la VPN		
13	La solución debe admitir redes privadas virtuales (VPN) basadas en dominio y VPN basadas en rutas que utilicen VTI y protocolos de enrutamiento dinámico.		
14	La solución debe incluir la capacidad de establecer VPN con puertos de enlace con IP públicas dinámicas		
15	La solución debe incluir compresión de IP para VPNs de cliente a sitio y sitio a sitio		
N	Gestión de seguridad		
1	Las comunicaciones entre todos los componentes que pertenezcan a la solución total (servidor de administración, gateways), deben establecer comunicaciones seguras y cifradas.		
2	Debe incluir una herramienta de búsqueda, que permita fácilmente filtrar objetos de red. Debe también incluir la opción de buscar objetos duplicados (con la misma IP) y objetos no usados (en una regla o política) y una lista de las reglas en que un objeto específico es usado		
3	Debe poderse realizar un cambio automático de logs, basados en programaciones de tiempo o del tamaño del archivo		
4	La solución debe tener la capacidad de hacer auditorías de las acciones de cada administrador que acceda a la plataforma		
5	La solución debe permitir realizar una completa auditoría, seguimiento en los cambios y evolución de las políticas de seguridad		
6	La solución debe tener la capacidad de forma nativa en tiempo real, de dar información sobre el estado de los dispositivos administrados (conectividad, nivel cpu, tráfico de red) e ilustrar de forma gráfica al menos eventos como la conexión de usuarios remotos vía vpn, estado de los túneles IPSEC y tráfico más común sobre las interfaces (monitor)		
7	Debe poder restringirse que direcciones IP (direcciones individuales, rangos, hostnames) pueden tener control sobre la consola de administración		

8	Capacidad de funcionar en un esquema de alta disponibilidad, para evitar que exista un solo momento de pérdida de funcionalidad de administración.		
9	La autenticación de administradores al sistema debe poder ser por lo menos mediante contraseña (password), certificados digitales y sistemas RADIUS		
10	Debe permitir la creación de filtros basados en cualquiera de las características del evento, tales como IP de origen y destino, servicio, tipo de evento, severidad del evento, nombre del ataque, país de origen o destino, etc. El administrador debe poder asignar estos filtros a diferentes líneas en un gráfico que sean actualizadas en intervalos regulares mostrando todos los eventos que concuerdan con ese filtro. Permitiendo que el operador se focalice en los eventos más importantes.		
11	La solución debe ser capaz de segmentar la base de reglas en una estructura de subpolíticas en la que solo el tráfico relevante se está reenviando al segmento relevante		
12	La solución debe ser capaz de segmentar la base de reglas a favor de la delegación de funciones en las que los cambios en un segmento no afectarán a otros segmentos.		
13	La solución debe poder segmentar la base de reglas en una estructura en capas		
14	La solución debe poder segmentar la base de reglas para permitir la flexibilidad de la estructura para alinearse con redes dinámicas		
15	La solución debe poder reutilizar el segmento de la base de reglas (por ejemplo, usar el mismo segmento de reglas en diferentes paquetes de políticas)		
16	La solución debe tener la granularidad de los administradores que trabajan en paralelo en la misma política sin interferir entre ellos		
17	La solución debe integrar registros, registros de auditoría en una consola para tener contexto mientras se trabaja en la política de seguridad		
18	La solución debe ser capaz de instalar protecciones relacionadas con amenazas y acceder a reglas relacionadas por separado para permitir su administración por equipos separados.		
19	La aplicación de administración de seguridad debe admitir cuentas de administrador basadas en roles. Por ejemplo, funciones para la administración de políticas de firewall solamente o rol para visualización de registros solamente		
20	La solución debe incluir un canal de comunicaciones seguro cifrado basado en certificado entre todos los componentes distribuidos por el proveedor que pertenecen a un único dominio de gestión		
21	La solución debe incluir una CA x.509 interna (Autoridad de certificación) que pueda generar certificados para las puertas de enlace y los usuarios para permitir una autenticación fácil en VPN.		
22	La solución debe incluir la capacidad de utilizar CA externas, que sea compatible con las normas PKCS # 12, CAPI o Entrust		
23	La administración debe proporcionar un contador de visitas a las normas de seguridad en la política de seguridad		
24	La solución debe incluir una opción de búsqueda para poder consultar fácilmente qué objeto de red contiene una dirección IP específica o parte de ella		
25	La solución debe incluir la opción de segmentar la base de reglas usando etiquetas o títulos de secciones para organizar mejor la política.		
26	La solución debe proporcionar la opción de guardar toda la política o parte específica de la política		

27	La solución debe tener un mecanismo de verificación de la política de seguridad antes de la instalación de la política		
28	La solución debe tener un mecanismo de control de revisión de la política de seguridad		
29	La solución debe incluir la capacidad de distribuir de forma centralizada y aplicar nuevas versiones de software de puerta de enlace		
30	La solución debe incluir una herramienta para administrar centralmente las licencias de todas las puertas de enlace controladas por la estación de administración		
31	La solución debe tener las capacidades para la administración multidominio y respaldar el concepto de política de seguridad global en todos los dominios		
32	Debe mostrar la distribución de eventos por países en un mapa.		
33	Debe permitir agrupar los eventos en base a cualquier característica de los mismos, pudiendo agrupar en varios niveles.		
34	Debe permitir realizar búsquedas dentro del listado de eventos.		
35	La GUI de administración debe tener la capacidad de excluir fácilmente la dirección IP de la definición de firma IPS.		
36	El Visor de registro debe tener la capacidad de excluir fácilmente la dirección IP de los registros de IPS cuando se detecta como falso positivo		
37	La GUI de administración debe tener la capacidad de acceder fácilmente a la definición de firmas IPS a partir de los registros de IPS		
38	Debe soportar agendar reportes para que se ejecuten automáticamente para extraer información en periodos regulares de tiempo (diarios, semanales y mensuales). También debe permitir al administrador la fecha y horario en que empezará a generar el reporte agendado.		
39	El Visor de registro debe tener la capacidad de ver todos los registros de seguridad (fw, IPS, urlf ...) en un panel de visualización (útil cuando se soluciona un problema de conectividad para una dirección IP)		
40	La herramienta de reportes debe soportar al menos 25 filtros (ej. Origen, destino, nombre del ataque, número de regla) que permita personalizar los reportes predefinidos a las necesidades del administrador (ej. Actividades web de un usuario específico)		
41	El Visor de registro debe tener la capacidad en el visor de registro de crear un filtro utilizando los objetos predefinidos (hosts, red, grupos, usuarios ...)		
42	El Visor de registro debe tener la capacidad en el visor de registro para crear múltiples "filtros guardados" personalizados para usar en un momento posterior.		
43	La solución de administración de políticas debe proporcionar registros de reglas similares para el usuario a medida que crea o modifica reglas.		
44	La GUI de la solución debe proporcionar una navegación fácil entre cientos de políticas, cada una con hasta 1 millón de reglas. Se deben proporcionar saltos entre subpolíticas y títulos de sección, así como una búsqueda exhaustiva.		
45	La administración de políticas debe proporcionar la búsqueda de reglas por paquetes, incluso sin tener registros de ese paquete en el sistema. La búsqueda debe estar integrada en el mismo panel que la configuración de la política y devolver todos los resultados en pocos segundos.		
46	La solución de administración de seguridad debe proporcionar la búsqueda de todas las referencias a cualquier objeto de red dado en todas sus políticas y configuraciones (donde se usa).		

47	La solución debe proporcionar administración integrada de tickets. Se debe asociar automáticamente a una sesión un conjunto de cambios en la política de seguridad para lograr la responsabilidad y la documentación adecuadas.		
48	La administración de seguridad debe proporcionar un conjunto de mejores prácticas de seguridad incorporadas que proporcionan puntaje automático para varias regulaciones de seguridad.		
49	La administración de seguridad debe tener la opción de alertar a los usuarios sobre una posible configuración incorrecta, al tiempo que les proporciona una forma de agregar excepciones a estas posibles configuraciones erróneas.		
50	El usuario debe proporcionar detalles de NAT para un objeto de red en el alcance del objeto de red. Las reglas NAT inferidas se deben agregar automáticamente a la política NAT.		
51	El usuario debería ser capaz de tratar sin problemas los objetos IPV4, IPV6 y de red dinámica en la misma política.		
52	La pasarela de seguridad debe inspeccionar el tráfico de la red, el contexto de la aplicación y los datos y el contenido dentro de una regla.		
53	El sistema IPS debe proporcionar acciones automáticas en Protecciones IPS basadas en las definiciones del usuario de sus activos críticos.		
54	El sistema IPS debe proporcionar perfiles inteligentes en tres niveles en el eje de seguridad frente al rendimiento. El usuario puede optar por habilitar protecciones granulares o, en su lugar, elegir uno de los perfiles inteligentes.		
55	Al crear o editar políticas de seguridad se debe poder forzar el uso de una descripción, tag o comentario de auditoría. Esto con el fin de garantizar buenas prácticas de documentación y organización y auditoría.		
56	La solución de permitir modificar e instalar políticas al mismo tiempo por diferentes administradores de la solución.		
57	La solución a ofertar debe permitir hacer un check de la configuración realizada antes de hacer un instalación de políticas a fin de poder revisar cualquier mala configuración o solapamiento de políticas.		
58	La solución debe permitir configurar diferenciar roles a los usuarios administradores a fin de poder limitar su funciones y no tener un control global de la plataforma.		
O	Actualizaciones de prevención de amenazas		
1	El proveedor debe proporcionar los detalles de su mecanismo de actualización de prevención de amenazas y su capacidad para manejar ataques de día cero en todas las aplicaciones de prevención de amenazas de próxima generación, incluyendo IPS, Control de aplicaciones, filtrado de URL, Anti-Bot y Anti-Virus.		
2	El proveedor debe proporcionar detalles sobre la reclasificación de URL, en las circunstancias en que se ha incluido un sitio web y, posiblemente, la distribución de malware		
3	El proveedor debe tener la capacidad de proporcionar manejo de incidentes		
P	Registro y Monitoreo		
	El registro central debe ser parte del sistema de gestión.		
1	El visor de registros debe tener una capacidad de búsqueda indexada		
2	La solución debe tener la capacidad de registrar todas las aplicaciones de seguridad integradas en la puerta de enlace e incluir IPS, Control de aplicaciones, Filtrado de URL, Antivirus, Anti-Bot, Anti-Spam, Identidad de usuario, Prevención de pérdida de datos, Acceso móvil		

