INVITACIÓN A COTIZAR DE MAYOR CUANTÍA No. 0 21 - 2024

CAPÍTULO I - INFORMACIÓN GENERAL

1.1. **OBJETO**

La Universidad Colegio Mayor de Cundinamarca, requiere contratar "**LA ADQUISICIÓN E IMPLEMENTACIÓN DE UN CONJUNTO INTEGRAL DE HERRAMIENTAS DE SEGURIDAD PARA LA PROTECCIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD COLEGIO MAYOR DE CUNDINAMARCA.",** de acuerdo con las especificaciones técnicas descritas en el capítulo III de la presente invitación.

1.2. **ALCANCE DE LA INVITACIÓN**

La Universidad Colegio Mayor de Cundinamarca, comprende la adquisición e implementación de un sistema de Control de Acceso a la Red (NAC), una herramienta de Sandbox, una herramienta de correlación de eventos de ciberseguridad (SIEM), todas las anteriores con licenciamiento por 36 meses, además una Plataforma avanzada de gestión de vulnerabilidades autónoma y patch management en equipos por 12 meses. Se debe incluir soporte técnico a la implementación y fallas en la operación de las herramientas por 12 meses para asegurar el correcto funcionamiento y mantenimiento de estas, así como transferencia de conocimiento a los usuarios del departamento de sistemas de la institución en el manejo de las herramientas.

1.3. **PRESUPUESTO OFICIAL**

La Universidad Colegio Mayor de Cundinamarca cuenta con un presupuesto oficial de **MIL NOVECIENTOS CINCUENTA Y OCHO MILLONES SEISCIENTOS SESENTA Y SEIS MIL DOSCIENTOS NOVENTA Y NUEVE PESOS M/CTE ($1.958.666.299) M/CTE**. IMPUESTOS INCLUIDOS, con cargo al Certificado de Disponibilidad Presupuestal 1004 del 13 de noviembre de 2024.

El proveedor deberá contemplar todos los costos asociados al cumplimiento del objeto de la invitación.

1.4. **CRONOGRAMA Y TRÁMITE DEL PROCESO**

ACTIVIDAD	FECHA Y HORA	LUGAR
Publicación de la Invitación a cotizar	28 de noviembre de 2024	Página Web
Visita Técnica	02 de diciembre de 2024 a las 10:00 am	Sede Principal Universidad (Calle 28 # 5 b 02) Secretaría General (para la visita los oferentes deberán registrarse a través del correo recepcionpropuestas@unicolmayor.edu.co
Recepción de observaciones	06 de diciembre de 2024 hasta las 4:00 p.m.	Correo electrónico recepcionpropuestas@unicolmayor.edu.co
Respuesta a las observaciones	09 de diciembre de 2024	Se dará respuesta a través de la página web y/o a través de los correos suministrados
Recepción de oferta	10 de diciembre de 2024 hasta las 4:00 p.m.	Subdirección de Servicios Administrativos y Contratación de la Universidad (calle 28 5b-02)
Apertura de las propuestas en acto publico	10 de diciembre de 2024 a las 4:10 p.m	Subdirección de Servicios Administrativos y Contratación de la Universidad (calle 28 5b-02), se realizaría con los oferentes que deseen asistir, quedará registrado en acta de apertura de sobres
Verificación componente jurídico y Técnico – habilitante	11 de diciembre de 2024	Oficina Jurídica – OTICS - publicación en la página web
Plazo para subsanación de documentos jurídicos y Técnico Habilitante (si aplica)	12 de diciembre de 2024 Hasta las 3:00 p.m.	Correo electrónico: recepcionpropuestas@unicolmayor.edu.co

ACTIVIDAD	FECHA Y HORA	LUGAR
Verificación de documentos jurídicos y técnico habilitante subsanados	13 de diciembre de2024	Oficina Jurídica- OTICS - publicación en la página web.
Verificación componentes técnico- económico y Financiero	16 de diciembre de 2024	Subdirección financiera - OTICS - publicación en la página web.
Comunicado sobre selección de oferente	17 de diciembre de 2024 o antes si no hay lugar a subsanación del componente técnico- habilitante - Página WEB	

NOTA 1: Cualquier modificación o adición a los términos de referencia se hará mediante comunicado, que será publicado en la página WEB de la Universidad, antes de la fecha límite de recepción de ofertas de la presente invitación.

NOTA 2: Para efectos de subsanabilidad se dará aplicación al término definido en el cronograma,sin menoscabo del término definido por la Ley hasta antes de la adjudicación del proponente, cuando a ello hubiere lugar.
NOTA 3: La Universidad informará a los interesados, la oferta seleccionada, mediante comunicado publicado en la página Web.

NOTA 4: La presente invitación no es vinculante para la entidad, ni implica la obligación de aperturar el presente proceso lo cual se surte con la publicación de los pliegos definitivos.

Durante el término los interesados en el proceso podrán presentar observaciones a los pliegos, las cuales serán analizadas por la entidad contratante a efectos de evaluar la pertinencia de la modificación de estos.

1.4 VISITA TÉCNICA

Se realizará una visita técnica a la sede de la Universidad Colegio Mayor de Cundinamarca el día establecido en el cronograma, siendo el sitio de encuentro la calle 28 No. 5B-02, Oficina de Tecnologías de la Información y Comunicaciones, desde allí se desplazarán a cada una de las otras sedes de la UNIVERSIDAD en Bogotá.

Las personas interesadas en presentar su propuesta a la Universidad deberán asistir a la visita técnica en el sitio, día y hora indicados en el cronograma, los asistentes a la visita deben estar acreditados por la firma o empresa a la cual representan.

Es responsabilidad del PROPONENTE, inspeccionar y examinar los diferentes espacios donde se realizará el proyecto, así como con los riesgos previsibles y sobre todas las circunstancias que puedan afectar o influir de alguna manera el trabajo, los costos, los precios y en general, sobre todas las circunstancias que puedan afectar o influir en el cálculo del valor de su propuesta, siempre cumpliendo con la normatividad vigente.

El hecho de que los proponentes no se familiaricen con los detalles y condiciones bajo las cuales será prestado el servicio, no se considerará como excusa válida para posteriores reclamaciones a la UNIVERSIDAD.

Los proponentes que estén interesados en hacer la visita técnica en las instalaciones de la universidad deberán registrarse a través del correo electrónico recepcionpropuestas@unicolmayor.edu.co un día antes de la misma, conforme al cronograma, para ello, deberá indicar el nombre de la Empresa, NIT, nombre de los asistentes o representantes de la Empresa, poder para ejercer la representación de la sociedad y Cámara de comercio.

La visita técnica es opcional, quien pretenda asistir a la visita deberá inscribirse para la misma a través de correo electrónico recepcionpropuestas@unicolmayor.edu.co.

Es necesario que los asistentes, cumplan con los horarios establecidos de visita; Los interesados en presentar propuesta podrán asistir al sitio, día y hora mencionados en el cronograma, con el fin de que:

- Les sean indicadas las obligaciones del objeto del proyecto que se pretende contratar.
- Se les brinde una mayor información acerca del objeto y los alcances del contrato a celebrarse y resolver las posibles dudas que tengan al respecto.

De la visita técnica se levantará un acta que será suscrita por todos los asistentes y la Universidad.

1.5 MODALIDADES DE PARTICIPACIÓN

Podrán presentar oferta las **PERSONAS NATURALES CON ESTABLECIMIENTO DE COMERCIO, PERSONAS JURÍDICAS Y/O CONSORCIOS O UNIONES TEMPORALES** que estén legalmente habilitadas, que cumplan con todos los requisitos exigidos en la presente Invitación, que no se encuentren dentro de las causales de inhabilidad e incompatibilidad previstas en la Constitución Política de Colombia y en la ley cuya actividad u objeto social esté relacionado con el de la presente invitación.

NOTA PARA PERSONAS NATURALES: Deberán estar inscritas ante la Cámara de Comercio con matrícula vigente y renovada con más de tres (3) años de constituidas a la fecha de recepción de ofertas.

En el caso que el oferente seleccionado sea persona natural, debe allegar con la presentación de su oferta

a la invitación a cotizar su consentimiento, para que sus datos personales recolectados en atención al trámite del objeto a contratar, puede ser almacenados, consultados y verificados por la Universidad.

NOTA PARA PERSONAS JURÍDICAS: Deberán estar inscritas en la Cámara de Comercio con matrícula vigente, renovada y con más de tres (3) años de constituida a la fecha de recepción de ofertas y tener una vigencia de tres (03) años más a la fecha de finalización del contrato. El representante legal deberá tener las atribuciones para la firma del contrato u orden por cuantía igual o superior al presupuesto de la presente invitación.

NOTA PARA CONSORCIOS O UNIONES TEMPORALES: en caso de consorcios o uniones temporales conformados por personas naturales con establecimiento de comercio y/o personas jurídicas, cada uno de los integrantes debe presentar certificado de existencia y representación legal dando cumplimiento a los requisitos anteriores según corresponda y teniendo presente en todo caso que actividades u objeto social de los integrantes debe tener relación directa con el requerimiento de la presente invitación.

Así mismo, debe allegar el documento de constitución del consorcio o unión temporal debidamente diligenciado y firmado por el proponente, el cual deberá contar con la siguiente información o cumplir con los siguientes requisitos:

1. Acreditar que la duración del consorcio o unión temporal debe extenderse por el plazo del contrato, su liquidación y dos (2) años más.

2. La designación de un representante que deberá estar facultado para actuar en nombre y representación del Consorcio o Unión temporal. Igualmente deberá designar un suplente que lo reemplace en los casos de ausencias temporales o definitivas.

1.6 PLAZO, LUGAR DE EJECUCIÓN Y FORMA DE PAGO

1.6.1 Plazo de ejecución

El plazo de ejecución será de hasta doce (12) meses, contados a partir de la firma del acta de inicio del proyecto, previa aprobación de la garantía única por parte de la Oficina Jurídica de la UNIVERSIDAD o hasta que se acaben los recursos del monto agotable definido. Cuando el último día del plazo pactado coincida con un sábado, domingo, día festivo o descanso obligatorio, el plazo se vencerá hasta el final del primer día hábil siguiente.

1.6.2 Lugar de ejecución

El lugar de ejecución del objeto del contrato son todas las sedes de la UNIVERSIDAD COLEGIO MAYOR DE CUNDINAMARCA.

1.6.3 Forma de pago

La UNIVERSIDAD pagará al contratista el valor del contrato de prestación de servicios en Dos (2) partes dividas en los siguientes porcentajes:

Primer Pago: Correspondiente al ochenta por ciento (80%) del valor total del contrato, sujeto a la entrega de los bienes conforme a las especificaciones establecidas, documento expedido por el fabricante de la solución que acredite la vigencia y titularidad de las suscripciones adquiridas conforme a las especificaciones y tiempos de vigencia y garantía establecidos. Lo anterior, acompañado de la respectiva certificación de cumplimiento de este entregable, emitida por el supervisor del contrato.

Segundo Pago: Correspondiente al veinte por ciento (20%) del valor total del contrato, sujeto a la instalación, configuración y parametrización de las herramientas y suscripciones adquiridas, documento que acredite la vigencia del soporte y mantenimiento contados a partir de la activación de las suscripciones e informe de recibo a satisfacción del objeto contractual expedida por parte del Supervisor designado.

NOTA 1. El oferente deberá presentar certificación expedida por el revisor fiscal del proponente, cuando éste exista de acuerdo con los requerimientos de ley, o por el proponente (persona natural) o representante legal, en la que conste que el proponente ha cumplido con sus obligaciones frente al sistema de seguridad social integral, caja de compensación familiar, ICBF y SENA, de sus empleados durante los seis (06) meses anteriores a la fecha de cierre del presente proceso de selección, si hay lugar a ello, de acuerdo con lo establecido en el artículo 50 de la ley 789 de 2002, en el artículo 23 de la ley 1150 de 2007 y en el artículo 20 de la ley 1607 de 2012.

1.7 OFERTAS

La Universidad **NO aceptará ofertas parciales.**

1.8 RÉGIMEN JURÍDICO APLICABLE

De conformidad con el artículo 69 de la Constitución Política y el artículo 93 de la Ley 30 de 1992 y el Acuerdo 027 del 04 de octubre de 2022, la presente invitación y el Contrato que se celebre se sujetan al derecho privado y a la normatividad de LA UNIVERSIDAD.

La presentación de la propuesta implica la aceptación por el OFERENTE de las reglas contenidas en la presente invitación a cotizar, así como las previstas en las Normas y las disposiciones institucionales de LA UNIVERSIDAD. La presente invitación no da lugar a licitación ni a concurso alguno. Ésta será evaluada internamente por la Universidad, de acuerdo con su régimen propiode contratación.

La UNIVERSIDAD se reserva el derecho a modificar, interpretar el contenido, cancelar la invitación o no contratar la misma.

CAPITULO II - PROPUESTA

2.1 PRESENTACIÓN DE LA PROPUESTA

EL PROPONENTE deberá elaborar la propuesta por su cuenta, riesgo y bajo su responsabilidad de acuerdo con lo solicitado en esta Invitación y sus modificaciones, si a estas hubiere lugar, e incluirá dentro de ella toda la información exigida.

2.2 LUGAR DE PRESENTACIÓN DE LA PROPUESTA

Las Propuestas deberán ser radicadas y entregadas en sobres sellados, en la Subdirección de Servicios Administrativos y Contratación de la Universidad Colegio Mayor de Cundinamarca, ubicada en la Calle 28 N° 5 B – 02 de la ciudad de Bogotá D.C., en la fecha y hora señalada en el cronograma del proceso de la Invitación Pública.

Después de la hora establecida como límite en el cronograma no se recibirá ninguna propuesta.

Las propuestas presentadas en forma extemporánea se entenderán no presentadas, y por tal motivo no harán parte del proceso precontractual y se procederá a su devolución en cualquier momento.

La entidad no asume ninguna responsabilidad si los oferentes no presentan sus ofertas a tiempo en el sitio indicado, por retrasos de ingreso a la institución o ubicación del sitio de radicación de la oferta.

Para el efecto, la Institución llevará un registro de entrega de las propuestas, el cual contendrá la fecha y hora de presentación, nombre del proponente, teléfono, dirección, correo electrónico, y nombre de la persona que entrega con su respectiva firma.

Las propuestas y todos los documentos que las acompañen deben obligatoriamente entregarse en sobres cerrados dirigidos a la entidad.
No se recibirán propuestas que lleguen por fax o correo electrónico.

No se aceptarán propuestas complementarias o modificaciones que fueran presentadas con posterioridad a la fecha y hora de cierre del presente proceso de contratación.

2.3. FORMA DE PRESENTACIÓN DE LA PROPUESTA

La propuesta deberá presentarse por escrito, en un (01) original y una (01) copia simple, en idioma español debidamente legajadas y foliadas con sello en orden consecutivo ascendente, sin incluir

hojas en blanco y con su respectivo índice, de igual manera se solicita una copia integral de la propuesta por medio de USB.

Para los casos de Consorcio o Uniones Temporales, la propuesta debe venir suscrita por el representante legal del Consorcio o unión temporal.

Para efectos de la presentación de la se reitera que deberá presentarse debidamente foliada, junto con todos sus anexos y **DEBIDAMENTE FIRMADA**, en sobres cerrados y rotulados, de la siguiente manera:

UNIVERSIDAD COLEGIO MAYOR DE
CUNDINAMARCA
Subdirección de Servicios Administrativos
y Contratación
(Proponente e Identificación)
INVITACIÓN A COTIZAR 021-2024
Dirección: Calle 28 5B-02
Bogotá D.C, Colombia

2.4. CIERRE DEL PROCESO DE SELECCIÓN Y APERTURA DE LAS PROPUESTAS

El proceso de selección se cerrará el día y a la hora señalada en el numeral **1.3 CRONOGRAMA DEL PROCESO**, para lo cual se expedirá la correspondiente acta de cierre.

La Entidad, en su sede Administrativa, procederá a la apertura de las propuestas en acto público, en el mismo día y hora indicada en el cronograma.

2.5. VALIDEZ DE LA PROPUESTA

La propuesta deberá permanecer vigente por un período de noventa (90) días calendario, a partir de la fecha límite de recepción de propuestas de la presente invitación. La Universidad podrá solicitar, si ello fuera necesario, la ampliación de la vigencia de la propuesta y por ende la ampliación de la garantía de seriedad por el término que se requiera.

Si por cualquier circunstancia se amplía el trámite del proceso y el proponente presenta una

ampliación a la garantía de seriedad de la propuesta que abarque este término, se entenderá, con dhecho de la presentación de dicha ampliación que mantiene la totalidad de las condiciones de la oferta.

La propuesta junto con los ajustes que se puedan presentar por solicitud de la Universidad formará parte integral del contrato. Se considera como documento oficial de la invitación, el que reposa en la Subdirección de Servicios Administrativos y Contratación de la Universidad.

La validez de la entrega de la propuesta queda sujeta a que la misma se realice tanto en el sitio como en la fecha y hora establecida para tal efecto en los términos de la invitación. Por lo tanto, no se debe hacer entrega en lugar diferente.

Nota: Si se presenta alguna discrepancia entre las cantidades expresadas en letras y números, prevalecerán las cantidades expresadas en letras. En caso de presentarse errores en el resultado final de la sumatoria de la propuesta económica, la Universidad, con base en los valores unitarios efectuará la operación matemática respectiva.

2.6. COMUNICACIONES

Cualquier comunicación con la Universidad podrá dirigirse al correo electrónico recepcionpropuestas@unicolmayor.edu.co

La **UNIVERSIDAD** enviará al proponente cualquier comunicación y/o notificación al correo electrónico registrado en el ANEXO 1 de la propuesta presentada.

CAPITULO III - ESPECIFICACIONES

La Universidad Colegio Mayor de Cundinamarca, requiere "**LA ADQUISICIÓN E IMPLEMENTACIÓN DE UN CONJUNTO INTEGRAL DE HERRAMIENTAS DE SEGURIDAD PARA LA PROTECCIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD COLEGIO MAYOR DE CUNDINAMARCA.",** de acuerdo con las siguientes especificaciones, las cuales, son la base para la elaboración del ANEXO 2, así:

3.1 ESPECIFICACIONES TÉCNICAS

Alcance del Proyecto

La Universidad Colegio Mayor de Cundinamarca, comprende la adquisición e implementación de un sistema de Control de Acceso a la Red (NAC), una herramienta de Sandbox, una herramienta de correlación de eventos de ciberseguridad (SIEM), todas las anteriores con

licenciamiento por 36 meses además una Plataforma avanzada de gestión de vulnerabilidades autónoma y patch management en equipos por 12 meses. Se debe incluir soporte técnico a la implementación y fallas en la operación de las herramientas por 12 meses para asegurar el correcto funcionamiento y mantenimiento de estas, así como transferencia de conocimiento a los usuarios del departamento de sistemas de la institución en el manejo de las herramientas.

Se deben tener en cuenta las siguientes características, las cuales se deben allegar junto con la propuesta:

HERRAMIENTAS A ADQUIRIR
CONTROL DE ACCESO A LA RED (NAC)
Adquisición de un sistema de Control de Acceso a la Red (NAC) que permita la gestión proactiva y mitigación de riesgos de seguridad mediante el uso de mecanismos combinados para la autenticación, autorización y control de acceso de dispositivos en la red. La solución debe facilitar la detección de dispositivos no autorizados, la evaluación de la postura de seguridad y la implementación de políticas de acceso basadas en el cumplimiento de normas y configuraciones de seguridad, asegurando así la protección y la integridad de la infraestructura tecnológica.
La solución NAC debe contar mínimo con las siguientes especificaciones:
Una conexión de 1 puerto Ethernet de 1 Gbps RJ45 y 4 puertos SFP+ de 10 Gbps. Mínimo de 24 GB de memoria DDR4. Mínimo dos discos SSD de 768 GB cada uno. Debe tener la capacidad de configuración de RAID 1 gestionado por software. Debe poseer un puerto RJ45 de acceso a consola. Debe ocupar como máximo una (1) unidad de Rack. Debe poseer una fuente de alimentación redundante 1+1 con capacidad de intercambio en caliente.
La solución NAC debe soportar:
Debe estar en capacidad de gestionar hasta 200 switches o 15000 sesiones concurrentes La solución de NAC debe implementarse como maquina física.
La solución NAC debe incluir los siguientes bloques funcionales:
Visibilidad de red y perfilado de dispositivos conectados. Automatización del proceso de provisión de red en función del tipo de dispositivo que se esté conectando OnBoarding de nuevos dispositivos sencillo, versátil y potente. Endpoint Compliance: Permitiendo a la organización desplegar políticas asociadas a diferentes grupos de usuarios, verificando su cumplimiento y notificando las desviaciones, permitiendo configurar diferentes protocolos de remediación, desde acciones de aislamiento inmediatas a simples notificaciones, pasando por acciones diferidas. Identificación de amenazas, a través de la integración con otros elementos, y ejecución de acciones de remediación en función del evento.

Gestión de invitados y usuarios externos: Fácil y rápida, sin necesidad de involucrar al personal de IT en el alta de nuevos usuarios externos por medio de patrocinadores o Sponsors y para eventos grandes dar de alta y de baja fácilmente,
La solución NAC debe contar las siguientes características:
La solución NAC debe ser agnóstica respecto a los fabricantes del equipamiento de acceso, tanto cableado como inalámbrico y por tanto válida en redes heterogéneas de diferentes fabricantes. La solución NAC debe estar integrada con los dispositivos de red y seguridad existentes, y los que se incluyan en la nueva arquitectura. Debe ser capaz de trabajar bien con agentes instalados en los endpoints, o bien sin agentes. La solución NAC no puede ser dependiente de soluciones 802.1x y RADIUS, pero debe de ser compatible. La solución debe tener incluidos los módulos de integración con terceros La solución debe integrarse con el Firewalls, SIEM, Generador de Analítica, Sandbox, EDR/ NDR y Honeypots transfiriendo todos los parámetros del cliente hacia las soluciones y deben ser del mismo fabricante del NAC para optimizar los tiempos de respuesta y resolución de eventos.
Perfilado de dispositivos
La solución NAC debe tener capacidad para realizar el inventario de todos los dispositivos de la red, incluyendo equipamiento que no sea PC, como impresoras, Smartphones (Iphone, Android y Windows Phone), teléfonos IP, cámaras y otros dispositivos IoT que pudieran existir (biométricos…) y dispositivos OT. Debe poder utilizar al menos 20 métodos diferentes para identificar el tipo de dispositivo: DHCP fingerprint, NMAP scan, Vendor OUI, ubicación, puertos abiertos o información obtenida a través de agentes. Debe soportar el perfilado de dispositivos interactuando con el dispositivo mediante HTTP/HTTPS, SSH/Telnet o incluso interaccionando con el dispositivo a través de scripts diseñados a medida. Debe incluir un servicio dinámico de identificación de dispositivos IoT que comparta la información disponible sobre el dispositivo a perfilar con un servicio en Nube, que emplee técnicas de inteligencia que ayuden a la identificación del dispositivo. Debe soportar el perfilado de dispositivos Windows pertenecientes al domino mediante WMI o WINRM, utilizando canales seguros y validados mediante certificado.
Authentication y enforcement
La solución debe permitir conectarse a la red corporativa solo a dispositivos autenticados/registrados, desplegando políticas de seguridad que bloqueen y aíslen dispositivos que no cumplan los criterios corporativos, enviándolos a un área de cuarentena sin necesidad de intervención por parte de los administradores de red.
Debe ser capaz de autorizar los accesos mediante asignación dinámica de VLAN's y/o aplicando ACLs al puerto de acceso.
Debe ser capaz de controlar escenarios en los que hay más de un equipo conectado a un puerto, asociando a cada equipo la VLAN adecuada, siempre que el equipo de acceso lo permita.
Debe ser capaz de integrarse con los firewalls para asociar los dispositivos a reglas de seguridad concretas, en función del tipo de dispositivo.
Debe permitir extender las políticas de seguridad al acceso VPN, ya sea SSL en modo túnel o IPSEC a través de una política de seguridad consistente.
Debe soportar autenticación de máquina y usuarios, pudiendo autenticar un endpoint sin usar agentes.
Debe de ser capaz de asociar al dispositivo atributos adicionales, como la ubicación, tipo de dispositivo, fabricante… además de los atributos del usuario conectado.

Debe soportar opciones de autenticación flexibles, incluyendo 802.1X, autenticación WEB y autenticación MAC.
Para despliegues 802.1X, debe poder actuar como Radius Proxy y como Radius local (TTLS/PAP, l TTLS/MSCHAPv2, PEAP/MSCHAPv2, TLS)
Debe soportar integración LDAP y Microsoft Active Directory, sin necesitar ningún componente adicional, para desplegar políticas en función de su pertenencia a ciertos grupos.
Debe soportar RADIUS Identity store.
Debe soportar la detección y perfilamiento de sistemas operativos Chrome
Integración de MDM incluida
Debe soportar enforcement por medio de SSH/SNMP para switches, controladoras inalámbricas y otros dispositivos.
Requisitos de Endpoint Compliance y Remediación
La solución debe soportar inspección de los dispositivos tanto basada en agente (persistente y disoluble) como sin agente. La solución NAC debe ser capaz de realizar, al menos, las siguientes comprobaciones: service packs, nivel de parcheo, que haya instalado las actualizaciones críticas, Antivirus y AntiSpyware, servicios y procesos, certificados, existencia de archivos y cualquier entrada del registro de Windows. Debe contar con un Motor de correlación de eventos. La solución debe proporcionar un rol de cuarenta que se interactúe con los Sistemas de parcheo. De esta manera, los dispositivos corporativos que no cumplan los requisitos serán enviados a un portal cautivo de "auto-remediación": Los equipos que no sean compliant debe de ser enviados a cuarentena dinámicamente, y o bien se le proporcionan instrucciones para la remediación o se ejecuta la remediación automática a través de sistemas como BigFix.
Gestión de invitados
El Sistema de control de acceso debe proporcionar una plataforma flexible y eficiente de gestión de usuarios no corporativos, que permita manejar el acceso de aquellos usuarios con un acceso transitorio (típicamente invitados) o con un acceso más estable (contratistas externos). Debe permitir definir perfiles limitados que solo tengan acceso a la gestión de cuentas de invitados. Debe permitir altas masivas (p.e. para conferencias), autoregistros, registros esponsorizados o dados de alta por un administrador. Debe permitir autenticaciones por medio de redes Sociales. Debe permitir la opción de Aceptar invitados por medio de patrocinadores o Sponsors. Debe ser flexible y permitir la definición de diferentes perfiles, como invitados de corta /larga estancia, asistentes a conferencias o auto-registrados.
Gestión y Reporte
El sistema de control de acceso almacena información crucial sobre la red, cuántos elementos hay conectados y sus características, cuántos cumplen la política de seguridad de la empresa … así como los eventos de seguridad que se puedan haber producido. También almacena información sobre eventos en la red (cambios en los puertos, conexiones…) que pueden ser de gran utilidad para realizar investigaciones después de que se produzca una investigación.
Debe ofrecer una consola de monitorización, reporting y troubleshooting que ayude a los administradores y operadores de helpdesk.
La consola debe ser accesible a través de una GUI Web, sin necesidad de aplicaciones específicas.

Debe permitir obtener, al menos, la siguiente información:
Eventos de conexión a lo largo del tiempo
Cambios en los puertos.
Eventos de seguridad detectados por la plataforma a lo largo del tiempo (por ejemplo, fingerprints que cambian, intentos de impersonación…).
Eventos de seguridad recibidos de otras plataformas, y las acciones tomadas
Resultado de los escaneos de compliance (fallados, pasados)
Histórico de dispositivos conectados, última conexión…)
Debe incluir plantillas de reportes, ejecutables bajo demanda o programados).
Debe permitir customizar los reportes.
Debe de incluir plantillas de despliegue de políticas.
Debe de permitir la opción de usar un Sistema de reporte y monitorización dedicado.
El oferente debe ser como mínimo Partner en uno de los dos niveles más altos de la solución ofertada, garantizando amplia experiencia en el manejo de licenciamiento sobre las diferentes soluciones, garantizando -ANS- el menor tiempo de respuesta en el suministro de equipos y soporte. El proponente debe presentar una carta expedida por la fábrica donde certifique su nivel de membresía en alguno de los 2 niveles más altos, con tiempo de expedición no mayor a 30 días calendario con respecto a la fecha de cierre de la presentación de propuestas.
Licenciamiento
El licenciamiento de la solución NAC debe ser perpetua para 1000 dispositivos terminales simultáneos que posea visibilidad, control y respuesta. El oferente deberá garantizar el soporte directo por parte de fabrica como mínimo por 3 años del equipo y/o licenciamiento ofertado.
HERRAMIENTA DE SANDBOX
Adquisición de un sistema de protección proactiva y mitigación de amenazas avanzadas que permita la utilización de mecanismos combinados para la detección de virus, virus polimórficos y otras amenazas avanzadas. Debido a la información manejada por la entidad, la solución debe ser del tipo appliance de propósito específico, por ende, no se aceptan soluciones en la nube. La solución debe estar certificada y recomendada por NSS Labs para sistemas de detección de brechas y sistemas de prevención de brechas. La solución debe estar certificada y recomendada por ICSA Labs para defensa de amenazas avanzadas.
Detección Proactiva y Mitigación:
Ejecución de código malicioso en sistemas operativos virtuales.