3	La solución debe incluir un mecanismo automático de captura de paquetes para eventos IPS para proporcionar un mejor análisis forense		
4	La solución debe proporcionar registros diferentes para la actividad habitual del usuario y los registros relacionados con la gestión.		
5	Debe proveer un reportador en tiempo real basado en una línea de tiempo, para reportes predefinidos o a la medida, permitiendo al administrador realizar análisis de contenido en tiempo real.		
6	La solución debe poder pasar del registro de registro de seguridad a la regla de política con un clic del mouse.		
7	Para cada regla de coincidencia o tipo de evento, la solución debe proporcionar al menos las siguientes opciones de eventos: registro, alerta, captura de SNMP, correo electrónico y ejecutar una secuencia de comandos definida por el usuario.		
8	Los registros deben tener un canal seguro para transferir el registro para evitar el espionaje, la solución debe ser autenticada y encriptada		
9	La solución debe incluir la opción de bloquear dinámicamente una conexión activa desde la interfaz gráfica de registro sin la necesidad de modificar la base de reglas		
10	La solución debe ser compatible con la exportación de registros en formato de base de datos		
11	La solución debe ser compatible con el cambio automático del archivo de registro, en función de un tiempo programado o tamaño de archivo		
12	La solución debe admitir la adición de excepciones a la aplicación de IPS del registro de registro		
13	La solución debe poder asociar un nombre de usuario y nombre de máquina a cada registro de registro		
14	La solución debe incluir una interfaz gráfica de monitoreo que proporcione una manera fácil de monitorear el estado de las puertas de enlace		
15	La solución debe proporcionar la siguiente información del sistema para cada puerta de enlace: sistema operativo, uso de la CPU, uso de la memoria, todas las particiones del disco y % del espacio libre en el disco duro.		
16	La solución debe proporcionar el estado de cada componente de la puerta de enlace (es decir, firewall, vpn, cluster, antivirus, etc.)		
17	La solución debe incluir el estado de todos los túneles VPN, sitio a sitio y cliente a sitio		
18	La solución debe incluir una configuración de umbral personalizable para tomar medidas cuando se alcanza un determinado umbral en una puerta de enlace. Las acciones deben incluir: Registrar, alertar, enviar una trampa SNMP, enviar un correo electrónico y ejecutar una alerta definida por el usuario		
19	La solución debe incluir gráficos preconfigurados para monitorear la evolución en el tiempo del tráfico y los contadores del sistema: reglas de seguridad superiores, usuarios P2P principales, túneles vpn, tráfico de red y otra información útil. La solución debe proporcionar la opción de generar nuevos gráficos personalizados con diferentes tipos de gráficos		
20	Solución debe incluir la opción de grabar vistas de tráfico y del sistema en un archivo para su posterior visualización en cualquier momento		
21	Solución debe ser capaz de reconocer fallos de funcionamiento y problemas de conectividad, entre dos puntos conectados a través de una VPN, y registrar y alerta cuando el túnel VPN está abajo		

22	Los reportes deben incluir una explicación acerca de las políticas que fueron violadas y que parte del contenido causó dicha violación.		
23	Los reportes debe mostrar los usuarios (cuando exista una tecnología de AD)		
24	Con el propósito de mejorar la administración, debe ser posible definir un número máximo de alertas para ser mostradas en la GUI, además poder definir un periodo de tiempo máximo para mostrar dichas alertas, por ejemplo mostrar solo las alertas generadas hace una hora.		
25	La solución debe contar con un mecanismo de revisión de políticas, previo a la instalación de las mismas, que ayude a buscar y corregir errores.		
26	El Servidor de administración, debe tener la opción de incorporar una base de datos, de mejores prácticas de seguridad, que provean una calificación, cuando se evalúen temas regulatorios/normativos (ej. ISO27000, NIST)		
27	La solución debe prevenir/ alertar al usuario administrador, cuando trate de realizar cambios que empeoren el alineamiento de la entidad frente a normativas/regulaciones de interés (ej. ISO 27000, NIST)		
28	El sistema de reportes debe proveer información consolidada sobre al menos: i. Top de eventos por origen ii. Top de eventos por destino iii. Eventos por fecha. iv. Eventos por semana. v. Top de eventos por producto vi. Top de eventos por servicios. vii. Severidad viii. Producto		
Q	Correlación de eventos y presentación de informes		
1	Solución debe incluir una herramienta para correlacionar eventos de todas las funciones de puerta de enlace y dispositivos de otros fabricantes		
2	La solución debe permitir la creación de filtros basados en cualquier característica del evento como aplicación de seguridad, IP de origen y destino, servicio, tipo de evento, nombre del evento ataque de la gravedad, país de origen y de destino, etc.		
3	La aplicación debe tener un mecanismo para asignar estos filtros para diferentes líneas de los gráficos que se actualizan en intervalos regulares que muestran todos los eventos que coincide con el filtro. Permitiendo que el operador se concentre en los eventos más importantes		
4	La aplicación de correlación de eventos debe suministrar una visión gráfica de los eventos en función del tiempo		
5	Solución debe mostrar la distribución de eventos por país en un mapa		
6	La solución debe permitir al administrador de eventos de grupo basada en cualquiera de sus características, incluyendo muchos niveles de anidamiento y exportar a PDF		
7	Solución debe incluir la opción de buscar dentro de la lista de eventos, profundizar en los detalles de la investigación y la medicina forense.		
8	Es la lista de eventos vista solución debe incluir la opción de generar automáticamente pequeños gráficos o tablas con el evento, el origen y la distribución de destino		
9	Solución debe detectar ataques de Denegación de Servicio que correlacionan eventos de todas las fuentes		

10	Solución debe detectar un inicio de sesión de administrador en horas irregulares		
11	Solución debe detectar ataques de adivinanzas de credenciales		
12	Solución debe informar sobre todas las instalaciones de la política de seguridad		
13	Solución debe incluir predefinido por hora, diaria, semanal y mensuales. Incluyendo al menos Top eventos, mejores fuentes, Principales destinos, mejores servicios, mejores fuentes y sus principales eventos, Principales destinos y sus principales eventos y mejores servicios y sus principales eventos		
14	La herramienta de informes debe ser compatible con al menos 25 filtros que permiten personalizar un informe predefinido para estar más cerca de las necesidades del administrador		
15	Solución debe ser compatible con la programación de informes automáticos para la información que necesitan para extraer de manera regular (diaria, semanal y mensual). Solución también debe permitir al administrador definir la fecha y hora en que comienza sistema de información para generar el informe programado		
16	Solución debe ser compatible con los siguientes formatos: informes HTML, CSV y MHT		
17	Solución debe ser compatible con la distribución automática de informes por correo electrónico, subir a un servidor FTP / Web y un script de distribución de informes personalizados externa		
18	Debe detectar ataques de denegación de servicio, correlacionando eventos de todas las fuentes.		
19	La consola de reportería o de administración debe tener la capacidad mostrar la matriz MITREK vs el evento de seguridad correlacionado.		
20	El sistema de información debe proporcionar información consolidada sobre:		
21	El volumen de conexiones que fueron bloqueados por la regla de seguridad.		
22	Principales fuentes de conexiones bloqueadas, sus destinos y servicios		
23	Top reglas utilizadas por la política de seguridad		
24	ataques de seguridad a nivel detectados por punto de aplicación (perímetro) que determinan sus principales fuentes y los destinos		
25	Número de políticas instalar y desinstalar en el punto de aplicación		
26	Top servicios de redes		
27	actividad en la web por el usuario que detalla los principales sitios visitados y los usuarios de Internet top		
28	Top servicios que crean la mayor parte de carga para el tráfico cifrado		
29	Los mejores usuarios en VPN que realizan las conexiones de más larga duración		
R	Mejor Práctica de Gobierno, Riesgo y Cumplimiento (GRC)		
1	La solución debe tener una modulo integrado de cumplimiento que permita supervisar los gateway, las políticas y ajustes de configuración de una manera dinámica y en tiempo real.		
2	La solución debe tener una módulo de cumplimiento que permita la supervisión de Cumplimiento en los diferentes módulos de seguridad		
3	La solución debe tener una módulo de cumplimiento que permita la evaluación en tiempo real de cumplimiento de las regulaciones principales de la industria (PCI-DSS, GDPR, HIPAA, SOX, ISO 27001, entre otros)		

4	La solución debe tener una módulo de cumplimiento que permita la notificación inmediata de los cambios de políticas que afecten el cumplimiento		
5	La solución debe tener una módulo de cumplimiento que permita proporcionar recomendaciones prácticas para mejorar el cumplimiento		
6	La solución debe tener una módulo de cumplimiento que permita recomendar Mejores prácticas de seguridad		
7	La solución debe tener una módulo de cumplimiento que permita traducir los requisitos reglamentarios en las mejores prácticas de seguridad accionable		
8	La solución debe tener una módulo de cumplimiento que permita el monitoreo en tiempo real de la puerta de enlace con las mejores prácticas de seguridad		
9	La solución debe tener una módulo de cumplimiento que permita generar informes de evaluación automatizada para calificar el cumplimiento de las regulaciones		
10	La solución debe tener una módulo de cumplimiento que permita comprobar el cumplimiento de todos los cambios en las políticas para los diferentes módulos de seguridad		
11	Capacidades		
12	Soportar puerto para conexión de consola serial RJ-45		
13	Soportar al menos 1024 VLANs a nivel la solución.		
14	Cada appliance gateway debe tener al menos 8 interfaces 10G SFP+ en Fibra con sus respectivos transceiver SFP+ y 8 interfaces 10/100/1000 en cobre y/o fibra con sus respectivos transceiver SFP, un puerto asignado para la administración vía consola, un puerto para administración y sincronización o HA independiente a las 8 interfaces de cobre a 1G.		
15	Cada appliance Gateway debe tener dos slot de expansión para intercambiar tarjetas de puertos, con la capacidad de colocar tarjetas de expansión de puertos de hasta 40GBase-F QSFP, con acceso frontal sin la necesidad de destapar todo el appliance.		
16	Cada Appliance gateway debe tener almacenamiento de dos discos duros de al menos 480 GB Estado Solido cada uno.		
17	La solución debe soportar 9.5 Gbps de throughput con todas sus funcionalidades activas por cada appliance gateway		
18	La solución debe soportar 25 Gbps de throughput de IPS por cada appliance gateway		
19	Cada appliance gateway debe soportar 22 Gbps de throughput de NGFW (FW, IPS, Control de aplicaciones)		
20	Cada appliance gateway debe manejar hasta 16 millones de conexiones concurrentes.		
21	Cada appliance gateway debe soportar 330 mil conexiones por segundo.		
22	Cada uno de los appliances gateway debe tener Doble fuente de poder hot-swap		

MODERNIZACIÓN TECNOLÓGICA DEL SISTEMA DE SEGURIDAD PERIMETRAL DE LA UNIVERSIDAD PEDAGÓGICA			
REFERENTES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS			
ITEM	REQUERIMIENTOS WAF	Cumple (SI)	¿Cómo se Verifica?
A	REQUERIMIENTOS GENERALES		
1	La solución debe incluir 1 WAF con capacidades de balanceador de carga		
2	La solución de Application Delivery Controller deberá estar ubicada en el cuadrante Leaders del informe Gartner Magic Quadrant for Application Delivery Controllers de los últimos tres años		
3	El equipo debe venir licenciado para soportar como mínimo un Throughput en L4/L7 de 6 Gbps		
4	El Equipo debe soportar crecimiento de throughput por licenciamiento sobre el mismo hardware de L4/L7 de 26/20 Gbps respectivamente. En caso de no soportar crecimiento a través de licenciamiento se deberá incluir una capacidad mínima de throughput de 26 Gbps.		
5	El Equipo debe soportar como mínimo 625000 conexiones por segundo en capa 4.		
6	El Equipo debe soportar como mínimo 50 Millones conexiones concurrentes en capa 4.		
7	Capa equipo debe soportar como mínimo 845000 request por segundo en capa 7.		
8	El equipo debe tener la siguiente capacidad en interfaces como mínimo (es necesario incluir los trancivers en fibra): - 8 puertos 1Gbps cobre y/o fibra - 2 puertos 10Gbps fibra (SR)		
9	El Equipo debe incluir un puerto de administración fuera de banda tipo RJ45 y otro USB para recovery.		
10	El Equipo debe incluir fuente de poder redundantes AC/DC hot swappable		
11	El Equipo debe incluir como mínimo un disco duro SSD de 500 GB de capacidad		
12	La solución debe ser capaz de integrarse con herramientas de automatización del mercado solamente utilizando software proporcionado por el fabricante, incluyendo al menos: OpenStack Vmware vRealize Orchestrator Cisco ACI Ansible Kubernetes		
13	La solución debe incluir un REST API donde se provea acceso completo a la funcionalidad el equipo, incluyendo crear, leer, actualizar o borrar información.		



B	REQUERIMIENTOS DE SWITCHING Y ROUTING		
1	La solución debe soportar link aggregation de acuerdo con el estándar 802.3ad, con capacidad de agregar hasta 8 puertos en físicos en un puerto lógico.		
2	La solución debe soportar LACP estático y dinámico		
3	La solución debe soportar los siguientes protocolos de spanning tree: - Spanning Tree Protocol STP (802.1D) - Rapid Spanning Tree RSTP (802.1w) - Multiple Spanning Tree MSTP (802.1s)		
4	La solución soporta como mínimo los siguientes tipos de NAT: - Dinámico: NAT muchos a uno. - Estático: NAT uno a uno. - Overlapping: Misma dirección IP, pero en diferentes VLAN.		
5	La solución debe soportar como mínimo los siguientes protocolos de enrutamiento: - RIPv1 y RIPv2 - BGP - OSPF y OSPFv3		
C	ADMINISTRACIÓN LOCAL DE LA PLATAFORMA		
1	La solución debe soportar administración local vía SSH y WBM (Web Based Management) vía HTTPS y debe permitir personalizar el certificado digital a presentar.		
2	La solución debe permitir crear reglas de acceso a la administración a través de la definición de las IP que podrán acceder y especificando los protocolos de administración.		
3	La solución debe permitir especificar límites de tasa de tráfico sobre el tráfico de administración		
4	La solución debe soportar autenticación local, RADIUS y TACACS+		
D	REQUERIMIENTOS DE BALANCEO LOCAL DE SERVIDORES (SLB)		
1	La solución debe balancear el tráfico enviado desde los clientes a través de la exposición de un servicio virtual y posterior entrega del tráfico a un grupo de servidores reales a balancear.		
2	La solución debe soportar las siguientes topologías IP - IPv4 pura, con clientes y servidores reales en IPv4. - IPv6 pura, con clientes y servidores reales en IPv6. - Clientes IPv4 y servidores en IPv6 o servidores IPv4 y clientes IPv6		



3	La solución debe soportar balanceo transparente, en donde se realice inspección del tráfico, clasificación y envío a uno o más grupos de balanceo, sin alterar el paquete original.		
4	La solución debe permitir filtrar el tráfico, permitiendo aceptar o denegar el mismo, utilizando como mínimo los siguientes parámetros: - Dirección MAC. - Dirección IP. - Protocolo. - Banderas TCP. - Tipos de mensaje ICMP. - Puertos capa 4. - String en Capa 7.		
5	La solución debe permitir configurar el máximo número de conexiones permitidas por servidor real.		
6	La solución debe permitir configurar peso sobre los servidores para trabajar con algoritmos de balanceo basados en el peso otorgado.		
7	La solución debe modificar los pesos asignados de forma dinámica basada en resultados de monitoreo de salud enviados vía SNMP.		
8	La solución debe permitir configurar un servidor real de backup para cada servidor real definido, el cual asumirá la carga en caso de que el servidor real principal falle.		
9	La solución debe soportar la definición de servidores reales a través de su FQDN.		
10	La solución debe soportar al menos los siguientes algoritmos de balanceo: - Hash - Persistent Hash - Tunable Hash - Weighted Hash - Highest Random Weights - Least Connections - Least Connections Per Service - Round-Robin - Response Time - Bandwidth		
11	La solución debe soportar chequeos de salud para validar el estado de los servidores reales objetos de balanceo, soportando al menos los siguientes métodos predefinidos: TCP, half-open TCP, ICMP, HTTP/S, DNS (TCP & UDP based), TFTP, SNMP, FTP, POP3, SMTP, IMAP, NNTP, RADIUS, SSL, LDAP/S, WAP, ARP, DHCP, RTSP		
12	La solución debe permitir personalizar y crear nuevos chequeos de salud con base en los chequeos de salud predefinidos.		



13	La solución debe permitir crear nuevos chequeos de salud utilizando scripts		
14	La solución debe permitir configurar chequeos de salud compuestos de chequeos individuales, a través de expresiones lógicas.		
15	La solución debe soportar balanceo por contenido HTTP de forma nativa y sin scripting adicional, utilizando al menos los siguientes elementos del protocolo HTTP para la creación de las reglas: - URL hostname - URL Path - URL Page name - URL page Type - Cualquier encabezado HTTP - Cookies - Texto específico en el encabezado o en el cuerpo del mensaje. - XML tags		
16	La solución debe permitir la inclusión de la IP original del cliente en un header HTTP para preservar la IP en caso de NAT de cliente.		
17	La solución debe permitir controlar los códigos de respuesta HTTP enviados por los servidores reales		
18	La solución debe permitir ocultar la información de identidad de los servidores HTTP balanceados, modificando las respuestas enviadas por los servidores reales.		
19	La solución debe permitir modificaciones de contenido en las respuestas enviadas por los servidores o en las solicitudes realizadas por los clientes, de forma nativa, sin necesidad de script, en al menos los siguientes elementos HTTP: - HTTP Headers: Podrán ser insertados, reemplazados o removidos. - Cookies - File Type - Status Line - URL -Text		
20	La solución debe permitir la personalización de la entrega de aplicación a través de scripts escritos por los usuarios.		
21	La solución debe soportar persistencia utilizando la dirección IP de origen.		
22	La solución debe soportar persistencia a través de cookie utilizando los siguiente métodos: - Cookie Insert. - Cookie Re-write. - Cookie Passive.		