Soporte de múltiples filtros antes de la ejecución en el sistema operativo virtual, entre los múltiples filtros se deben incluir como mínimo: filtros de antivirus, consultas a base de datos en la nube y simulación de código independiente del sistema operativo. Todos los análisis y bloqueos de malware y / o códigos maliciosos deben realizarse en tiempo real y el bloqueo debe ser inmediato, no se aceptarán soluciones que solo detecten malware y / o códigos maliciosos. La solución debe admitir las reglas YARA como estándar para crear reglas que permitan detección de malware. Identificación en tiempo real de sitios de phishing de día cero incluyendo spam y malware hosteados. Análisis de código estático impulsado con IA para identificar riesgos sin ejecución de código Uso de Deep learning para detección de códigos ejecutables Windows (PEXbox) Detección de riesgos de red en modo sniffer. Identificación de botnets, ataques en la red y visita de sitios maliciosos por medio de URLs Debe soportar realizar análisis de OT.
Debe incluir un prefiltro por Inteligencia Artificial La solución debe permitir la carga de máquinas virtuales personalizadas. La solución debe permitir la creación de firmas en tiempo real para las amenazas detectadas mediante el análisis de comportamiento a través de la distribución de firma local entre los dispositivos integrados, como Firewall de Nueva Generación, Gateway de correo electrónico, protección de punto final, balanceador de cargas o firewall de aplicaciones web del mismo fabricante. Por lo tanto, todos los dispositivos integrados en la solución Sandbox están inmediatamente protegidos contra nuevas amenazas. • La solución debe estar en la capacidad de detectar los siguientes tipos de infección y ataques: -Gusanos -Botnet: Archivos que actúan como un cliente de una red Bot. -Hijack: Archivos que tratan de modificar registros para tener acceso al sistema. -Stealer: Archivos que tratan de substraer información confidencial. -Backdoor: Archivos que tratan de instalarse como servicios nuevos de red para permitir el acceso remoto. -Injector: Archivos sospechosos que inyectan código en los procesos del sistema. -RootKit: Archivos que tratan de esconder su comportamiento funcionando en conjunto con procesos del sistema. -Adware: Archivos tratando de acceder a sitios web. -Troyanos: Archivos con un payload malicioso. -Riskware: Software que tiene posibles procesos que puedan poner en riesgo la infraestructura. -Greyware: Archivos con comportamiento similar al de virus.

• Toda la clasificación (Maliciosos, alto, medio, bajo riesgo) deben ser presentados en un dashboard intuitivo. • Debe presentarse información completa del análisis de amenazas del ambiente virtual incluyendo actividades del sistema, acción del exploit, trafico web, intentos de comunicación entre otros. • Deberá permitir al administrador de la solución descargar el archivo original, analizado por la solución sandbox. • En caso de un veredicto positivo, debe presentar una descripción detallada del comportamiento de la maquina comprometida, que contenga al menos información sobre el tipo de archivo, la fuente de malware, IP de destino (cliente que descargó el malware) y un resumen del comportamiento del malware para fines de auditoría. • La solución debe grabar un video de toda la interacción del malware o debe permitir interactuar manualmente con el malware en un entorno simulado.}
Protección de amenazas avanzadas
• La solución debe realizar análisis de código estático basado en IA que identifica posibles amenazas dentro del código que no se ejecuta. • La solución debe proporcionar la capacidad de emular ataques en sistemas operativos y aplicaciones Windows 8.1, Windows 10, Windows 11, MacOS, Linux y Android y sistemas ICS • Soporte de análisis de archivos ejecutables Windows: .bat, .cab, .cmd, .dll, .exe, .js, .msi, .ps1, .vbs, wsf •MicrosoftOffice: .doc, .docm, .docx, .dot, .dotm, .dotx,. iqy, .one, .pot, .potm, .potx, .ppt, .pptm, .pptx, .ppam, .pps, .ppsm, .ppsx, .pub, .rtf, .sldm, .sldx, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, xltx, • Archivos de Documentos/Email: .eml, .pdf,. rl • Android files: .apk • Linux files:. elf • Archivos MacOS: .app, .dmg, Mach-O • Archivos Web: .htm, html, .lnk, WEBLink • Archivos comprimidos: .7z,. ace, .arj, .bz2, .gz, .iso, .jar, .kgb, .lzh, .rar, .swf, .tar, .tgz, .upx, .xz, .z, .zip • Técnicas de Anti-evasión: Sleep calls, process y registry queries. • Detección de modificación de archivos, comportamiento de procesos, comportamiento de registros y comportamientos de red. • Detección de callbacks: Visitas a URL maliciosas, comunicaciones con servidores de comando y control (C&C) y todo el tráfico generado desde la muestra de malware.

• El número de clones por cada tipo de máquina virtual debe poder ser parametrizable a criterio de la entidad. • Debe mostrar los paquetes de software instalados en cada tipo de Máquina Virtual. • Debe permitir crear listas negras y listas blancas. • Debe permitir seleccionar que tipos de archivos serán analizados en cada máquina. • Debe permitir que el usuario cree sus propios tipos de archivos. • Debe permitir inspección de nuevas amenazas, incluyendo ransomware y mitigación de malware protegido por contraseña. • Análisis heurístico / patrones / basado en la reputación • Debe soportar como mínimo los siguientes tipos de archivos: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar,.rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, .rl, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
• Protocolos/Aplicaciones: o Modo Sniffer – http, ftp, pop3, imap, smtp, smb, o Modo integrado con solución de seguridad perimetral: http, smtp, pop3, imap, mapi, ftp, im y sus equivalentes en SSL. o Modo BCC/MTA para SMTP. • La plataforma deberá enviar de forma automática los archivos catalogados como maliciosos al laboratorio del fabricante para creación y distribución de firmas. • La solución debe incluir un módulo de filtrado web para inspeccionar y marcar las conexiones a URL maliciosas que traten de hacer los procesos ejecutados por los archivos que se inspeccionan. • Los archivos que son analizados con el OS Sandbox deben entregar un análisis posterior a la ejecución de las siguientes características: o Descarga de Virus o Modificación de registro. o Conexiones externas a IPs maliciosas. o Infección de procesos. • La solución debe estar en la capacidad de procesar múltiples archivos al mismo tiempo, se debe contar con múltiples VM para el análisis de Sandbox OS.

• El resultado de los análisis debe clasificar los archivos de acuerdo con el nivel de riesgo como Alto, medio o bajo. Esta clasificación se hará de acuerdo a un puntaje y la cantidad de puntos que tenga cada archivo en su análisis. • Debe ser posible habilitar él envió de notificaciones cada vez que el análisis detecte archivos maliciosos. • Debe soportar sandboxing que incluya escaneo dinámico con Inteligencia artificial. • Debe soportar a través de IA el aprendizaje de nuevas técnicas de Malware y ransomware. • Debe tener instancias de VM concurrentes • Debe tener como mínimo la detección de las siguientes técnicas antievasion: o API Obfuscation o Detección de o Comando y Control o Direct System Calls o Retardo de ejecucion - Execution Delay o Memory Only Payload o Proceso Hollowing/Injection o Runtime Encryption/Packing
o System Fingerprinting o Time Bomb o User Files Check o User Interaction Check o VM/Sandbox Detection
Modo de Implementación
• La solución debe poder ser implementada de una de las siguientes formas: o File Input: Debe ser posible manualmente hacer una subida de los archivos a analizar. o Sniffer: El equipo debe estar en la capacidad de recoger el tráfico de un puerto en modo espejo. o La solución debe admitir topologías de implementación integradas (con un Firewall de Nueva Generación, solución de protección de correo electrónico, ADC, WAF o punto final) del mismo fabricante. o La solución debe admitir topologías de implementación con adaptadores para la integración con soluciones de terceros a través del protocolo ICAP o BCC. o La solución debe admitir topologías de implementación mediante el intercambio de archivos. o La solución debe admitir topologías de implementación bajo demanda, es decir, mediante envío manual a través de la consola gráfica. o La solución debe admitir topologías de implementación a través de la API JSON para automatizar la carga de muestras y la descarga de indicadores de malware accionables para remediar. • Soporte de rutas estáticas. • La solución debe tener integración certificada con los siguientes terceros: CarbonBlack, Ziften y SentinelOne.

• La solución debe permitir intercambio compartido de indicadores de compromiso (IOC) entre plataformas Sandbox del mismo fabricante. • Debe poder realizar escaneo de grandes archivos en modo netshare por medio de CIFs, NFS, AWS S3 y Azure blob.
Especificaciones: "Sandboxing Appliance"
• 4 interfaces a 1Gbps RJ45, • 960 GB de capacidad de disco y/o superior • El equipo debe soportar múltiples archivos simultáneos en análisis. • Se deben soportar al menos 6 máquinas virtuales. • Numero de Archivos por Hora (Análisis en VM): 6000 • Numero de archivos en Análisis estático por hora: 10.000 • Numero de archivos en análisis dinámico por hora: 250 • Numero de correos que puede soportar por hora: 60.000 • Número de usuarios soportados: 1000 • Se deben incluir mínimo 4 máquinas VM así: o Win 10, Win 11, Office 19, Office 21
Generación de Reportes:
• La solución debe proporcionar un reporte con análisis detallado que mapea las técnicas de malware descubiertas en el marco Mitre ATT & CK con potentes herramientas de investigación integradas que permiten al equipo de Operaciones de Seguridad (SecOps) descargar paquetes capturados, archivo original, registro de seguimiento y captura de pantalla de malware. • Soport de Mittre Attack V11 • Descarga de logs, pcap e indicadores en formato stix 2.0 • Notificaciones vía correo cuando un archivo malicioso sea detectado • Visor de eventos que incluya acciones, nombre del malware, rating, tipo, fuente, destino, hora de detección, y camino de descarga. • Despliegue en tiempo real de actividades escaneadas, top de hosts objetivos, top de malware, top de urls infectadas, top de dominios callback. • Reportes detallados en características y comportamiento. Modificación de archivos, comportamiento de procesos, comportamiento de registros, comportamientos de red. • Se deben presentar estadísticas de TOP N, con datos de los hosts atacados, malware, URLs, Call Back Domains. • La solución debe estar en la capacidad de enviar reportes semanalmente. • La solución debe entregar información en línea específica de los análisis realizados, esto debe ser sobre una interfaz gráfica con filtros predeterminados como eventos, malware, entre otros. • La información del análisis debe poder ser descargada en un log para análisis posterior. • Debe ser posible descargar un archivo PCAP para revisar el comportamiento del archivo. • En los casos que aplique debe ser posible descargar un pantallazo de las acciones graficas del archivo sospechoso., logs y capturas de paquetes.

• La solución debe permitir integración con una plataforma de logs y reportes del mismo fabricante.
Administración:
• La solución debe soportar configuraciones a través de GUI y CLI. • Debe permitir la creación de múltiples cuentas de administradores. • Debe permitir el monitoreo del estado de las máquinas virtuales. • Permitir autenticación RADIUS para administradores. • La solución debe permitir verificación automática y descarga de nuevas imágenes de máquinas virtuales. • La solución debe permitir notificaciones por correo electrónico cuando se detecta un archivo malicioso. • La solución debe tener una página de búsqueda centralizada que permite a los administradores crear condiciones de búsqueda personalizadas. • El proponente deberá adjuntar en su propuesta certificación expedida directamente por el fabricante, donde se le acredite como distribuidor autorizado en los dos más altos niveles de fábrica.
Se requiere soporte especializado por (1) año por parte del oferente, para los productos adquiridos a partir de la fecha de acta de inicio del contrato
El oferente debe ser como mínimo Partner en uno de los dos niveles más altos de la solución ofertada, garantizando amplia experiencia en el manejo de licenciamiento sobre las diferentes soluciones, garantizando -ANS- el menor tiempo de respuesta en el suministro de equipos y soporte. El proponente debe presentar una carta expedida por la fábrica donde certifique su nivel de membresía en alguno de los 2 niveles más altos, con tiempo de expedición no mayor a 30 días calendario con respecto a la fecha de cierre de la presentación de propuestas.
Licenciamiento:
El oferente deberá garantizar el soporte directo por parte de fabrica como mínimo por 3 años del equipo y/o licenciamiento ofertado.
HERRAMIENTA DE CORRELACION DE EVENTOS (SIEM)
Adquisición de un sistema de monitoreo y correlación de eventos de seguridad (SIEM) que permita la detección proactiva y mitigación de amenazas avanzadas mediante el uso de mecanismos combinados para la recolección, análisis en tiempo real y correlación de eventos, facilitando la identificación de incidentes de seguridad, comportamientos anómalos y vulnerabilidades en la infraestructura tecnológica. La solución ofertada debe ser capaz de realizar la ingesta de eventos para un mínimo de 100 equipos y 50 sistemas de registro y monitoreo de integridad de archivos (Log & FIM), con licenciamiento perpetuo.
Debido a la información manejada por la entidad, la solución debe ser del tipo appliance de propósito específico, por ende, no se aceptan soluciones en la nube.
La solución de correlación de eventos debe estar posicionada en el "Gartner® Magic Quadrant™ for Security Information and Event Management (SIEM) 2024" en las categorías de **Challenger** o **Leaders**. El oferente deberá adjuntar una carta del fabricante, emitida en un plazo no mayor a 30 días, que