23	La solución debe soportar persistencia basada en cualquier parámetro del header o el cuerpo del mensaje HTTP, incluyendo Tags de XML		
24	La solución debe soportar persistencia a través de SSL Session ID.		
25	La solución debe soportar persistencia a través de SIP Call ID.		
26	La solución debe soportar persistencia en Windows Terminal Server		
27	La solución debe soportar persistencia para cualquier protocolo TCP/UDP a través de scripting.		
E	REQUERIMIENTOS DE OPTIMIZACIÓN GENERAL		
1	La solución debe soportar caching conforme al RFC 2616		
2	La solución debe utilizar la memoria RAM para almacenar el contenido "cacheado" y la cantidad de RAM destinada para el cache podrá ser definida en la configuración.		
3	La solución debe incluir la funcionalidad de compresión HTTP		
4	La funcionalidad de compresión deberá soportar al menos los siguientes algoritmos de compresión: - gzip - Deflate		
5	La solución debe soportar HTTP multiplexing incluso si el servicio virtual se encuentra configurado con SSL offloading, caché y compresión.		
6	La solución debe soportar TCP pooling para mejorar el overhead que impone el establecimiento y terminación de las conexiones TCP con los servidores reales.		
7	La solución debe permitir definir políticas de optimización TCP que se podrán aplicar de forma independiente a la comunicación de cara al cliente y a la comunicación de cara al servidor.		
8	La solución debe soportar HTTP/2 Gateway, con la conexión de cara al cliente en HTTP/2 y de cara al servidor en HTTP 1.1		
9	La solución debe soportar HTTP/2 Full Proxy con cliente y servidor en HTTP/2.		



10	La solución debe soportar aceleración a través de SSL offloading como mínimo para los siguientes protocolos: - HTTPS - SSL Genérico - SIP - SMTP (STARTTLS) - IMAP (STARTTLS) - POP3 (STARTTLS) - LDAP (STARTTLS) - FTPS		
11	La solución debe soportar SSLv3, TLSv1, TLSv1.2, TLSv1.3		
12	La solución debe soportar SNI para mantener múltiples hosts detrás de una única IP y puerto.		
13	La solución debe soportar FIPS 140-2 Level 3, a través del uso de un HSM integrado		
14	La solución debe soportar HSM de red y ser compatible con SafeNet Luna Network HSM 7 de Gemalto/Thales		
15	La solución debe contar como mínimo con el siguiente desempeño de SSL: - RSA CPS (llaves de 2K): X - ECC CPS (P256): Z - SSL Throughput (Gbps): W		
F	REQUERIMIENTOS DE OPTIMIZACIÓN DE DESEMPEÑO EN CAPA DE APLICACIÓN WEB		
1	La optimización de desempeño WEB debe permitir trabajar en un modo aprendizaje, en donde no se apliquen las técnicas configuradas, pero si se pueda probar el sitio a través de una URL específica.		
2	La solución debe soportar PUSH Automático en HTTP/2, basado en el análisis del sitio, para enviar los recursos al navegador tan rápido como sea posible.		
3	La solución debe soportar técnicas de aceleración específicas para dispositivos móviles		
4	La solución debe soportar optimización específica por tipo de navegador.		
5	La solución debe soportar Predictive Browser Caching permitiendo precargar recursos del sitio web para acelerar la carga del mismo.		
6	La solución debe soportar la consolidación de los siguientes recursos dinámicos: - Consolidación de CSS. - Consolidación de Javascripts - Consolidación de Imágenes.		
7	La solución debe soportar el rendering progresivo de las imágenes, permitiendo comprimir las imágenes, cargarlas		



	en una resolución menor y luego mejorarla una vez la página haya sido cargada.		
8	La solución debe soportar compresión de imágenes usando configuración específica para cada dispositivo: Desktop, Dispositivos Móviles y Tabletas.		
G	REQUERIMIENTOS DE BALANCEO GLOBAL		
1	La solución debe permitir el balanceo de tráfico a través de múltiples sitios físicos.		
2	La solución debe permitir redirección global basada en los siguientes métodos: DNS, HTTP y Proxy (NAT de los clientes) para las aplicaciones que no usen DNS ni sean HTTP.		
3	La redirección DNS debe soportar DNSSEC		
4	La solución debe monitorear el estado de los balanceadores en sitios remotos, como mínimo: - Tiempo de respuesta de los servidores - Uso de la CPU - Disponibilidad y uso de sesiones		
5	La solución debe soportar como mínimo las siguientes reglas de balanceo global: - Red o redes de origen. - Ubicación geográfica. - Menor número de conexiones. - Roundrobin - Weighted Roundrobin - Menor tiempo de repuesta - Combinación de tiempo de respuesta y menor número de conexiones. - Ancho de banda - Proximidad, midiendo el tiempo de respuesta entre cada datacenter y el cliente - Persistencia - Hash de la IP de origen y el nombre del dominio		
6	La solución debe permitir la configuración de balanceo global, aún estando detrás de un dispositivo que realice un NAT de las direcciones IP públicas como un Firewall y no debe requerir hardware adicional para realizar esto.		
H	REQUERIMIENTOS DE BALANCEO DE ENLACES		
1	La solución debe soportar balanceo de enlaces para tráfico entrante y para tráfico saliente.		
2	El balanceo de enlaces debe contar con al menos las siguientes opciones de despliegue: - Capa 3 o modo ruteo - Capa 2 o modo bridge		



3	La solución debe permitir definir los enlaces a balancear especificando: - Dirección IP del router de upstream. - Chequeo de salud por enlace. - NAT a configurar para el balanceo de salida		
4	La solución debe permitir configurar reglas de balanceo de salida que permitan clasificar el tráfico y balancearlo de acuerdo a las características del mismo.		
5	El balanceo de enlaces de salida debe permitir clasificar el tráfico con al menos los siguientes parámetros: - Vlan - Dirección IP Origen/destino - Puerto Origen/Destino - Protocolo - Contenido a capa 7 - Estático definiendo los grupos por donde se debe enviar el tráfico		
6	La solución debe contar con al menos las siguiente métricas en el balanceo de salida para determinar el mejor enlace: - Least Connections - Round-Robin - Response Time - Bandwidth		
7	La solución debe soportar al menos los siguientes tipos de conversiones de direcciones de red (NAT): - No NAT: que el tráfico se reenvíe de forma transparente - NAT dinámico - NAT estático - NAT de prefijos de IPv6		
8	En cuanto al balanceo de enlaces entrante, la solución debe actuar como un DNS autoritativo para las URLs balanceadas		
9	La solución debe soportar al menos los siguientes tipos de records: A, AAAA y PTRs.		
10	La solución debe soportar al menos las siguientes métricas para el balanceo de enlaces entrante: - Red o redes de origen. - Ubicación geográfica. - Menor número de conexiones. - Roundrobin - Weighted Roundrobin - Menor tiempo de repuesta - Combinación de tiempo de respuesta y menor número de conexiones. - Ancho de banda - Persistencia - Hash de la IP de origen y el nombre del dominio		



11	La solución debe incluir una métrica por proximidad que correlacione la latencia y el número de saltos hacia un origen determinado, para el balanceo de salida y desde un origen determinado para el balanceo entrante.		
I	REQUERIMIENTOS DE VIRTUALIZACIÓN		
1	La solución debe soportar instancias virtuales de balanceo que se ejecuten sobre un hypervisor de balanceo especializado.		
2	La propuesta debe incluir como mínimo con 5 balanceadores virtuales con capacidades de WAF y con posibilidad de crecimiento hasta 22 instancias sin necesidad de modificar el hardware propuesto.		
3	La solución debe soportar administración independiente para cada uno de los balanceadores virtuales configurados.		
4	La solución debe permitir asignar recursos físicos independientes, CPU, Memoria, sobre cada instancia virtual y WAF; los recursos físicos asignados no debe compartirse entre las instancias virtuales de balanceo.		
5	La solución debe permitir que cada balanceador virtual maneje su propia infraestructura de red independiente, tanto en capa 2 como en capa 3, incluyendo protocolos de enrutamiento dinámicos.		
6	La solución soporta múltiples imágenes de software por cada balanceador virtual. Cada balanceador podrá correr una imagen de software distinta.		
7	La solución debe permitir realizar actualización sobre una instancia virtual sin afectar las otras instancias virtuales aprovisionadas.		
8	La solución debe permitir asignar recursos físicos independientes para la funcionalidad de Optimización de desempeño Web.		
9	La solución debe permitir asignar recursos físicos independientes para la funcionalidad de Web Application Firewall, para evitar que el balanceador y el WAF comportan los mismos recursos.		
J	REQUERIMIENTOS DE SEGURIDAD		
1	La solución debe soportar ACL (listas de control de acceso) para controlar el acceso a los dispositivos que conforman la solución y a los servidores balanceados		
2	La solución debe permitir configurar rate limits en TCP, UDP e ICMP.		
3	La solución debe permitir configurar manualmente patrones de ataques y luego crear reglas de bloqueo de tráfico TCP o UDP, basadas en dichos patrones de tráfico.		