certifique el nivel actual de la solución. Además, deberá proporcionar un enlace que permita verificar dicha información.
La solucion debe estar en capacidad de instalarse en Sitio (On-Prem), virtual, Nube Publica, Nube Privada o como Cloud SaaS.
La solución ofertada debe utilizar aprendizaje automático para detectar comportamientos inusuales de usuarios y entidades (UEBA) sin que sea necesario que el administrador escriba reglas complejas.
Debe permitir la identificación de amenazas internas y externas que puedan evadir las defensas tradicionales. Además, la solución debe generar alertas de alta fidelidad para ayudar a priorizar las amenazas que requieren atención inmediata.
La solución ofertada debe contar con un motor de correlación de eventos en tiempo real distribuido, capaz de detectar patrones complejos de eventos en tiempo real. Este motor debe permitir gestionar una gran cantidad de reglas en tiempo real a altas tasas de eventos, asegurando tiempos de detección acelerados.
La solución ofertada debe incluir un motor de descubrimiento de aplicaciones e infraestructura inteligente, capaz de detectar infraestructura física y virtual, tanto local como en nubes públicas o privadas. Este motor debe realizar el descubrimiento utilizando únicamente credenciales, sin necesidad de conocimiento previo sobre los dispositivos o aplicaciones existentes.
La solución ofertada debe incluir un lenguaje de análisis de eventos basado en XML, que sea funcional como los lenguajes de programación de alto nivel, permitiendo su fácil modificación. Además, este lenguaje debe ser compilable en tiempo de ejecución, garantizando una alta eficiencia en el procesamiento de eventos.
La solución ofertada debe permitir el uso de objetos CMDB descubiertos, junto con datos de usuario, identidad y ubicación, en la creación de búsquedas y reglas para el monitoreo y la correlación de eventos.
La solución ofertada debe permitir la integración con sitios web externos para la búsqueda de direcciones IP, facilitando así la obtención de información adicional sobre estas direcciones.
La solución ofertada debe estar disponible en formato de máquinas virtuales para implementaciones tanto locales como en nubes públicas y privadas. Debe ser compatible con los siguientes hipervisores: VMware ESX, Microsoft Hyper-V, KVM, Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).
Debe soportar métodos de autenticación multifactor y control granular de accesos para garantizar la seguridad y el cumplimiento de políticas.
La solución debe identificar y gestionar identidades de usuarios y dispositivos, integrándose con sistemas de gestión de identidades y accesos (IAM).
La solución debe integrarse fácilmente con sistemas y herramientas existentes, incluyendo firewalls, antivirus, sistemas de gestión de vulnerabilidades, soluciones de backup y las soluciones ofertadas.
La solucion SIEM debe contar minimo con las siguientes especificaciones:
La solución ofertada debe cumplir con las siguientes normas y regulaciones: FCC, ISED, CE, RCM, VCCI, BSMI, UL/cUL y CB.

La solución ofertada debe incluir como mínimo las siguientes interfaces: 3 puertos Ethernet RJ45 de 1 Gbps y 2 puertos SFP28 de 25 Gbps.
La solución ofertada debe contar con un mínimo de las siguientes capacidades de almacenamiento: 6 discos duros de 3.5 pulgadas intercambiables en caliente de 4 TB cada uno. 3 unidades de estado sólido (SSD) de 2.5 pulgadas intercambiables en caliente de 1.92 TB cada una.
La solución ofertada debe incluir como mínimo 96 GB de memoria DDR4 (módulos ECC RDIMM).
Debe ocupar como máximo dos (2) unidades de Rack.
El oferente debe ser como mínimo Partner en uno de los dos niveles más altos de la solucion ofertada, garantizando amplia experiencia en el manejo de licenciamiento sobre las diferentes soluciones, garantizando -ANS- el menor tiempo de respuesta en el suministro de equipos y soporte. El proponente debe presentar una carta expedida por la fábrica donde certifique su nivel de membresía en alguno de los 2 niveles más altos, con tiempo de expedición no mayor a 30 días calendario con respecto a la fecha de cierre de la presentación de propuestas.
Licenciamiento:
El oferente deberá garantizar el soporte directo por parte de fabrica como minimo por 3 años del equipo y/o licenciamiento ofertado.
PLATAFORMA AVANZADA DE GESTIÓN DE VULNERABILIDADES AUTÓNOMA y PATCH MANAGEMENT EN SERVIDORES
El proveedor deberá suministrar el licenciamiento de la solución para 200 equipos entre servidores y equipos finales, por un término mínimo de DOCE (12) MESES, contados a partir del ACTA DE INICIO del contrato.

Descripción del Bien y/o Servicio	Cantidad Mínima
Adquisición de licenciamiento y configuración de Plataforma avanzada de gestión de vulnerabilidades autónoma y patch management en servidores.	200

PLATAFORMA
La plataforma debe ser Cloud – SaaS
La plataforma debe tener visibilidad y cobertura en tiempo real para los sistemas operativos y aplicaciones de su organización, es decir, cualquier cambio en el inventario (instalación / desinstalación / cambio de aplicaciones y / o activos debe reflejarse instantáneamente en su panel de control)
La plataforma debe proporcionar una solución integrada para la gestión de vulnerabilidades, la priorización de riesgos y la corrección en una plataforma.
La plataforma debe correr en alguna de las Clouds más usadas.
Debe contar por lo menos con dos métodos de autenticación (Ej: User y pass, mail de verificacion, SAML2 with IDPs).
La plataforma debe tener la posibilidad de instalar un proxy en la red para poder hacer patching caching.
El proxy debe correr en al menos sistema Linux Ubuntu o Red Hat.

El proxy no debe tener costo adicional.
CARACTERISTICAS
Actualización de los servidores sin interrumpir el servicio
En caso de ser necesario, se debe suministrar soporte directo de fábrica.
La plataforma debe soportar las apps en el SO
Modelo de riesgo personalizable
Evaluación continua de vulnerabilidades
Reconocimiento automático de aplicaciones
Priorización de vulnerabilidades combinada con inteligencia interna.
Priorización y reparación de vulnerabilidades desde una única consola
Proceso de clasificación de riesgos para priorizar la corrección de vulnerabilidades descubiertas.
Clasificación de riesgo basada en activos
Clasificación de riesgo por aplicaciones
Debe presentar la clasificación de riesgo y priorizar las vulnerabilidades a corregir en orden de criticidad no solo desde CVE, sino también en relación con el contexto de desempeño y la situación del entorno.
Mapeo de priorización
Administración de parches para Windows OS
Administración de parches para aplicaciones de terceros en Windows
Administración de parches para Linux OS
Administración de parches para aplicaciones de terceros en Linux
Administración de parches para Mac OS
Administración de parches para aplicaciones de terceros en Mac OS
Detección de vulnerabilidades en tiempo real
Proteger la explotación de software en tiempo real utilizando tecnología de Virtual Patch o Patchless Protection
Debe tener la funcionalidad para agregar protección contra vulnerabilidades de Process Memory Scrapping, Direct API Abuse o Process Impersonation, sin necesariamente aplicar el parche (Virtual Patch o Patchles Protection).
Información en la plataforma de que se trata cada CVE
Actualización en tiempo real de vulnerabilidades
Debe admitir al menos el número de vulnerabilidades heredadas igual o superior a 160.000 que se presentan en el NIST
Debe identificar parches de seguridad en los sistemas operativos
Debe permitir la ejecución de comandos en todos los puntos finales que tengan agentes.
Programación de la instalación de parches o ejecución de scripts
Posibilidad de ejecutar acciones automáticas pre-configuradas y customizadas

Posibilidad de generar scripts en la misma plataforma para Windows, Linux y Mac
Protección contra vulnerabilidades del día 0
Un motor de acciones recomendadas para darle al administrador una lista de opciones a ejecutar
Debe contar con templates de scripting para realizar tareas de Red Team y Blue Team
Debe contar con la posibilidad de integrarse con tecnologías de AI para la remediación automatica de vulnerabilidades
Debe contar con templates de scripting para el equipo de SysAdmin
Ejecución de scripts de detección y remediación de CVEs.
Permitir el despliegue de los agentes por la línea de comandos
Permitir la implementación de los agentes a través de la GPO
Debe soportar varios roles de usuarios
Debe poder segregar diferentes activos entre diferentes grupos de usuarios con diferentes niveles de permisos
AGENTE
Los agentes deben poder escanear al menos las plataformas Windows, Linux y Mac.
Los agentes deben poder parchear al menos las plataformas Windows, Linux y Mac.
El agente debe poder parchearse a sí mismo
INTEGRACIONES y REPORTES
La plataforma debe soporta integraciones con SIEMs (Splunk, SumoLogic y más)
La plataforma debe soporta integraciones con cualquier software via API
Debe soportar integraciones via SAML2 con los sistemas más conocidos (ej: Okta, Ping Identity y más)
Genere informes sobre vulnerabilidades encontradas en uno de los siguientes tipos: formatos PDFm con exportación a CSV, PDF: • Resumen ejecutivo, con información resumida sobre el escaneo Informe detallado, con toda la información técnica necesaria para que los lectores reproduzcan los problemas identificados "
Debe tener un tablero con resultados en tiempo real de las vulnerabilidades existentes
Informe de riesgo integrado en la misma plataforma
Soporte de informes de riesgos de múltiples aplicaciones
Debe contar con integración con herramientas de terceros para hacer Network Scanning (ejemplo Nmap)
El proponente debe presentar una carta expedida por la fábrica donde certifique que es partner de solución ofertada, con tiempo de expedición no mayor a 30 días calendario con respecto a la fecha de cierre de la presentación de propuestas.

CONDICIONES TECNICAS ESPECIFICAS

ASISTENCIA, ACTUALIZACIONES DE SOFTWARE, FIRMWARE Y PARTES HARDWARE PARA LAS

SOLUCIONES OFERTADAS

- El proveedor deberá suministrar el licenciamiento de las soluciones Control de Acceso a la Red (NAC), una herramienta de Sandbox, un sistema de correlación de eventos (SIEM) con licenciamiento de 36 meses y Plataforma avanzada de gestión de vulnerabilidades autónoma y patch management en equipos por 12 meses, contados a partir del ACTA DE INICIO del contrato.
- El CONTRATISTA debe realizar la actualización del firmware para todos los dispositivos relacionados en el anexo técnico, instalando las últimas actualizaciones liberadas y aprobadas por el fabricante, y que sean soportadas por el hardware que tiene la Entidad, previa programación y aprobación del supervisor del contrato.
- El CONTRATISTA deberá instalar las actualizaciones del licenciamiento de la Universidad Colegio Mayor de Cundinamarca, sobre las herramientas ofertadas, durante la vigencia del Contrato de soporte entre la Universidad Colegio Mayor de Cundinamarca y el Fabricante.
- El Oferente deberá instalar las actualizaciones de la plataforma de gestión que el fabricante tenga previstas para los modelos relacionados de equipos.
- El proveedor deberá suministrar asistencia durante las acciones de actualización de software, firmware y partes de Hardware para los equipos relacionados.
- En caso de ser necesario, se debe suministrar soporte directo de fábrica.

POLITICA AMBIENTAL

- Con el fin de garantizar que el proponente esté alineado y comprometido con el cuidado del medio ambiente y la reducción de la huella de carbono, el oferente deberá contar con una certificación vigente en Sistemas de Gestión Ambiental en su versión más reciente. Esta certificación acreditará que las operaciones del oferente, incluyendo la implementación y administración de licencias de software, están alineadas con prácticas sostenibles y responsables desde un punto de vista ambiental. La certificación deberá ser emitida directamente por el ente certificador y deberá presentarse junto con la oferta económica al cierre del proceso de licitación actual.

MESA DE AYUDA

- El proponente debe incluir el soporte técnico a través de una mesa de ayuda por un periodo de 12 meses, la cual será la encargada de gestionar todos los incidentes y requerimientos reportados, con el fin de realizar un seguimiento del cumplimiento de los acuerdos de nivel de servicio garantizando calidad de la asistencia brindada.
- El oferente deberá garantizar la prestación de asistencia no programada sin límite de solicitudes incluidos las que requieran cambio de partes de Hardware durante el tiempo contractual pactado entre las partes.
- El CONTRATISTA debe dar soporte telefónico y/o presencial en horario hábil (7AM - 6PM)

lunes a viernes y si se requiere, ventanas de mantenimiento en horarios no hábiles (7x24) de lunes a Domingo; Este soporte técnico en primera instancia se deberá realizar por medio de una línea telefónica provista por el CONTRATISTA, y/o de forma remota si el incidente no es solucionado telefónicamente, y de no corregirse la falla; deben presentarse en las instalaciones de la Universidad Colegio Mayor de Cundinamarca en un tiempo que no supere las cuatro (4) horas

- El prestador de servicio debe contar con certificación vigente en la norma de estándares internacionales del Sistema de Gestión de Servicios en su versión más reciente para los procesos relacionados con seguridad y mesa de ayuda, a fin de garantizar la calidad, gestión y mejora de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente. El oferente deberá garantizar que el personal que prestará la asistencia en el presente contrato cuente con los elementos necesarios para la prestación de la asistencia al evento presentado.
- El oferente deberá coordinar con el personal de la Universidad Colegio Mayor de Cundinamarca la ejecución de asistencias de inspecciones trimestrales y/o solicitadas sin que haya afectación en la prestación del servicio de red para la entidad o minimizando su impacto a los usuarios.
- El contratista apoyara al personal técnico de la Universidad Colegio Mayor de Cundinamarca en la Administración de la plataforma de seguridad perimetral durante la vigencia del contrato.