4	La solución debe permitir generar y enviar alertas vía syslog y snmp, a otros dispositivos de seguridad, cuando se superen, como mínimo, los siguientes thresholds: - Ancho de banda. - Conexiones por Segundo. - Latencia. - Paquetes por segundo.		
5	La solución debe incluir IP reputation, con configuración de acciones, Alertar, Permitir y bloquear, de acuerdo con: - La región (ubicación) - La categoría: Tor Exit Nodes e IP Maliciosas - El nivel de riesgo.		
6	El balanceador debe contar con la posibilidad de integración nativa a futuro con un servicio de administración de bots (Bot Management) del mismo fabricante, con las siguientes características mínimas: - Configuración por servicio virtual. - Soportar aplicaciones WEB, aplicaciones móviles y API. - Soportar análisis de comportamiento para análisis de intención, inteligencia colectividad de bots, fingerprinting de browsers y de máquinas. - Permitir desde el balanceador, configurar al menos las siguientes respuestas ante ataques detectados: Permitir, Captcha, Bloqueo.		
K	REQUERIMIENTOS DE INSPECCIÓN SSL		
1	La solución debe proveer visibilidad SSL/TLS para ambos, el tráfico hacia el Datacenter y el tráfico saliente a Internet, permitiendo a la solución ser la responsable de la orquestación y distribución dinámica de tráfico entre dispositivos de seguridad.		
2	La solución de inspección SSL debe soportar al menos los siguientes tipos de despliegue: - Solución transparente en capa 2. - Dispositivo en modo ruteo en capa 3.		
3	En cuanto al número de dispositivos, la solución deberá poder desplegarse: - Solución de una sola instancia. - Solución con dos (2) instancias utilizando dos equipos físicos o dos instancias virtuales		
4	La solución debe ser diagnóstica a los dispositivos de seguridad conectados y debe soportar como mínimo, los siguientes tipos de dispositivos de acuerdo a su tipo de despliegue de red: - Dispositivos en capa 3, que pueden estar conectados en one-leg o two-legs. Ejemplos: Antimalware, Firewalls. - Dispositivos en capa 2 conectados en two-legs. Ejemplo: ATP, IPS.		



	- Dispositivos pasivos en donde solo se copie el tráfico, como DLPs e IDS. Conectados en one-leg. - La solución debe soportar dispositivos tipo ICAP, como DLP activos y anti-virus.		
5	La solución para la inspección SSL de salida debe soportar Proxy Transparente y Proxy Explícito.		
6	La solución para la inspección SSL debe soportar bypass de inspección SSL la cual podrá definirse como mínimo a través de: - Dirección IP origen o destino. - Sitios específicos o categorías. Se debe incluir todo el licenciamiento.		
7	La solución para la inspección SSL de salida debe detectar tráfico HTTPS y enviar para inspección en: - Un puerto específico definido - Rango de puertos TCP. - Cualquier puerto TCP.		
8	La solución debe soportar la inspección de protocolos distintos a HTTP y que sean transportados sobre SSL/TLS: - Conexiones SSL/TLS - SSL/TLS explícitas, solicitadas vía STARTTLS para SMTP, IMAP y POP3 y AUTHTLS para FTP. - Conexiones implícitas SSL, cualquier tráfico no-http.		
9	La solución debe soportar múltiples grupos de dispositivos de seguridad en la cadena de inspección.		
10	La solución debe permitir agrupar los dispositivos de seguridad y balancear el tráfico hacia los dispositivos definidos en los grupos.		
11	La solución debe permitir crear políticas de inspección que definan a que grupos de dispositivos de seguridad se debe enviar el tráfico a ser inspeccionado.		
12	La solución debe permitir crear políticas que permitan manejar el tráfico que NO debe ser inspeccionado, por ejemplo, el tráfico en texto plano.		
L	REQUERIMIENTOS DE WAF		
1	La solución debe incluir protección contra ataques en capa de aplicación WEB, WAF, y dicho WAF debe estar certificado por ICASA LABS		
2	La solución debe ofrecer protección de aplicaciones WEB contra amenazas registradas OWASP Top Ten vulnerabilities.		



3	La solución propuesta debe proteger contra ataques conocidos y ataques de día cero, soportando modelos de seguridad positivos y modelos de seguridad negativos		
4	La solución propuesta debe proteger contra mínimo los siguientes ataques en capa de aplicación WEB: - XSS - SQL injections - OS command injections - LDAP injections - SSI injections - XPath injections - Sensitive information leakage - Application DoS - CSRF - Parameter tampering - From field manipulation - Session hijacking - Cookie poisoning - Application buffer overflows - Brute Force attacks - Access to predictable resource locations - Unauthorized navigation - Web server reconnaissance - Directory/path traversal - Forceful browsing - Hotlink - HTTP response splitting - Evasion and illegal encoding - XML validation - Web services method restrictions and validation - HTTP RFC violations - HTTP request format and limitation violations - Use of revoked or expired client certificates - File upload violations - Clickjacking		
5	La solución debe incluir una suscripción que permita actualizar las firmas de ataques conocidos, base de datos de geolocalización e IP de proxies anónimos.		
6	La solución debe permitir configurar una página de bloqueo interna o utilizar una página de bloqueo externa por cada aplicación configurada		



7	La solución debe soportar los siguientes modos operacionales por cada aplicación configurada: - Modo Reporte - Modo Bloqueo - Modo bypass		
8	La solución debe incluir un mecanismo que permita priorizar los recursos de procesamiento otorgados a las aplicaciones más críticas		
9	La solución debe permitir los hostnames (virtual hosts) asociados a una aplicación, permitiendo usar wildcards en la definición de los hostnames y configurar políticas de seguridad por cada virtual host configurado		
10	La solución debe controlar el tiempo timeout de conexión de los clientes a nivel TCP, definiendo para cada aplicación protegida el TCP Timeout de la sesión.		
11	La solución debe controlar el tiempo timeout de conexión de los clientes a nivel HTTP, definiendo para cada aplicación protegida: - El tiempo que espera por datos de request del cliente. - El tiempo que espera por una respuesta por parte del servidor.		
12	La solución debe bloquear queries con valores de parámetros definidos, pero sin un nombre de parámetro asociado al valor (NULL parameter name).		
13	La solución debe permitir purgar múltiples slashes en las urls y cambiarlos por un solo slash. Este comportamiento podrá ser modificado por cada aplicación.		
14	La solución debe permitir analizar las cookies como parámetros restringiendo el tamaño y los caracteres permitidos dentro de ellas.		
15	La solución debe bloquear métodos que no estén en compliance con el RFC HTTP (rfc 2616)		
16	La solución debe proteger contra ataques de denegación de servicio de tipo low and slow a través de análisis de comportamiento		
17	La solución debe permitir reemplazar los mensajes de respuesta HTTP por mensajes personalizados por cada aplicación protegida.		
18	La solución debe configurar los tamaños de mensajes permitidos para los requerimientos del cliente y las respuestas enviadas por el servidor, permitiendo definir como mínimo: - El tamaño del cuerpo del mensaje - El tamaño total de los encabezados - El tamaño total de un solo encabezado - El tamaño total de headers individuales.		

19	La solución debe permitir configurar listas blancas, listas negras de direcciones IP y políticas por geolocalización.		
20	La solución debe contar con un mecanismo de bloqueo por origen que cuente con las siguientes características mínimas: - Debe hacer seguimiento a los ataques generados por una dirección IP en particular. - Debe hacer seguimiento a los ataques generados por un fingerprinting de dispositivo particular. - Dependiendo al nivel de ataque, la IP o el Fingerprinting serán bloqueados por un tiempo en minutos configurable. - Las IP o los fingerprinting de los dispositivos se podrán desbloquear desde el WBI de la solución		
21	La solución debe enviar las IP bloqueadas por el mecanismo de source blocking a un mitigador de ataques DDoS del mismo fabricante, para que este efectúe el bloqueo en el perímetro		
22	La solución debe descubrir de forma automática y a través del tráfico que cursa a través de ella, la estructura de cada aplicación web configurada.		
23	La solución debe incluir un mecanismo de generación automática de política basado en el auto descubrimiento y en un análisis de amenazas realizado sobre los paths descubiertos.		
24	El mecanismo de generación automática de políticas debe realizar como mínimo las siguientes acciones sin intervención humana: - Generar automáticamente los paths de cada aplicación - Configurar las protecciones para cada path configurado - Refinar las protecciones - Cambiar las protecciones de modo monitoreo a modo bloqueo		
25	La solución debe continuar auto descubriendo el sitio, modificando la política de seguridad y refinando las protecciones, aun estando sus protecciones en modo bloqueo		
26	La generación automática de políticas también debe ser capaz de ajustar automáticamente parámetros del protocolo HTTP, como mínimo: -Definición del tamaño de los mensajes HTTP permitidos. -Las propiedades de parsing del protocolo HTTP en URLs específicas o de forma global		
27	La solución debe permitir definir los métodos permitidos hacia una determinada aplicación o path dentro de la aplicación		