PERSONAL REQUERIDO

GERENTE DE PROYECTO

- Ingeniero electrónico, de sistemas, de telecomunicaciones o afines con un Máster y/o especialización en Gestión de proyectos informáticos.
- Mínimo ocho (8) años de experiencia especifica en proyectos de tecnología como Gerente de Proyectos. Todas contadas a partir de la expedición de la T.P. mediante la presentación de certificaciones laborales y/o contratos
- El profesional postulado debe contar con la totalidad de las certificaciones que se relacionan a continuación:
    - ITIL Foundation V4
    - SCRUM MÁSTER
    - ISO/IEC 27001:2022 Auditor interno

PROFESIONAL EN SEGURIDAD OFENSIVA

- Ingeniero electrónico, sistemas o telecomunicaciones o afines con especialización en seguridad de redes o Magister en Seguridad de las Tecnologías de la Información y de las Comunicaciones.
- Mínimo diez (10) años de experiencia especifica en proyectos de tecnología como Gerente

de Proyectos.
- El profesional postulado debe contar con la totalidad de las certificaciones que se relacionan a continuación:

    - CRISC (Certified in Risk and Information Systems Control)
    - CISA (Certified Information System Auditor)
    - CEH (Certified Ethical Hacker)
    - CISM (Certified Information Security Manager)
    - CISSP (Certified Information Systems Security Professional)
    - Auditor Líder ISO 27001:2013

PROFESIONAL DE IMPLEMENTACION

- Ingeniero electrónico, sistemas o telecomunicaciones o afines con especialización en seguridad informática.
- Mínimo cuatro (4) años de experiencia especifica en proyectos de seguridad informática, todas contadas a partir de la expedición de la T.P. mediante la presentación de certificaciones laborales y/o contratos.
- El profesional postulado debe contar con la totalidad de las certificaciones que se relacionan a continuación:
    - ITIL V4 FUNDATION
    - Certificación auditor interno 27001:2013 o superior
    - Certified Solution Specialist Network Security
    - Certified Professional Network Security

PROFESIONAL DE SEGURIDAD INFORMATICA

- Ingeniero electrónico, sistemas o telecomunicaciones o afines con especialización en seguridad informática.
- Mínimo un (1) año de experiencia profesional en áreas de seguridad o SOC, todas contadas a partir de la expedición de la T.P. mediante la presentación de certificaciones laborales y/o contratos.
- El profesional postulado debe contar con la totalidad de las certificaciones que se relacionan a continuación:
    - Certificación auditor interno 27001:2022
    - Certificación de la marca ofertada en niveles básicos o superiores.
    - Certificación de capacitación como experto en pentest y Vulnerabilidades

PROFESIONAL DE APOYO DE SEGURIDAD INFORMATICA

- Ingeniero electrónico, sistemas o telecomunicaciones o afines con especialización en

seguridad informática.

- Mínimo Seis (6) años de experiencia general todas contadas a partir de la expedición de la T.P., y mínimo tres (3) años de experiencia especifica en proyectos de seguridad informática, mediante la presentación de certificaciones laborales y/o contratos.
- El profesional postulado debe contar con la totalidad de las certificaciones que se relacionan a continuación:
    - Certificación de la marca ofertada en niveles básicos o superiores.
    - Certificación de capacitación como experto en pentest y Vulnerabilidades

POLITICA DE SEGURIDAD DE RED

- El oferente deberá ajustar y mantener todos los aspectos de seguridad de los equipos siempre que haya modificaciones y/o actualizaciones que puedan afectar la configuración existente, siendo este aspecto responsabilidad del oferente, por los cambios realizados.
- El prestador de servicio debe contar con certificación vigente en la norma de estándares internacionales del Sistema de Gestión de Seguridad de la Información en su versión más reciente para los procesos relacionados con seguridad y mesa de servicios, a fin de garantizar la calidad, gestión y mejora de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente.

DOCUMENTACION DEL PROYECTO

- El CONTRATISTA informará oportunamente al supervisor del contrato las dificultades encontradas para la correcta ejecución de este.
- El contratista mensualmente debe enviar un informe mensual al supervisor del contrato del estado de funcionamiento de los appliances y las observaciones que a su criterio se deben implementar o ejecutar para fortalecer su uso.

ACUERDO DE NIVELES DE SERVICIO

- El proveedor se compromete durante el tiempo de prestación del servicio de soporte, a respetar los Acuerdos de Niveles de Servicio (ANS), así:

	TIEMPO DE RESPUESTA (Horas Hábiles)	TIEMPO DE RESOLUCIÓN TEMPORAL (Horas Hábiles)	TIEMPO DE RESOLUCIÓN DEFINITIVA (Horas Hábiles)
FALLAS CRITICAS	Hasta dos (2) horas	Máximo ocho (8) horas	Máximo dos (2) días hábiles
FALLAS MAYORES O	Hasta cuatro (4) horas	Máximo un (1) día hábil	Máximo tres (3) días hábiles

URGENTES			
FALLAS MENORES O LEVES	Hasta ocho (8) horas	Máximo dos (2) días hábiles	Máximo cinco (5) días hábiles

- Fallas críticas (Prioridad Alta): Se consideran casos de prioridad alta, aquellas fallas que impiden el funcionamiento del sistema de seguridad en forma total o parcial y aquellos que impidan el normal funcionamiento de partes u opciones del sistema que impacten directamente sobre actividades consideradas de vital importancia. Adicionalmente, la vulneración de la disponibilidad, integridad o confidencialidad de la información a través de ataques cibernéticos de cualquier índole a la Entidad.
- De ser necesaria la atención en sitio, será prestada por un ingeniero del proveedor en las instalaciones de la Universidad Colegio Mayor de Cundinamarca dentro del tiempo de respuesta establecido.
- Fallas Mayores o Urgentes (Prioridad Media): Se consideran casos de prioridad media, aquellos que impidan el normal funcionamiento de partes u opciones del sistema que impactan sobre actividades consideradas no críticas.
- Fallas menores o leves (Prioridad Baja): Se consideran casos de prioridad baja, aquellos que impidan el normal funcionamiento de opciones de generación de reportes o consultas que impactan sobre actividades consideradas no críticas o aquellos que impidan el normal funcionamiento, opciones generales no cubiertas por las demás.
- Prioridades definidas: Fallos en la ejecución de consultas y reportes no críticos, preguntas y cuestiones
-

REQUISITO DE OBLIGATORIO CUMPLIMIENTO

Confidencialidad De La Información: En virtud del presente proceso de contratación y su respectiva ejecución, el oferente se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente contrato y que se encuentra marcada como confidencial a terceros; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo.
El proponente se compromete a guardar la confidencialidad de toda la información que le sea entregada y/o que se encuentre bajo su custodia o que por cualquier otra circunstancia deba conocer o manipular y responderá civil, penal y disciplinariamente por los perjuicios que su divulgación y/o utilización indebida, por sí o por un tercero cause a la entidad o a terceros. Para tal efecto el oferente deberá diligenciar el Anexo de Acuerdo de confidencialidad.

El personal comprometido en la ejecución del objeto del presente proceso de contratación podrá ser sometido a un estudio de seguridad realizado por la Universidad Colegio Mayor de Cundinamarca, este estudio podrá ser desarrollado durante la vigencia del contrato. En el evento de que alguna(s) de la(s) persona(s) vinculada(s) con el desarrollo del objeto del presente proceso de contratación no llegase a pasar dicho estudio, el oferente deberá cambiar a dicha(s) persona(s) por otra que también deberá someterse al estudio de seguridad.

Así mismo deberá dar estricto cumplimiento a lo siguiente:

De acuerdo con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia, y en cumplimiento de sus directrices, se deberá realizar un proceso de borrado seguro y/o sanitización de datos en todos los discos duros de las laptops y equipos de escritorio utilizados por el personal contemplado en el proyecto en curso.

El software utilizado para el borrado seguro debe estar debidamente licenciado y no puede ser de código abierto. Además, debe generar un certificado auditable que garantice que el borrado de los datos ha sido irreversible, el cual podrá ser presentado ante auditorías sobre el tratamiento de la información.

Este software debe cumplir con las normas nacionales e internacionales aplicables a la eliminación segura de información sensible, tales como: la Guía de Borrado Seguro según la Ley 1581, Artículo 4; ISO 27001 A.11.2.7 sobre control de la eliminación o reutilización de equipos; y los estándares NIST 800-53 y 800-88.El software de sobreescritura de discos debe ofrecer múltiples métodos de borrado, incluyendo, entre otros, los métodos Gutmann, DoD 5220.22-M, CESG CPA – Higher Level, NIST 800-88 Clear y Purgue, NSA 130-1, RCMP TSSIT OPS-II, y TCG Cryptographic Erasure. Además, el oferente debe aportar una certificación expedida por la marca que lo acredite como partner en el nivel más alto de la solución ofertada, la certificación la cual debe ser expedida a nombre de la entidad con fecha de expedición no superior a 30 días.

ASESORIA Y TRANSFERENCIA DE CONOCIMIENTO

- El oferente por medio de su personal de ingeniería de la empresa deberá asesorar técnicamente a los encargados de la administración de la solución ofertada en la Universidad Colegio Mayor de Cundinamarca, con el fin de mejorar el servicio, utilizar bien su capacidad y demás manipulaciones que afecten la protección de los sistemas Informáticos. (Incluye asesoría para Update de Equipos-modelos recientes) por el periodo de 12 meses.
- El CONTRATISTA deberá ofrecer una transferencia de conocimiento a funcionarios del Grupo de informática de la Universidad Colegio Mayor de Cundinamarca. Esta transferencia de conocimiento debe ser de la administración y el análisis de la seguridad de la red. Esta será programada entre el supervisor del contrato y el CONTRATISTA a partir de la firma del acta de inicio y se realizará en las instalaciones de la Universidad Colegio Mayor de Cundinamarca o en las instalaciones del contratista.

3.1 OBLIGACIONES GENERALES DEL CONTRATISTA

- ✓ Constituir con su propio presupuesto las garantías suficientes posterior a la adjudicación del proceso.
- ✓ Guardar la debida y completa reserva y confidencialidad sobre la información y los documentos de que tenga conocimiento, o a los que tenga acceso.
- ✓ Participar en las reuniones que se programen para la planificación de las actividades a realizar.
- ✓ Atender las observaciones, solicitudes y sugerencias que formule el Supervisor del Contrato y

realizar los ajustes a que haya lugar de acuerdo con los niveles de servicio ofrecidos.

- ✓ Entregar una vez culmine el plazo de ejecución mediante inventario a la Universidad y por conducto del Supervisor designado, los documentos que se encuentren en su poder en formato físico y/o electrónico producto del objeto contratado, si a ello hubiere lugar.
- ✓ Acatar los principios y valores establecidos en el Código de Ética de la Universidad Colegio Mayor de Cundinamarca.
- ✓ Actuar con la debida transparencia, idoneidad, celeridad y publicidad en todas las actividades.
- ✓ Cumplir con el objeto del servicio establecido en la presente Orden y desempeñar todas las actividades y obligaciones pactadas.
- ✓ Ejecutar el objeto del Contrato con la diligencia y oportunidad requerida, con la calidad y en el tiempo establecido con el Supervisor, utilizando las herramientas y el talento humano necesario para tal fin y dando cumplimiento a las condiciones ofertadas de la propuesta.
- ✓ Las demás que requiera la Universidad en virtud del objeto del servicio de la presente orden de trabajo.

3.2 OBLIGACIONES ESPECIFICAS DEL CONTRATISTA

- Ejecutar el proyecto objeto de acuerdo con las especificaciones, cantidades, características y alcance del presente proceso.
- Suministrar el personal idóneo para la prestación de los servicios objeto de este contrato.
- En caso de daño de algún equipo durante el periodo de ejecución del contrato, el proveedor deberá suministrar un equipo con características iguales o superiores en calidad de préstamo sin valor adicional.
- Informar al inicio del contrato los siguientes medios de comunicación y acceso a soporte técnico y actualizaciones del fabricante:
    - Número(s) telefónico(s) para soporte.
    - Dirección de correo electrónico.
    - Información pertinente y Usuario de contacto para gestión de soporte por diferentes medios, así como el respectivo procedimiento.

- Realizar todas las actividades que conlleven a la solución de requerimientos técnicos, operativos y de información que se puedan presentar durante la ejecución del proyecto.
- Suministrar cada 6 meses un informe Técnico de los incidentes y/o requerimientos de servicio.
- Atender las solicitudes que haga el supervisor del contrato, relacionadas con las dificultades que se puedan presentar, durante la ejecución del objeto contractual.
- Las demás que contribuyan a garantizar el cumplimiento del contrato y las que por su naturaleza le sean atribuibles conforme al objeto y alcance de este.

CAPÍTULO IV - CONDICIONES DE VERIFICACIÓN DE CUMPLIMIENTO HABILITANTES

COMPONENTE JURÍDICO (cumple o no cumple)

Se verificará que la documentación allegada con cada propuesta y su contenido se encuentre presentada de conformidad con las condiciones y requisitos establecidos en los términos de referencia.

A esta verificación no se le asignará puntaje, su resultado será CUMPLE O NO CUMPLE.

El OFERENTE deberá anexar a su propuesta la siguiente documentación, para lo cual, en el mismo orden en el que se relacionan a continuación, incluirán un separador para identificar cada uno de los siguientes documentos, así:

4.1.1 Formato para propuesta de oferentes o proveedores de bienes y/o servicios

El oferente deberá allegar el Formato propuesta de oferentes o proveedores de bienes y/o servicios diligenciados en su totalidad y firmado por el Representante Legal, mediante el **ANEXO 1** de la presente invitación.

En caso de que la propuesta sea presentada por una persona jurídica o por un Consorcio o Unión Temporal, la carta de presentación deberá ser suscrita por la persona que represente la persona jurídica, el Consorcio o la Unión Temporal. En todo caso, a la propuesta deberá anexarse el documento de Consorcio o Unión Temporal en donde conste que quien la presenta acredita la capacidad para tal fin, así como la capacidad para suscribir el contrato a que haya lugar.

4.1.2. Certificado de existencia y representación legal

El proponente deberá acreditar con los certificados de Existencia y Representación Legal expedidos por la Cámara de Comercio, expedidos con fecha no superior a 30 días calendario anteriores a la fecha de cierre de la Invitación a cotizar, los siguientes aspectos:

Que el proponente es una sociedad que ha sido legalmente constituida como tal, que el objeto social se relacione con el objeto de la presente Invitación a cotizar y que el término de vigencia de sociedad es de dos (02) años o más; deberá estar inscrita en la Cámara de Comercio con matrícula renovada y vigente y con más de dos (02) años de constitución.

Quien ejerce la representación legal y sus facultades.

Para tal efecto se solicita indicar si las facultades del representante legal son suficientes para la presentación de la oferta, en razón a lo dispuesto en un artículo específico de los estatutos sociales, en tal caso indicar qué artículo, o en razón a una autorización impartida por el órgano social competente, en tal caso indicar qué órgano social y el número del Acta de la reunión a través de la cual se impartió la autorización.

Cuando el monto de la propuesta fuere superior al límite autorizado al Representante Legal, el oferente deberá anexar, desde el momento de la presentación de su oferta, la correspondiente autorización impartida por la Junta de Socios, o el estamento de la sociedad que tenga esa función y que lo faculte específicamente para presentar la propuesta en este proceso de selección y celebrar el contrato respectivo, en caso de resultar seleccionado.

Si la propuesta se presenta a nombre de una Sucursal, se deberán anexar los Certificados de Existencia y Representación Legal expedidos por la Cámara de Comercio tanto de la Sucursal como de la Casa Principal.