28	La solución debe contar con una protección que evalúe las solicitudes de los clientes y bloquee aquellas que no hagan match con las expresiones definidas, las cuales deben contar como mínimo con las siguientes opciones de configuración - host - Path dentro de la aplicación - Método HTTP - Página - Expresión Regular		
29	La solución debe contar con una protección contra ataques de fuerza bruta que bloquee intentos de atacantes de hallar el usuario y password de un usuario autorizado.		
30	La protección contra ataques de fuerza bruta debe validar las respuestas de autenticación enviadas por los servidores WEB y bloquear la IP origen en caso que se genere un número configurable de respuestas de autenticación invalidas.		
31	La solución debe usar un motor de análisis de consulta de base de datos para detectar comandos de tipo SQL que los hackers puedan usar para realizar una manipulación de datos.		
32	La solución debe permitir crear reglas para controlar el upload de archivos con al menos los siguientes parámetros: - Path de la aplicación. - Extensión del archivo - Método HTTP - Permitir descarga de los archivos		
33	La solución debe evaluar las respuestas de los servidores para determinar si estas están exponiendo información sensible, con al menos las siguientes características: - Debe redirigir a página de bloqueo o ocultar los caracteres, si la respuesta del servidor incluye información de tarjetas de crédito. - Debe redirigir a página de bloqueo o ocultar los caracteres, si la respuesta del servidor incluye un parámetro personalizado por el administrador a través de expresiones regulares.		
34	La solución debe incluir protección contra ataques dirigidos a WebServices, filtrando los componentes del WebService y validando cada uno de estos a través los distintos mecanismos de seguridad.		
35	La solución debe validar las operaciones SOAP detectando ataques de tipo diccionario, codificaciones, manipulación de estructuras y otras amenazas comunes, como inyección de SQL y manipulación de parámetros.		



36	La solución debe permitir importar el archivo WSDL y proveer al menos tres (3) niveles de validación: - Validar que la estructura del XML esté correcta. - Validar el XML y asegurar que los requerimientos usen operaciones permitidas. - Validar la estructura XML, la operación y que los mensajes estén en cumplimiento con los requerimientos definidos en el WSDL		
37	La solución debe analizar XML en una solicitud, extraer los valores y pasar la información por otros mecanismos de seguridad, para detectar y mitigar ataques		
38	La solución debe soportar protección a API permitiendo importar el documento de OpenAPI y proveer: - Visibilidad sobre los endpoints definidos. - Permitir únicamente el tráfico que haga match con los endpoints definidos en el documento. - El tráfico permitidos debe validarse por los otros mecanismos de seguridad de la solución. - Administración de cuota por cada endpoint definido.		
39	La solución debe permitir evaluar parámetros dentro de una solicitud de usuario detectando y bloqueando aquellas que no sean válidas de acuerdo a los siguientes criterios que podrán ser configurados: - Tipo de parámetro: Long, Float, Número, Letra, Alfa numérico, Expresión, Cadena, Null Parameter. - Longitud mínima. - Longitud máxima. - Si permite o no valores nulos.		
40	La solución debe permitir bloquear el acceso a path específicos dentro de la aplicación		
41	La solución debe permitir cifrar la información de cookies para mitigar ataques que busquen manipular el estado de la sesión		
42	La solución debe permitir cifrar la información en parámetros de tipo form, path y query para bloquear ataques que busquen manipular el estado de la sesión		
43	La solución debe incluir una base de datos de firmas de vulnerabilidades conocida.		
44	La solución debe permitir crear patrones personalizados para que sean validados junto con los incluidos en la base de datos de firmas de ataques conocidos.		
45	La solución debe permitir configurar protección contra ataques de tipo Directory Listing para un grupo de hosts o para un host en particular		
46	La solución debe permitir ofuscar la estructura real de la aplicación de un atacante potencial a través de la configuración de reescritura de la URL (URL Rewrite)		



47	La solución debe soportar device fingerprinting para realizar seguimiento a las actividades utilizando un identificador de dispositivo y no la dirección IP origen.		
48	La solución debe detectar bots de tipo motores de búsqueda para excluirlos de la lista de orígenes a los cuales se les hará seguimiento.		
49	La solución debe registrar al menos los siguientes eventos de auditoría: - Modificaciones de configuración. - Intentos de acceso no autorizados. - Reinicios de la solución o servicios.		
50	La solución debe registrar los eventos de seguridad detectados o bloqueados incluyendo como mínimo la siguiente información: - Severidad del evento - Fecha - Descripción corta del evento - El tipo de ataque. - Dirección IP origen - Geolocalización - Puerto Origen - Host - Path de la aplicación - URI - Nombre del Parámetro - Valor del Parámetro - Tipo de Parámetro		
51	La solución debe permitir refinar las políticas desde la vista de los eventos de seguridad.		
52	La solución debe permitir visualizar, para cada evento registrado, el header HTTP de la solicitud.		
53	La solución debe permitir visualizar, para cada evento registrado y si la protección específica está en modo monitoreo, el header HTTP de la respuesta del servidor.		
M	CONSOLA DE GESTIÓN		
1	La consola de gestión debe ser del tipo físico (appliance dedicado)		
2	La consola de gestión debe soportar la administración y monitoreo de los equipos que hacen parte de la propuesta. Es decir se debe administrar en balanceador físico, sus instancias virtuales y los módulos de WAF de cada instancia virtual.		
3	La consola de gestión permitirá asignar roles de administración y monitoreo de seguridad por cada uno de los equipos administrados.		



4	La consola de gestión debe permitir el acceso a la interfaz gráfica a través del protocolo HTTPS.		
5	La consola de gestión debe soportar autenticación remota a través de los protocolos de autenticación RADIUS, LDAP y TACACS+.		
6	La consola de gestión debe permitir la configuración de NTP.		
7	La consola de gestión deberá permitir el acceso por REST API. Todas las operaciones que puedan realizarse a través de esta API deben estar completamente documentadas.		
8	La consola de gestión deberá permitir contar con un repositorio de logs que permitan visualizar todos los cambios de configuración que se realizan sobre los equipos.		
9	La consola de gestión debe soportar al menos las siguientes alertas de auditoría y sistema: - Alarmas de servidor. - Alarmas generales del dispositivo (fan, CPU) - Mensajes de auditoría		
10	La consola de gestión debe permitir configuración de alertas a servidores de syslog y snmp externos		
11	La consola de gestión debe permitir sincronización con un servidor NTP		
12	La consola de gestión debe permitir visualizar la utilización de CPU de los dispositivos administrados		
13	La consola de gestión debe permitir creación de tareas calendarizadas para las actualizaciones de seguridad del dispositivo		
14	Desde la consola de gestión se podrá realizar la actualización de la versión principal de los equipos administrados		
N	ALERTAS Y REPORTE		
1	La consola de gestión debe permitir generar reportes históricos de los ataques detectados y mitigados por la solución		
2	La consola de gestión debe permitir programar tareas de reportes y enviar los reportes vía correo electrónico.		
3	La consola de gestión debe permitir configurar un rango de tiempo de hasta 1 año para la generación de reportes históricos		
4	Debe soportar formatos PDF, CSV y HTML para los reportes históricos		
5	Debe permitir la personalización del logo de la entidad en los reportes		
6	Debe permitir escoger la o las aplicaciones que harán parte del reporte		



7	La consola de gestión debe permitir búsquedas de eventos de seguridad a través de la definición de criterios de búsqueda. Como mínimo se deben incluir los siguientes criterios: - Nombre del Ataque - IP Origen e IP Destino - Nombre de la aplicación - Severidad - Tipo de amenaza		
8	La consola de gestión debe permitir anidar múltiples criterios a través de expresiones regulares		
9	Desde la consola de gestión se deben enviar alertas de ataques		
10	Debe permitir escoger las aplicaciones específicas sobre las cuales se realizará la configuración de la alerta		
11	Desde la consola de gestión se podrá personalizar el tipo de alertas que se enviarán a través de la creación de expresiones regulares con al menos los siguientes criterios: - Nombre del Ataque - IP Origen e IP Destino - Nombre de la aplicación - Severidad - Tipo de amenaza		
12	Desde la consola de gestión se podrá configurar la severidad de la alerta		
0	MONITOREO Y REPORTE DE LAS APLICACIÓN BALANCEADAS		
1	La consola de gestión centralizada debe contar con dashboards que resuman el estado de las aplicaciones balanceadas.		
2	Los dashboards deben entregar información de todos los balanceadores, incluyendo como mínimo: Nombre del dispositivo, estado de salud del equipo, IP de administración, factor de forma, versión, throughput, Conexiones por segundo, Conexiones por Segundo SSL y uso de CPU y memoria.		
3	Los dashboards debe contar con un monitoreo de todos los chequeos de salud configurados en los balanceadores.		
4	Los dashboards debe entregar al menos los siguientes valores totales de tráfico hacia las aplicaciones balanceadas: Throughput, Conexiones por Segundo y Conexiones Concurrentes		
5	Los dashboards debe mostrar el top de aplicaciones por Throughput y por Request por segundo		
6	Los dashboards debe mostrar información de Throughput, Conexiones por Segundo, Conexiones concurrentes, Request por segundo para cada aplicación por separado.		