Para los casos de Consorcio o Uniones Temporales, cada una de las empresas que Conforman el consorcio la unión temporal deberá cumplir con este requisito en la forma indicada.

4.1.3. Cédula de ciudadanía del representante legal.

Presentar fotocopia del documento de identidad del oferente o representante legal del oferente persona jurídica, y del apoderado, según el caso.

En el caso de consorcios o uniones temporales, este debe ser cumplido por cada uno de los representantes legales que lo integran, como por el representante legal designado como representante del consorcio o unión temporal.

4.1.4 Registro Único Tributario – RUT Vigente.

De acuerdo con el artículo 555-2 del Estatuto Tributario, el proponente debe estar inscrito en la Dirección de Impuestos y Aduanas Nacionales en el Registro Único Tributario, por tanto, debe presentar copia del certificado correspondiente expedido por la DIAN.

Para los casos de Consorcio o Uniones Temporales, cada una de las empresas que conforman el consorcio o la unión temporal deberá cumplir con este requisito en la forma indicada.

4.1.5. Documento de Constitución de Consorcio / Unión Temporal

En el caso de consorcios o uniones temporales conformados por personas naturales con establecimiento de comercio y/o personas jurídicas, cada uno de los integrantes debe presentar certificado de existencia y representación legal constitución y cuya actividad u objeto social tengan relación directa con el requerimiento del presente termino de referencia. Así como el documento de constitución del consorcio o unión temporal en los términos establecidos en el presente termino de referencia

El documento de constitución del Consorcio o Unión Temporal debe estar debidamente diligenciado y firmado por el proponente, el cual deberá contar con la siguiente información o cumplir con los siguientes requisitos:

1. Acreditar que la duración del consorcio o unión temporal debe extenderse por el plazo del contrato, su liquidación y un (1) año más.

2. La designación de un representante que deberá estar facultado para actuar en nombre y representación del Consorcio o Unión temporal. Igualmente deberá designar un suplente que lo reemplace en los casos de ausencias temporales definitivas.

NOTA 1: En el caso consorcios y de las uniones temporales cada uno de sus integrantes deberá cumplir con los requisitos solicitados en los numerales anteriores.

NOTA 2: Única y exclusivamente se evaluará el presente numeral, en el evento en que se llegaran apresentar consorcios o uniones temporales.

4.1.6. Acta de Junta de Socios o Junta Directiva

En caso de existir limitación en las facultades del representante legal señaladas en los estatutos, anexar la copia del Acta de Junta de Socios o Junta Directiva, según el caso, donde se le autorice para comprometer a la sociedad en la presente contratación y suscribir los documentos que se requieran en su desarrollo. Dicho documento debe cumplir con los requisitos legales para su validez.

4.1.7. Poder

Cuando el oferente actúe a través de un representante o apoderado deberá acreditar, mediante documento debidamente expedido, que su representante o apoderado está expresamente facultado para presentar la oferta y firmar el contrato respectivo.

4.1.8. <u>Garantía de Seriedad de la Propuesta – firmada por el Representante Legal(original)</u>

El PROPONENTE deberá anexar una garantía expedida en formato **DE ENTIDADES PÚBLICAS CON RÉGIMEN PRIVADO DE CONTRATACIÓN**, a favor de la Universidad Colegio Mayor de Cundinamarca identificada con el NIT 800.144.829-9 que ampare la seriedad de su propuesta, por un valor equivalente mínimo al diez por ciento (10%) del valor de su propuesta, con una vigencia de noventa (90) días calendario, contados a partir de la fecha de apertura de la propuesta. Dicha fecha se encuentra en el número 1.3 cronograma y tramite del proceso. Deberá ser expedida por una compañía de seguros legalmente autorizada para funcionar en el país.

El **PROPONENTE** deberá aportar Original de la Garantía de seriedad de la propuesta.

En caso de prórroga del cierre del proceso, la vigencia de esta Garantía deberá ser ampliada de conformidad con lo requerido por la UNIVERSIDAD. La póliza debe ser tomada a nombre del **PROPONENTE**, con la razón social que figura en el certificado de existencia y representación legal expedido por la Cámara de Comercio, sin utilizar sigla, a no ser que el Certificado de la Cámara de Comercio establezca que la firma podrá identificarse con sigla.

Para los casos de Consorcio o Unión Temporal, la póliza debe ser expedida a nombre del consorcio o unión temporal y deberá ser suscrita por su representante legal.

NOTAS. El **PROPONENTE** deberá aportar Original de la Garantía de seriedad de la propuesta, debidamente suscrita por el tomador y allegar constancia de pago de la prima correspondiente y/o incluirse constancia de que la garantía no expirará por falta de pago de la prima ni por revocación unilateral.

Los proponentes no seleccionados, podrán retirar la póliza en la Subdirección de Servicios Administrativos, una vez culmine la etapa de adjudicación.

Al **PROPONENTE** se le hará efectiva la Garantía de Seriedad de la Propuesta, en el evento que:

- Solicite el retiro de su propuesta después del cierre del proceso, excepto cuando el retiro de dicha propuesta obedezca a circunstancias de fuerza mayor o caso fortuito.

- Cuando el **PROPONENTE** favorecido con la adjudicación no suscriba el contrato en el término señalado por la UNIVERSIDAD o no cumpla con las garantías contractuales.

- Los demás eventos descritos en el decreto 1082 de 2015.

4.1.9 Registro Único de Proponentes – RUP.

El proponente debe aportar con carácter obligatorio el Registro Único de Proponentes (RUP) expedido por la Cámara de Comercio respectiva y con fecha de expedición vigente, en donde se encuentren los Estados Financieros con el último corte de acuerdo con las disposiciones del decreto 1082 de 2015, es decir, aquellos que se encuentren consignados y en firme en el Registro Único de Proponentes cuyo máximo plazo de renovación es el quinto día hábil del mes de abril de cada año.

Podrán participar en el presente proceso de selección todas las personas naturales o jurídicas nacionales o extranjeras domiciliadas o con sucursal en Colombia, que se encuentren inscritas en el registro único de proponentes (RUP) de la Cámara de Comercio.

En este documento se verificarán los requisitos de capacidad jurídica, técnica, financiera (Estado financiero o condición financiera) y organizacional, y experiencia, conforme lo dispuesto en los presentes términos de referencia y la información contenida en el RUP.

El certificado debe ser expedido con una fecha no superior a 30 días calendario anterior a la fecha de cierre del proceso de selección.

La Entidad verificará los requisitos habilitantes, en el RUP que se encuentre vigente y en firme de quien efectúe la renovación del registro dentro del término establecido en la ley para ello.

En consecuencia, si un proponente ha solicitado oportunamente la renovación del RUP, la Entidad verificará los requisitos habilitantes con la información existente antes de la solicitud de renovación, la cual está vigente y en firme hasta que la información en proceso de renovación adquiera firmeza.

Para el caso de consorcios y uniones temporales todos los miembros deberán acreditar su inscripción y renovación en el RUP.

Si la propuesta se presenta en forma individual, el oferente debe cumplir en forma total con la inscripción y clasificación exigido en los presentes términos de referencia.

NOTA 1: La no inscripción del proponente en el Registro Único de Proponentes a la fecha de cierre del presente proceso de selección, causará el rechazo de su propuesta, pues la inscripción en el RUP debe existir al momento de presentación de la propuesta.

NOTA 2: Cada uno de los miembros o partícipes de Consorcios o Uniones Temporales deberá estar inscrito en el Registro Único de Proponentes al momento del cierre de proceso de selección.

NOTA 3: El RUP a ser allegado por los proponentes con la propuesta, deberá estar actualizado a la presente vigencia, salvo que se encuentre en trámite su renovación, debidamente radicado dentro de los cinco (5) días hábiles del mes de abril de esta vigencia, ante la Cámara de Comercio de la

jurisdicción, caso en el cual, el proponente deberá anexar con su propuesta el último RUP renovado y la constancia de solicitud de renovación, debidamente radicado en término, ante la Cámara de Comercio de la jurisdicción

4.1.10 Certificación sobre el Cumplimiento de las Obligaciones Parafiscales y de Seguridad Social

Expedida por el revisor fiscal del proponente, cuando éste exista de acuerdo con los requerimientos de ley, o por el proponente (persona natural) ó representante legal, en la que conste que el proponente ha cumplido con sus obligaciones frente al sistema de seguridad social integral, caja de compensación familiar, ICBF y SENA, de sus empleados durante los 6 meses anteriores a la fecha de cierre del presente proceso de selección, si hay lugar a ello, de acuerdo con lo establecido en el artículo 50 de la ley 789 de 2002, en el artículo 23 de la ley 1150 de 2007 y en el artículo 20 de la ley 1607 de 2012.

Dicha certificación puede ser firmada por:

a. El representante legal.
b. Revisor Fiscal si está obligado a tenerlo, para lo cual deberá adjuntarse el **certificado de antecedentes disciplinarios de la Junta Central de Contadores (vigente) y tarjeta profesiona**l.

Si se trata de un consorcio o unión temporal, se deberá allegar la certificación de cumplimiento antes mencionada para cada uno de los miembros.

4.1.11 Certificado de Antecedentes Disciplinarios expedido por la Procuraduría General de la Nación

Ningún proponente, ni los integrantes de consorcios o uniones temporales, podrán presentar antecedentes disciplinarios vigentes que impliquen inhabilidad para contratar con el Estado, a la fecha establecida para el cierre del presente proceso de selección, de conformidad con lo establecido en la Ley 1238 de 2008. Los oferentes deberán presentar el certificado precitado, al momento de presentar la oferta, con fecha de emisión no superior a 30 días calendario anteriores a la fecha de presentación de la propuesta, en el que conste que ni la sociedad ni su Representante Legal y/o la persona natural, registran sanciones ni inhabilidades vigentes.

Si el oferente es persona jurídica deberá presentar tanto el de la empresa, como el de su representante legal. Si la oferta es presentada por un consorcio o unión temporal, cada uno de sus miembros deberá presentar de manera independiente la certificación solicitada en el presente literal.

Tratándose de proponentes extranjeros sin domicilio o sin sucursal en Colombia y en cuyo país de origen no exista ente Estatal que certifique la ausencia de antecedentes disciplinarios, se deberá

indicar esta circunstancia así como la declaración de no contar con antecedentes disciplinarios que impliquen inhabilidad para contratar en documento suscrito bajo la gravedad de juramento por el proponente persona natural o representante legal de la persona jurídica, como proponente individual o integrante del proponente plural.

El proponente podrá presentar las certificaciones referidas en el presente numeral, no obstante, la Entidad verificará mediante consulta en el SIRI que el proponente no reporta antecedentes disciplinarios en la Procuraduría General de la Nación. En cumplimiento de lo dispuesto por la Ley 734 de 2002.

4.1.12 Certificado de Antecedentes Fiscales Expedido por la Contraloría General de la República

Con el fin de acreditar el cumplimiento de la obligación establecida en el artículo 60 de la Ley 610 de 2000, la Universidad verificará en el último boletín de responsables fiscales expedido por la Contraloría General de la República que el proponente y cada uno de sus integrantes cuando el mismo sea un consorcio o una unión temporal, no se encuentre (n) reportado (s) en dicho boletín.

Los oferentes deberán presentar el certificado precitado, al momento de presentar la oferta, con fecha de emisión no superior a 30 días calendario.

Si el oferente es persona jurídica deberá presentar tanto el de la empresa, como el de su representante legal. Si la oferta es presentada por un consorcio o unión temporal, cada uno de sus miembros deberá presentar de manera independiente la certificación solicitada en el presente literal.

Tratándose de proponentes extranjeros sin domicilio o sin sucursal en Colombia y en cuyo país de origen no existe Boletín de Responsables Fiscales o su equivalente, deberá indicar esta circunstancia, en documento suscrito bajo la gravedad de juramento por el proponente persona natural o representante legal de la persona jurídica, como proponente individual o integrante del proponente plural.

El proponente podrá presentar las certificaciones referidas en el presente numeral, no obstante, LA ENTIDAD verificará mediante consulta en el boletín de responsables fiscales que el proponente no se encuentra allí reportado.

4.1.13 Registro de Medidas Correctivas establecidas en el Código de Policía

De acuerdo con lo establecido en la ley 1801 de 2016 artículo 183, para el caso de proponentes personas naturales y de los representantes legales del proponente persona jurídica, así como de los representantes legales que conforman el consorcio o unión temporal el proponente deberá consultar y aportar el certificado que emite la página Web de Policía Nacional de Colombia – Portal

de Servicio al Ciudadano, el Sistema Registro Nacional de Medidas Correctivas, con el objeto de verificar si existen multas en mora en los últimos 6 meses, impuestas por virtud del artículo 183 del Código Nacional de Policía, Ley 1801 de 2016, del representante legal de la persona jurídica individual, de los representantes legales de los consorcios y/o uniones temporales que van a participar en el presente proceso. En el evento que registre multa, si transcurridos seis meses desde la fecha de imposición de una multa, esta no ha sido pagada con sus debidos intereses, hasta tanto la persona no se ponga al día no podrá contratar o renovar contrato con cualquier entidad del Estado. Por tanto, en dicho evento los proponentes (Representante legal o personal natural) deberán aportar comprobante en el que conste que se encuentra al día por este concepto.

Los oferentes deberán presentar el certificado precitado, al momento de presentar la oferta, con fecha de emisión no superior a 30 días calendario.

4.1.14 Certificado de Antecedentes Judiciales y de no inhabilidad por comisión de delitos sexuales contra menores de 18 años

Para el caso de proponentes personas naturales y de los representantes legales del proponente persona jurídica el proponente, deberá aportar el certificado de antecedentes judiciales y el certificado de no inhabilidad por comisión de delitos sexuales contra menores de 18 años, que expide la Policía Nacional de Colombia, a través de su página web.

Los oferentes deberán presentar el certificado precitado, al momento de presentar la oferta, con fecha de emisión no superior a 30 días calendario

4.1.15 Certificado de Antecedentes Disciplinarios y Tarjeta Profesional tanto del Contador como del Revisor Fiscal cuando conforme a la Ley se requiera

Los interesados y todos los integrantes de los Consorcios o Uniones Temporales, acompañarán copia de la tarjeta profesional y certificado de antecedentes disciplinarios o documentos equivalentes, tanto del Contador como del Revisor Fiscal, cuando conforme a la Ley se requiera, expedido por la Junta Central de Contadores vigente a la fecha de cierre de la presente convocatoria.