7	Los dashboards debe mostrar información de Throughput, Conexiones por Segundo, Conexiones concurrentes para cada servidor real que hace parte de un grupo de balanceo		
8	Los dashboards debe mostrar por cada aplicación balanceada el round trip time total, el round trip time entre el cliente y el balanceador, el round trip time entre el balanceador y la aplicación y el tiempo de respuesta de la aplicación.		
9	Para el tráfico SSL los dashboards deben mostrar las conexiones por segundo por cada aplicación, de acuerdo a la versión de TLS utilizada		
10	Para el tráfico SSL los dashboards deben mostrar los algoritmos de intercambio de llaves por cada aplicación		
11	Para el tráfico SSL los dashboards deben mostrar el TOP de los Ciphers utilizados por cada aplicación		
12	Para el tráfico SSL los dashboards deben mostrar el porcentaje de handshakes rechazados por cada aplicación		
13	Para el tráfico SSL los dashboards deben mostrar las conexiones por segundo SSL dando estadísticas gráficas de las nuevas conexiones, las conexiones reusadas y aquellas rechazadas		
14	La consola de gestión debe incluir los logs de las transacciones que van a los sitios web publicados en los balanceadores.		
15	La consola de gestión debe almacenar hasta 3 meses de logs de transacciones que van a los sitios web publicados en los balanceadores.		
16	La consola de gestión debe permitir la navegación sobre los logs de transacciones, con al menos las siguientes características:		
17	Modificar el rango de tiempo de búsqueda		
18	Debe dar el número total de transacciones en un rango de tiempo seleccionado		
19	Debe clasificar las conexiones en transacciones normales y transacciones fallidas, mostrando el número total para cada una de ellas		
20	Por cada transacción debe entregar detalles del request, el response, el tiempo de respuesta, los parámetros del cliente que realiza la conexión, detalles de SSL y los detalles del balanceo		
21	Debe permitir búsquedas rápidas dentro de conjunto de logs transaccionales guardados, a través de criterios flexibles y pesonalizables.		
22	La consola de gestión debe permitir generar reportes históricos de las aplicaciones balanceadas		

23	La consola de gestión debe permitir programar tareas de reportes y enviar los reportes vía correo electrónico.		
24	La consola de gestión debe permitir configurar un rango de tiempo de hasta 1 año para la generación de reportes históricos		
25	Debe soportar formatos PDF, CSV y HTML para los reportes históricos		
26	Debe permitir la personalización del logo de la entidad en los reportes		
27	Debe permitir escoger las aplicaciones específicas sobre las cuales se ejecutará el reporte		
28	La consola de gestión debe permitir personalizar el contenido de los reportes con mínimo las siguientes estadísticas:		
29	Tiempo de Respuesta		
30	Throughput		
31	Conexiones Concurrentes		
32	Conexiones por Segundo		
33	Request por Segundo		
P	MONITOREO Y REPORTES DE SEGURIDAD WEB		
1	La consola de gestión debe contar con un dashboard que resuma los eventos de seguridad.		
2	El dashboard debe permitir seleccionar la información a mostrar, las aplicaciones y el rango de tiempo.		
3	El dashboard debe contener al menos los siguientes cuadros de información:		
4	Top de Ataques por categoría		
5	Top de Orígenes y Destinos		
6	Ataques por acción		
7	Top de Ataques por Severidad		
8	Geolocalización de los ataques		
9	La consola de gestión debe permitir generar reportes históricos de los ataques detectados y mitigados por la solución		
10	La consola de gestión debe permitir programar tareas de reportes y enviar los reportes vía correo electrónico.		
11	La consola de gestión debe permitir configurar un rango de tiempo de hasta 1 año para la generación de reportes históricos		
12	Debe soportar formatos PDF, CSV y HTML para los reportes históricos		



13	Debe permitir la personalización del logo de la entidad en los reportes		
14	Debe permitir escoger la o las aplicaciones que harán parte del reporte		
15	La consola de gestión debe permitir búsquedas de eventos de seguridad a través de la definición de criterios de búsqueda. Como mínimo se deben incluir los siguientes criterios:		
16	Nombre del Ataque		
17	IP Origen e IP Destino		
18	Nombre de la aplicación		
19	Severidad		
20	Tipo de amenaza		
21	La consola de gestión debe permitir anidar múltiples criterios a través de expresiones regulares		
22	Desde la consola de gestión se deben enviar alertas de ataques		
23	Debe permitir escoger las aplicaciones específicas sobre los cuales se realizará la configuración de la alerta		
24	Desde la consola de gestión se podrá personalizar el tipo de alertas que se enviarán a través de la creación de expresiones regulares con al menos los siguientes criterios:		
25	Nombre del Ataque		
26	IP Origen e IP Destino		
27	Nombre de la aplicación		
28	Severidad		
29	Tipo de amenaza		
30	Desde la consola de gestión se podrá configurar la severidad de la alerta		

MODERNIZACIÓN TECNOLÓGICA DEL SISTEMA DE SEGURIDAD PERIMETRAL DE LA UNIVERSIDAD PEDAGÓGICA			
REFERENTES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS			
ITEM	OTROS REQUERIMIENTOS HABILITANTES	Cumple (SI)	¿Cómo se Verifica?
A	OTRAS OBLIGACIONES DEL CONTRATISTA		
1	Realizar Instalación, afinamiento, configuración, pruebas y puesta en funcionamiento, cuando aplique, de los equipos y software suministrado tipo APPLIANCE-FIREWALL (hardware y software) que adquiera la Universidad.		

2	Realizar las nuevas configuraciones después de realizar el proceso de Instalación y actualización, se acordará el proceso de administración de cambios para la creación de nuevas reglas o configuraciones, previa aprobación de la UNIVERSIDAD PEDAGÓGICA NACIONAL.		
3	Instalación, Transferencia de conocimientos, capacitación, visitas proactivas Mensuales, Soporte telefónico Web y en sitio cuando se solicite, Durante la vigencia del contrato, 7x24. Incluye servicio de Monitoreo.		
4	Realizar la Actualización de nuevas versiones de software y parches, previa autorización de la UNIVERSIDAD PEDAGÓGICA NACIONAL y por medio del proceso de control de cambios, Durante la vigencia de las licencias.		
6	Realizar Backup de las configuraciones antes y después de cada cambio, con el fin de garantizar una respuesta oportuna en caso de alguna eventualidad que requiera la reconfiguración de los equipos utilizados en la solución.		
7	Aplicar las mejores prácticas sugeridas por el fabricante y aseguramiento de los servicios para minimizar los riesgos		
8	El proponente deberá entregar la documentación técnica detallada de toda la actualización realizada		
9	El proponente deberá entregar un informe técnico mensual durante el tiempo de garantía y/o soporte, del desempeño de la Plataforma Adquirida		
10	Deberá realizar análisis previo de la plataforma tecnológica actual: hardware, software, red de comunicaciones, condiciones ambientales y sistemas de información.		
11	Deberá efectuar Transferencia de conocimientos en los productos ofrecidos. Esta transferencia debe ser realizada virtual o en sitio, por una entidad certificada por el fabricante. Se debe adjuntar certificación dirigida a la Universidad Pedagógica emitida por el fabricante de dicha entidad.		
12	Realizar las Pruebas necesarias Para garantizar el buen funcionamiento de la solución		
13	Efectuar administración, Seguimiento, monitoreo a los equipos objeto del contrato.		
B	VISITAS, INCIDENCIAS DE MANTENIMIENTO, SOPORTE Y GARANTIA		
1	Para la prestación del servicio se requiere que el proponente cuente con un esquema de mesa de Ayuda, donde se puedan generar los reportes de incidentes frente a la prestación del servicio.		



2	Adjuntar la metodología utilizada y licencia o certificación del software utilizado para la Mesa de ayuda el cual sigue las mejores prácticas de ITIL		
3	Detectar y reaccionar oportunamente ante incidentes de seguridad de la información, de acuerdo a los de servicio (SLAs) expuestos		
4	Brindar constantemente recomendaciones que permitan obtener un mejor nivel de mitigación de riesgos derivados del uso de la tecnología.		
5	Se debe brindar un componente de alarma para la detección automática de eventos de seguridad, que faciliten la gestión de los mismos sobre la infraestructura tecnológica		
6	En caso de no ser posible la solución remota o telefónica, se requiere prestación del servicio en sitio, de acuerdo a los niveles de servicios pactados		
7	Una vez realizada la instalación, puesta en marcha del producto y soportada la estabilidad de la solución, durante la vigencia de las Licencias deberá realizar una visita mensual para validar el correcto funcionamiento de la solución.		
8	Se requiere servicio de análisis de log y generación de reportes de manera periódica.		
9	El contratista deberá brindar soporte remoto y/o en sitio dependiendo el nivel de criticidad de la solicitud realizada para fallas e implementaciones.		
10	Para el presente proceso el contratista debe colocar un gerente de proyectos. Ingeniero con Especialización en seguridad de la información. Experiencia como Auditor líder en la norma ISO27001 ver 2013, CISM (Certified Information Security Manager. Para lo cual deberá presentar Hoja de vida documentada, soportada y tarjeta profesional. Experiencia demostrable desarrollando proyectos de temas de sistemas de seguridad de la información. Adjuntar mínimo tres (3) certificaciones de su participación en dichos proyectos como gerente y/o consultor en procesos de seguridad informática.		
11	Realizar y presentar un (1) informe de vulnerabilidades que incluya lista de vulnerabilidades encontradas con su respectivo plan de remediación y efectuar la presentación y socialización al personal técnico de la Subdirección de Gestión de Sistemas de Información. Lo anterior, dentro del marco de la Norma ISO-27000.		
12	El proponente deberá adjuntar a la propuesta mínimo una certificación de haber realizado un análisis de vulnerabilidad en una entidad superior a 500 usuarios y		