Para el caso de las propuestas presentadas por Consorcios o Uniones temporales, cada uno de sus integrantes deberá allegar la misma documentación y requisitos mencionados, según corresponda.

Los oferentes deberán presentar el certificado precitado, al momento de presentar la oferta, con fecha de emisión no superior a 90 días calendario, de conformidad con la vigencia establecida por la Junta Central de contadores.

4.1.16 Reporte de Búsqueda en la Lista Clinton (Sanctions List Search the Office of Foreign Assets

Control)

Deberá allegar las personas naturales con establecimiento de comercio y las personas jurídicas que se presenten el certificado que acredite que no se encuentra reportado en la lista Clinton con el fin de verificar que los OFERENTES no estén relacionadas con actividades o dineros provenientes del narcotráfico, el terrorismo o el lavado de activos.

Si el oferente es persona jurídica deberá presentar tanto el de la empresa, como el de su representante legal.

En el caso de consorcios o uniones temporales cada uno de los miembros debe cumplir el presente requisito en la forma indicada.

4.1.17. Formato de Declaración de Inhabilidades e Incompatibilidades o conflicto de intereses

Se deberá allegar certificación de no encontrarse incurso en causal de inhabilidad, incompatibilidad o conflicto de intereses, no mayor a un (1) mes de expedición.

Para el caso de las personas naturales con establecimiento de comercio, esta debe estar suscrita por la persona natural

Para el caso de las personas jurídicas, esta debe estar suscrita por el representante legal de la sociedad en la cual se debe certificar que tanto el representante legal como los socios no se encuentran en causal de inhabilidad, incompatibilidad o conflicto de intereses.

Para el caso de consorcios o uniones temporales, cada uno de los miembros debe cumplir el presente requisito en la forma indicada.

Se verificará que la documentación allegada con cada propuesta y su contenido se encuentre presentada de conformidad con las condiciones y requisitos establecidos en los términos de referencia.

Dicho formato será publicado en la página web junto con la presente invitación.

4.1.18. Formato de Declaración de Conflicto de Intereses Permanente para Contratistas y Administrativos

Se deberá allegar certificación donde acredite que da a conocer cualquier situación que pueda generar un conflicto de intereses en el ejercicio contractual, con el fin de garantizar el interés general, no mayor a un (1) mes de expedición.

Para el caso de las personas naturales con establecimiento de comercio, esta debe estar suscrita por la persona natural.

Para el caso de las personas jurídicas, esta debe estar suscrita por el representante legal de la sociedad en la cual se debe certificar que tanto el representante legal como los socios no se encuentran en causal de inhabilidad, incompatibilidad o conflicto de intereses.

Para el caso de consorcios o uniones temporales, cada uno de los miembros debe cumplir el presente requisito en la forma indicada. Se verificará que la documentación allegada con cada propuesta y su contenido se encuentre presentada de conformidad con las condiciones y requisitos establecidos en los términos de referencia.

Dicho formato será publicado en la página web junto con la presente invitación.

4.2. EVALUACIÓN TÉCNICO HABILITANTE (CUMPLE O NO CUMPLE)

En este aspecto se verificará que la propuesta presentada cumpla con los aspectos técnicos señalados por la Universidad en el Capítulo III, los respectivos formatos y anexos técnicos, en virtud de las obligaciones descritas en la presente invitación a cotizar para la prestación del servicio.

Adicionalmente, se tendrán en cuenta las condiciones físico-técnicas verificadas durante la visita realizada a las instalaciones de cada oferente.

4.2.1 Soportes de Cumplimiento de Contratos - experiencia

Los proponentes, interesados en participar en el presente proceso, deberán acreditar una experiencia habilitante mediante la presentación de un máximo de cinco (5) certificaciones de contratos ejecutados al 100%, suscritos con entidades públicas o privadas y debidamente registrados en el RUP. La suma total de estos contratos deberá alcanzar el valor del presupuesto oficial, y su objeto deberá estar relacionado con la ejecución de las siguientes actividades:

- Adquisición e implementación de herramientas de seguridad para la protección de la infraestructura tecnológica.
- Herramientas de SIEM (correlación de eventos).
- Administración y/o monitoreo de plataformas de seguridad informática.
- Actualización y/o renovación de garantías de soluciones de firewall y sandbox.

Es fundamental destacar que todos los contratos presentados para acreditar la experiencia del proponente deben estar registrados en el RUP, en conformidad con el Decreto 1082 de 2015, y encontrarse vigentes y en firme.
Para la acreditación de la experiencia reportada en el Registro único de Proponentes, se debe dar cumplimiento en conjunto de por lo menos dos (2) de los códigos UNSPSC relacionados a continuación:

Clasificación UNSPSC	Segmento	Familia	Clase
43222500	Difusión de Tecnologías de Información y Telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipo de seguridad de red
43222600	Difusión de Tecnologías de Información y Telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipo de seguridad de red
43231500	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software funcional especifico de la empresa
43232300	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de consultas y gestión de datos.
43232400	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Programas de desarrollo
43233200	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de seguridad y protección
81112200	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Mantenimiento y soporte de software

La sumatoria del valor total de los contratos debe ser igual o superior al cien por ciento (100%) del valor del presupuesto del presente proceso, expresado en salarios mínimos mensuales legales vigentes (**1.522,14 SMMLV**), de acuerdo con el año en que fueron ejecutados.

Para propuestas presentadas en modalidad de Consorcio, Unión Temporal o promesa de sociedad futura, todos los miembros que las componen deben aportar experiencia, en por lo menos uno de los códigos. La experiencia de los proponentes plurales será la sumatoria de la experiencia de sus integrantes, presentada con la propuesta con máximo cinco (5) contratos en total.

Los contratos deben haberse ejecutado satisfactoriamente dentro de los últimos cinco (5) años anteriores al cierre del proceso, y deben contener la siguiente información:

- Nombre o razón social de la entidad que certifica, dirección y teléfono.
- Nombre y cargo de la persona que expide la certificación y datos de contacto.
- Nombre y NIT del contratista
- Número y fecha del contrato.
- Objeto Este debe tener relación con el objeto indicado en el presente proceso.
- Fecha de suscripción e inicio: Anterior a la fecha de cierre del proceso.

- Fecha de terminación: Estos contratos deberán estar terminados antes de la fecha de cierre del proceso.
- Valor del contrato: La sumatoria del valor de los contratos debe ser igual o superior al 100% del valor del presupuesto oficial estimado. En caso de consorcio o Unión Temporal, se tendrá en cuenta la sumatoria de las certificaciones presentadas por sus miembros.

Para consorcios o uniones temporales, cada uno de sus integrantes deberá acreditar experiencia mediante la presentación de mínimo una (1) certificación y la experiencia del proponente plural corresponderá a la sumatoria de la experiencia de sus integrantes.

NOTA 1: Las certificaciones para acreditar la experiencia especifica podrá corresponder a los contratos que se presenten para acreditar la experiencia en el RUP. En todo caso, **los contratos cuya certificación sea aportada para acreditar la experiencia específica, deberán estar inscritos en el RUP.**
NOTA 2: No se aceptarán certificaciones de contratos en ejecución, ni relación de contratos celebrados o referencias comerciales o facturas por si solas.
NOTA 3: Si el contrato se refiere a servicios diferentes a los descritos en este documento para el presente proceso de selección, se debe efectuar dentro de la certificación una discriminación por cada uno de los servicios prestados y su valor, pues para realizar la verificación de experiencia, solo se toma el valor correspondiente a las actividades directamente relacionadas con el objeto del proceso de selección abreviada que se adelanta, y este será el que se tenga en cuenta para efectos de establecer el valor mínimo requerido expresado en S.M.M.L.V. En caso de no cumplir con los requerimientos o no realizarse la discriminación de los suministros o servicios objeto de esta selección y su valor, esta certificación no será tenida en cuenta para establecer la experiencia mínima requerida.
NOTA 6. Los oferentes no podrán acreditar experiencia con contratos en ejecución.
NOTA 4. Para efectos de la acreditación de la experiencia del proponente, NO se aceptarán contratos ni auto certificaciones.
NOTA 5: El Universidad Colegio Mayor de Cundinamarca se reserva el derecho de verificar o solicitar los documentos y aclaraciones que considere convenientes, relacionadas con la acreditación de la experiencia. Sin embargo, en el caso de que un proponente o cualquier otro interesado cuestionen la veracidad o legalidad de los documentos presentados por otro proponente, deberá remitirse a las autoridades judiciales para que estas se pronuncien al respecto, habida consideración que esta entidad carece de competencia para pronunciarse y decidir sobre el asunto.

Lo anterior, sin perjuicio de las causales de rechazo previstas en el presente documento, referentes a inconsistencias que imposibiliten la selección objetiva y que no puedan ser resueltas por los proponentes y cuando verificada la información, esta no corresponda a la realidad.

4.2.2 CERTIFICACIONES

El oferente debe presentar junto con la oferta las siguientes certificaciones:

- El prestador de servicio debe contar con certificación vigente en la norma de estándares internacionales del Sistema de Gestión de Servicios en su versión más reciente para los procesos relacionados con seguridad y mesa de ayuda, a fin de garantizar la calidad, gestión y mejora de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente. El oferente deberá garantizar que el personal que prestará la asistencia en el presente contrato cuente con los elementos necesarios para la prestación de la asistencia al evento presentado.
- El prestador de servicio debe contar con certificación vigente en la norma de estándares internacionales del Sistema de Gestión de Seguridad de la Información en su versión más reciente para los procesos relacionados con seguridad y mesa de servicios, a fin de garantizar la calidad, gestión y mejora de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente.
- Con el fin de garantizar que el proponente esté alineado y comprometido con el cuidado del medio ambiente y la reducción de la huella de carbono, el oferente deberá contar con una certificación vigente en Sistemas de Gestión Ambiental en su versión más reciente. Esta certificación acreditará que las operaciones del oferente, incluyendo la implementación y administración de licencias de software, están alineadas con prácticas sostenibles y responsables desde un punto de vista ambiental. La certificación deberá ser emitida directamente por el ente certificador y deberá presentarse junto con la oferta económica al cierre del proceso de licitación actual.
- La solución de correlación de eventos debe estar posicionada en el "Gartner® Magic Quadrant™ for Security Information and Event Management (SIEM) 2024" en las categorías de Challenger o Leaders. El oferente deberá adjuntar una carta del fabricante, emitida en un plazo no mayor a 30 días, que certifique el nivel actual de la solución. Además, deberá proporcionar un enlace que permita verificar dicha información.
- El oferente debe ser como mínimo Partner en uno de los dos niveles más altos de la solucion ofertada (SIEM), garantizando amplia experiencia en el manejo de licenciamiento sobre las diferentes soluciones, garantizando -ANS- el menor tiempo de respuesta en el suministro de equipos y soporte. El proponente debe Anexar la Certificación del Fabricante junto a su propuesta la cual debe ser expedida a nombre de la entidad con fecha de expedición no superior a 30 días.
- El oferente debe ser como mínimo Partner en uno de los dos niveles más altos de la solucion ofertada (NAC), garantizando amplia experiencia en el manejo de licenciamiento sobre las diferentes soluciones, garantizando -ANS- el menor tiempo de respuesta en el suministro de equipos y soporte. El proponente debe Anexar la Certificación del Fabricante junto a su propuesta la cual debe ser expedida a nombre de la entidad con fecha de expedición no superior a 30 días.
- El oferente debe ser como mínimo Partner en uno de los dos niveles más altos de la solucion ofertada (SANDBOX), garantizando amplia experiencia en el manejo de licenciamiento sobre las diferentes soluciones, garantizando -ANS- el menor tiempo de respuesta en el suministro de equipos y soporte. El proponente debe Anexar la Certificación del Fabricante junto a su propuesta la cual debe ser expedida a nombre de la entidad con fecha de expedición no superior a 30 días.
- El oferente debe ser como mínimo Partner de la solucion ofertada (GESTION DE

VULNERABILIDADES Y PATCH MANAGEMENT), garantizando amplia experiencia en el manejo de licenciamiento sobre las diferentes soluciones, garantizando -ANS- el menor tiempo de respuesta en el suministro de equipos y soporte. El proponente debe Anexar la Certificación del Fabricante junto a su propuesta la cual debe ser expedida a nombre de la entidad con fecha de expedición no superior a 30 días.

- El oferente debe aportar una certificación expedida por la marca de Borrado seguro que lo acredite como partner en el nivel más alto de la solución ofertada, la certificación la cual debe ser expedida a nombre de la entidad con fecha de expedición no superior a 30 días.