	otra certificación adicional en una entidad de 3000 usuarios.		
13	El ingeniero que realizará el análisis de vulnerabilidad debe adjuntar mínimo 2 certificaciones de experiencia en mínimo 2 entidades en donde haya realizado, soportado consecutivamente durante 5 años esta labor de análisis de vulnerabilidades.		
14	Entregar un documento de continuidad de la operación de la Universidad en caso de fallas de seguridad, dentro del marco de la Norma ISO-22301.		
15	El proponente debe ser distribuidor autorizado del fabricante del equipo ofertado, lo cual debe acreditar, mediante presentación de certificación vigente, expedida por el representante en Colombia, no mayor a 15 días anteriores a la fecha del cierre de la presente Convocatoria Pública y dirigida a la UNIVERSIDAD PEDAGOGICA NACIONAL, donde se especifique se encuentra autorizado para vender y soportar técnicamente las soluciones de seguridad en Colombia.		
16	La garantía de todos los equipos y productos suministrado debe ser mínimo (1) Un año, a partir de la fecha de la aprobación de la póliza.		
17	El oferente deberá realizar el correspondiente soporte técnico en sitio (7x24) cada vez que se realice el requerimiento por fallas de funcionamiento del producto durante el tiempo de vigencia del contrato y de las licencias.		
18	El soporte deberá incluir la puesta en marcha de últimas versiones y actualizaciones necesarias para corregir problemas y efectuar mejoras sobre la solución y mantenerla actualizada en su última versión disponible en el mercado.		
19	El oferente debe ofrecer soporte técnico vía telefónica e Internet, como primer nivel de atención.		
20	El oferente debe realizar la Generación y envío de reportes mensuales del estado de la solución implementada durante la duración del contrato		
21	El proponente debe especificar claramente en su propuesta los datos mediante los cuales la UNIVERSIDAD PEDAGOGICA NACIONAL podrá solicitar los servicios de soporte y que deberán ser como mínimo: Una dirección de correo electrónico, un sistema de tickets vía web, un teléfono fijo y por lo menos una línea de celular, ésta última disponible 7 días x 24 horas a la semana. Durante la vigencia de las licencias, el proponente debe realizar dos (2) mantenimientos preventivos de la solución, para		



	ello debe entregar un plan de trabajo que contenga al menos: Nombre de la actividad, tiempo estimado, fecha estimada, posibles afectaciones y responsables. Así mismo, al finalizar el mantenimiento preventivo debe entregar un informe con los resultados de éste.		
22	La garantía ofrecida por el fabricante debe cubrir todos los incidentes por fallas de Hardware y Software. Si la falla no puede ser resuelta por el fabricante dentro de las 12 horas siguientes al reporte del incidente (Interrupción del servicio altamente crítica para la Universidad Pedagógica), el proponente se debe comprometer a gestionar con el fabricante, el cambio del equipo de las mismas o mejores condiciones técnicas, y a restablecer el servicio en un periodo adicional de máximo de 24 horas.		
23	El proponente deberá demostrar que cuenta con unos equipos Firewall Appliances del mismo fabricante de los equipos ofertados, que permitirán reemplazar los equipos que adquiera la Universidad en caso de alguna falla o indisponibilidad de los mismos.		
C	OTRAS CERTIFICACIONES Y CAPACITACIÓN DEL SISTEMA		
1	De acuerdo con lo establecido en el Artículo 5 de la resolución 2710 de 2017 del Ministerio de las Tecnologías de Información y Comunicaciones, el proponente deberá entregar certificación del fabricante en donde se evidencie que la solución ofertada soporta IPV6 nativo en coexistencia con IPV4, de la solución o servicios listados en las especificaciones técnicas mínimas, expedida por el fabricante.		
2	Los proponentes deben adjuntar certificaciones vigentes del fabricante dirigidas a la Universidad que incluya los siguientes aspectos:		
3	Carta expedida por el fabricante con autorización al distribuidor para vender lo requerido, dirigida a la Universidad Pedagógica Nacional, con fecha de expedición no mayor a quince (15) días antes del cierre de la presente convocatoria.		
4	Indicando que son aptos para el diseño en implementación, instalación y puesta en producción de la solución tecnológica ofrecida.		
5	El proponente debe haber renovado, licenciado, instalado o configurado mínimo 3 soluciones de características similares del mismo fabricante de Firewall de la solución ofertada en alta Disponibilidad. Adjuntar Certificaciones en		



	donde se describa: la Entidad, que expide la certificación, Objeto, Tiempo de ejecución, nombre, teléfono de quien firma la certificación.		
6	Se verificará la experiencia del proponente en la celebración y ejecución de máximo de tres (3) contratos cuyo objeto corresponda o esté relacionado con el de ésta convocatoria, ejecutados en los últimos 4 años anteriores a la fecha del cierre del presente proceso de selección cuya sumatoria sea igual o superior al 100% del presupuesto oficial representado en SMMLV. Dos (2) certificaciones de Entidades Educativas Públicas y Una (1) certificación de una Entidad del Sector Público.		
7	El proponente deberá capacitar mínimo 1 persona directamente con la marca de los equipos Firewall Ofrecidos. Se debe entregar igual número de Voucher para presentación exámenes de certificación.		
8	El proponente debe brindar capacitación de la solución instalada cuando la Universidad lo solicite. (mínimo una capacitación semestral).		
9	El proponente debe entregar en físico y en digital la documentación de la configuración del estado inicial y del estado posterior a la implementación de la solución.		
10	El proponente debe garantizar la capacitación y certificación de la solución ofrecida.		
11	El proponente debe contar como mínimo con dos (2) Ingenieros Certificados por el fabricante como expertos de la solución Firewall ofrecida. Adjuntar (Hoja de vida, certificaciones del fabricante, Parafiscales).		
12	La implementación de la solución Web Application Firewall debe hacerse directamente por parte del fabricante. Para lo cual debe contar con mínimo 2 ingenieros en Colombia con las siguientes certificaciones:		
13	Primer ingeniero. Certified information systems security professional , Ec-council certified ethical hacker. Certified Security Expert, Certified Security Administrator de la solución Firewall ofrecida y Certified Security Specialist, Certified Application Specialist de la solución Web Application Firewall ofrecida.		
14	El segundo Ingeniero Certified professional Services Enginer (de la solución Web Application Firewall ofrecida.)		
D	CERTIFICACIONES DEL GRUPO DE TRABAJO DEL PROPONENTE		
1	Un Ingeniero especialista en Proyectos Informáticos Certificado por el PMI como PMP, que actuará como Gerente y/o Líder del Proyecto.		



2	El Auditor del análisis de vulnerabilidades deberá ser certificado ISO 27001 y Ethical Hacking. Deberá aportar certificación de experiencia laboral del empleador contratante y/o representante del proveedor o fabricante donde conste haber dirigido al menos un equipo de auditores como auditor líder en ISO27001.		
---	--	--	--

(Firma del Proponente o de su representante legal)



PROFORMA NO. 5

EXPERIENCIA DEL PROPONENTE	
CONVOCATORIA PÚBLICA N° 5 de 2021	CONTRATAR LA ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UNA NUEVA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL (CLÚSTER DE FIREWALLS) Y DE APLICACIONES (FIREWALLS DE APLICACIONES WEB) PARA LA UNIVERSIDAD PEDAGÓGICA NACIONAL

CE RTI F. No.	FOLIO DE UBICA CIÓN EN EL RUP	NÚMERO CONSECUTI VO DEL REPORTE DEL CONTRATO EJECUTADO (RUP)	UNIVER SIDAD CONTRA TANTE	CÓDIGO DEL CONTRATO SEGÚN CLASIFICADOR DE BIENES Y SERVICIOS	No. CONTRATO Y OBJETO	PORCENTAJ E DE PARTICIPAC IÓN EN LA EJECUCIÓN DEL CONTRATO (%)	FECHA DE INICIO DEL CONTRAT O	FECHA DE TERMINA CIÓN DEL CONTRAT O	VALOR TOTAL DEL CONTR ATO EJECU TADO EXPRESADO EN SMMLV
1									
2									
3									

FIRMA: _____

Nombre del Representante Legal: _____

C.C. No. _____ de _____

Nombre o Razón Social del Proponente: _____

NIT: _____

**PROFORMA NO. 6
VALORES AGREGADOS OFRECIDOS**

ITEM	VALORES AGREGADOS	OFRECE (SI/NO)
1	Ofrecer una solución de SOC, donde se realice un monitoreo en tiempo real de los equipos implementados durante la duración del contrato, para de esta manera ser lo más proactivo posibles ante cualquier fallo y/o error que se pueda presentar en la infraestructura ofertada	
2	Dar curso para dos personas de certificación de la solución dictado directamente por el fabricante, incluido el Voucher para la presentación del examen de certificación	
3	Dar curso de la solución para cinco (5) personas de la entidad dictado fuera de las instalaciones de la universidad por un ente certificado por el fabricante con entrega de certificado de asistencia	
4	Transferencia de conocimiento y sensibilización de la norma ISO27000 y ISO27001 a los funcionarios de la unidad de sistemas de la UPN realizado en las instalaciones de la universidad (Aproximadamente 20 personas)	

Nombre y Firma representante legal C.C.