4.2.3 PERSONAL IDONEO PARA LA INSTALACIÓN DE LOS EQUIPOS

El oferente debe presentar junto con la oferta las siguientes hojas de vida:

GERENTE DE PROYECTO

- Ingeniero electrónico, de sistemas, de telecomunicaciones o afines con un Máster y/o especialización en Gestión de proyectos informáticos.
- Mínimo ocho (8) años de experiencia especifica en proyectos de tecnología como Gerente de Proyectos. Todas contadas a partir de la expedición de la T.P. mediante la presentación de certificaciones laborales y/o contratos
- El profesional postulado debe contar con la totalidad de las certificaciones que se relacionan a continuación:
    - ITIL Foundation V4
    - SCRUM MÁSTER
    - ISO/IEC 27001:2022 Auditor interno

PROFESIONAL EN SEGURIDAD OFENSIVA

- Ingeniero electrónico, sistemas o telecomunicaciones o afines con especialización en seguridad de redes o Magister en Seguridad de las Tecnologías de la Información y de las Comunicaciones.
- Mínimo diez (10) años de experiencia especifica en proyectos de tecnología como Gerente de Proyectos.
- El profesional postulado debe contar con la totalidad de las certificaciones que se relacionan a continuación:

    - CRISC (Certified in Risk and Information Systems Control)
    - CISA (Certified Information System Auditor)
    - CEH (Certified Ethical Hacker)
    - CISM (Certified Information Security Manager)
    - CISSP (Certified Information Systems Security Professional)
    - Auditor Líder ISO 27001:2013

PROFESIONAL DE IMPLEMENTACION

- Ingeniero electrónico, sistemas o telecomunicaciones o afines con especialización en seguridad informática.
- Mínimo cuatro (4) años de experiencia especifica en proyectos de seguridad informática, todas contadas a partir de la expedición de la T.P. mediante la presentación de certificaciones laborales y/o contratos.
- El profesional postulado debe contar con la totalidad de las certificaciones que se relacionan a continuación:
    - ITIL V4 FUNDATION
    - Certificación auditor interno 27001:2013 o superior
    - Certified Solution Specialist Network Security
    - Certified Professional Network Security

PROFESIONAL DE SEGURIDAD INFORMATICA

- Ingeniero electrónico, sistemas o telecomunicaciones o afines con especialización en seguridad informática.
- Mínimo un (1) año de experiencia profesional en áreas de seguridad o SOC, todas contadas a partir de la expedición de la T.P. mediante la presentación de certificaciones laborales y/o contratos.
- El profesional postulado debe contar con la totalidad de las certificaciones que se relacionan a continuación:
    - Certificación auditor interno 27001:2022
    - Certificación de la marca ofertada en niveles basicos o superiores.
    - Certificación de capacitación como experto en pentest y Vulnerabilidades

PROFESIONAL DE APOYO DE SEGURIDAD INFORMATICA

- Ingeniero electrónico, sistemas o telecomunicaciones o afines con especialización en seguridad informática.
- Mínimo Seis (6) años de experiencia general todas contadas a partir de la expedición de la T.P., y mínimo tres (3) años de experiencia especifica en proyectos de seguridad informática, mediante la presentación de certificaciones laborales y/o contratos.
- El profesional postulado debe contar con la totalidad de las certificaciones que se relacionan a continuación:
    - Certificación de la marca ofertada en niveles básicos o superiores.
    - Certificación de capacitación como experto en pentest y Vulnerabilidades

4.2.4 FORMATO PROPUESTA ECONÓMICA (ANEXO 2)

El oferente deberá allegar el formato de Propuesta Económica Agafo 16 (Anexo 2) Debidamente diligenciado en todos sus campos, en este punto se revisa que se allegue la propuesta económica, se revisará que el OFERENTE cumpla con lo mínimo requerido en las especificaciones técnicas de la presente invitación y se tendrá en cuenta lo observado en la visita técnica las sedes de los oferentes.

4.3 COMPONENTE FINANCIERO (cumple o no cumple)

4.3.1. Capacidad Financiera (cumple o no cumple)

Se efectuará un análisis de la capacidad financiera del proponente con base en la información solicitada en el numeral 4.1.9. del capítulo IV de la presente Invitación a Cotizar, teniendo en cuenta entre otros, los siguientes indicadores, así:

INDICADOR	FÓRMULA	MARGEN REQUERIDO
ÍNDICE DE LIQUIDEZ	Activo Corriente Dividido por el Pasivo Corriente	Mayor o igual a 1,6
ÍNDICE DE ENDEUDAMIENTO	Pasivo total dividido por el Activo Total.	Menor o igual a 59%
RAZON DE COBERTURA DE INTERES	Utilidad Operacional Dividida por los Gastos de Intereses	Mayor o igual a 6
CAPITAL DE TRABAJO	Activo Corriente – Pasivo Corriente.	MAYOR O IGUAL AL 100% del Presupuesto Asignado

NOTA: Cuando el proponente no cumpla con alguno de los indicadores de la capacidad financiera, la propuesta será considerada como NO HABILITADA.

4.3.2. CAPACIDAD ORGANIZACIONAL (cumple o no cumple)

Se efectuará un análisis de la capacidad Organizacional del proponente con base en la información solicitada en el numeral 4.1.9. del capítulo IV de la presente Invitación a Cotizar, teniendo en cuenta entre otros, los siguientes indicadores, así:

INDICADOR	FÓRMULA	MARGEN REQUERIDO
Rentabilidad sobre el Patrimonio	Utilidad Operacional dividido Patrimonio	Mayor o igual a 0,18
Rentabilidad sobre Activos	Utilidad Operacional dividido Activo Total	Mayor o igual al 0.15

NOTA 1: Se considera que el oferente cumple con la capacidad financiera y organizacional solicitada y que está habilitado para continuar en el proceso, si obtiene el resultado mínimo anteriormente establecido, en cada uno de los indicadores.

NOTA 2: Para la determinación de los indicadores financieros en el caso de los Consorcios o Uniones Temporales, se sumarán los componentes que se utilizan para el cálculo de dichos indicadores, correspondientes a cada uno de sus integrantes y sobre los totales se obtendrá el índice del Consorcio o Unión Temporal.

NOTA 3: El proponente deberá manifestar el régimen tributario al que pertenece.

CAPÍTULO V – CRITERIOS DE VERIFICACION TECNICA-ECONOMICA

5.1. PROPUESTA TÉCNICO-ECONÓMICA.

El proponente deberá presentar la propuesta técnico-económica (original y medio magnético) mediante el uso obligatorio del formato establecido en el ANEXO 2, con el cumplimiento de todos los requerimientos señalados en el Capítulo III - Especificaciones Técnicas de la presente Invitación a Cotizar.
Si en concepto de la Universidad es necesaria alguna aclaración, ésta será solicitada mediante correo electrónico.
Los precios unitarios antes de impuestos de ley no sufrirán variación durante el tiempo de validez de la oferta y de ejecución del contrato y servirán de base para la selección del proponente.
Igualmente, la propuesta debe presentarse incluyendo todos los valores que puedan generarse con ocasión de tasas, impuestos y demás emolumentos que se puedan presentar en la ejecución del objeto contractual. En el evento en que se ofrezcan DESCUENTOS, éstos deben estar involucrados en el valor de la oferta presentada.

La propuesta económica debe presentarse en pesos colombianos, sin centavos y valores unitarios antes de impuestos de ley, si a ellos hubiere lugar, indicando por separado dichos valores. Si el oferente no discrimina los impuestos y el objeto contratado causa dichos impuestos, la oferta será rechazada.
La propuesta técnico-económica contenida en el ANEXO 2 no es subsanable, si no cumple con los criterios solicitados, la misma será rechazada

5.2. SELECCIÓN

5.2.1. CRITERIO DE EVALUACION DE LAS PROPUESTAS

La universidad seleccionará la oferta que obtenga el mayor puntaje de acuerdo con los siguientes criterios de evaluación:

CRITERIO	PUNTAJE MAXIMO
Precio	640
Ofrecimientos de ponderacion Adicional	250
Estímulo a la Industria Nacional	100
Apoyo personal en condición de discapacidad	10
TOTAL	**1.000**

5.2.2. PRECIO (640 Puntos)

El puntaje máximo que es posible obtener será de 640 puntos al oferente que presente su oferta por el menor valor, obtendrá 640 puntos, para los demás se asignarán los puntos utilizando regla de tres simple.

5.2.3 OFRECIMIENTOS DE PONDERACION ADICIONAL (250 PUNTOS)

Se asignará máximo 250 puntos a los ofrecimientos de ponderación, considerando como ofrecimientos de ponderación adicional lo siguiente:

CRITERIO	PUNTAJE
Se otorgará una ponderación adicional al oferente que, sin costo adicional para la entidad. suministre 50 licencias para uso interno de la entidad destinadas al proceso de borrado seguro de equipos de usuario final. El software provisto deberá cumplir con los mismos requisitos técnicos establecidos en el ITEM de CARACTERISITICAS GENERALES, asegurando que cumple con las normativas nacionales internacionales para e la eliminación segura de información sensible, y que se emiten los certificados auditables correspondientes que garanticen la irreversibilidad del borrado de datos	250
TOTAL	**250**

5.2.4 ESTÍMULO A LA INDUSTRIA NACIONAL

El puntaje máximo que es posible obtener será de 100 puntos.

De acuerdo con el artículo 2.2.1.2.4.2.1. del Decreto 1082 de 2015 y con el fin de apoyar la industria nacional, conforme lo previsto en la Ley 816 de 2003, se asignará un puntaje máximo de cien (100) puntos al proponente que ofrezca el 100% de servicios de origen nacional, para lo cual se tendrá en cuenta lo establecido en el artículo 3 del Decreto 1510 de 2013, que define los servicios de origen nacional como “los servicios prestados por personas naturales colombianas o residentes en Colombia o por personas jurídicas

constituidas de conformidad con la legislación colombiana", hecho que se acreditará con el certificado de existencia y representación legal, para el caso de las empresas; con la copia de la cédula de ciudadanía para las personas naturales, y en caso de consorcio o unión temporal se acreditará con los documentos anteriormente mencionados, teniendo en cuenta la conformación del mismo.
Se otorgará un puntaje de cincuenta (50) puntos a las ofertas de bienes y servicios extranjeros que incorporen por lo menos un cincuenta por ciento (50%) de servicios profesionales, técnicos y operativos nacionales.

En consecuencia, los puntajes que se asignan en cada uno de los casos serán de acuerdo con la Tabla 4:

Tabla 4. Factores y Puntaje de estímulo industria nacional

CONCEPTO	PUNTAJE MÁXIMO
El Proponente que ofrezca el 100% de bienes y/o servicios de origen nacional, es decir aquellos prestados por empresas constituidas de acuerdo con la legislación nacional, por personas naturales colombianas o por residentes en Colombia; o servicios originarios de países con los que Colombia ha negociado trato nacional o países que aplican el principio de reciprocidad.	100
EL proponente que ofrezca a las ofertas de bienes y/o servicios extranjeros que incorporen por lo menos un cincuenta por ciento 50% de servicios profesionales, técnicos y operativos nacionales, se otorgará un puntaje de cincuenta (50) puntos.	50
El proponente que no ofrezca servicios de origen nacional.	0

5.2.5 INCENTIVO EN FAVOR DE PERSONAS EN CONDICIÓN DE DISCAPACIDAD

El puntaje máximo que es posible obtener será de 10 puntos.
El puntaje se asignará conforme lo previsto en el Artículo 2.2.1.2.4.2.6. del Decreto 1082 de 2015, el cual fue adicionado por el artículo 1° del Decreto 392 de 2018, el cual establece:

"***Artículo 2.2.1.2.4.2.6. Puntaje adicional para proponentes con trabajadores con discapacidad****. En los procesos de licitaciones públicas y concursos de méritos, para incentivar el sistema de preferencias a favor de las personas con discapacidad, las entidades estatales deberán otorgar el uno por ciento (1%) del total de los puntos establecidos en el pliego de condiciones, a los proponentes que acrediten la vinculación de trabajadores con discapacidad en su planta de personal, de acuerdo con los siguientes requisitos: 1. La persona natural, el representante legal de la persona jurídica o el revisor fiscal, según corresponda, certificarán el número total de trabajadores vinculados a la planta de personal del proponente o sus integrantes a la fecha de cierre del proceso de selección. 2. Acreditar el número mínimo de personas con discapacidad en su planta de personal, de conformidad con lo señalado en el certificado expedido por el Ministerio de Trabajo, el cual deberá estar vigente a la fecha de cierre del proceso de selección.*

Verificados los anteriores requisitos, se asignará el 1%, a quienes acrediten el número mínimo de trabajadores con discapacidad, señalados a continuación:

Número total de trabajadores de la planta de personal del proponente	Número mínimo de trabajadores con discapacidad exigido
Entre 1 y 30	1
Entre 31 y 100	2
Entre 101 y 150	3
Entre 151 y 200	4
Más de 200	5

Parágrafo. *Para efectos de lo señalado en el presente artículo, si la oferta es presentada por un consorcio, unión temporal o promesa de sociedad futura, se tendrá en cuenta la planta de personal del integrante del proponente plural que aporte como mínimo el cuarenta por ciento (40%) de la experiencia requerida para la respectiva contratación*."

Basado en lo anterior, el oferente que cumpla con lo exigido en el factor INCENTIVO EN FAVOR DE PERSONAS EN CONDICIÓN DE DISCAPACIDAD le será asignado los diez (10) puntos correspondientes.

El oferente que desee acreditar dicho factor debe anexar certificación firmada por la persona natural, el representante legal de la persona jurídica o el revisor fiscal, según corresponda, sobre el número total de trabajadores vinculados a la planta de personal del proponente o sus integrantes a la fecha de cierre del proceso de selección. Igualmente debe anexar la correspondiente copia del certificado expedido por el Ministerio de Trabajo según el Decreto 392 de 2018 que acredite la vinculación del número de trabajadores en condición de discapacidad.

5.3. CRITERIOS DE DESEMPATE

En el caso de que dos oferentes o más empaten, se adjudicará por sorteo mediante el método de balotas, en este caso se citará a los oferentes empatados y mediante acta se dejará constancia del sorteo, estén o no estén presentes los oferentes en empate.

5.4. CAUSALES DE RECHAZO

Son causales para que una oferta no sea considerada por LA UNIVERSIDAD:

a) Que el proponente no oferte la totalidad de los bienes y/o servicios requeridos y señalado en el Capítulo III de la presente invitación a cotizar, ya que la Universidad NO ACEPTA OFERTAS PARCIALES
b) Que el proponente se encuentre en una situación de incapacidad, inhabilidad o incompatibilidad que le impida contratar con LA UNIVERSIDAD.
c) Cuando se presenten dos o más propuestas por el mismo oferente bajo el mismo nombre o con nombres diferentes.
d) Cuando la UNIVERSIDAD haya solicitado aclaración o documento alguno y el proponente

no lo corrija o no lo entregue en el término establecido.

e) Cuando la propuesta exceda los PRESUPUESTOS PARCIALES determinados por la Universidad.
f) Cuando la propuesta se presente extemporáneamente o no se presente en el lugar y hora establecido en este documento.
g) Cuando se compruebe cualquier irregularidad en los documentos presentados durante el trámite de la propuesta.
h) Cuando a criterio de la UNIVERSIDAD la propuesta presente deficiencias que no puedan ser aclaradas y que impidan compararla.
i) Si el oferente no cumple con la política ambiental de la entidad para la disposición de residuos que puedan afectar el medio ambiente y determinar la correcta disposición final de los mismos.
j) Cuando alguno de los documentos que se presenten carezcan de algún aspecto sustancial que soporte el contenido de la oferta y no sea susceptible de subsanación.
k) Si como persona Natural o Jurídica no tiene más de tres (3) años de constituida y registrada ante la Cámara de Comercio o en caso de consorcios o uniones temporales al menos uno de los consorciados no cuente con más de tres (3) años de constitución.
l) Cuando la UNIVERSIDAD encuentre inexactitud en la oferta que le permita cumplir con un requisito obligatorio.
m) Si el oferente no discrimina los impuestos y el objeto contratado causa dichos impuestos, la oferta será rechazada.

5.5. NO ACEPTACIÓN DE OFERTAS

LA UNIVERSIDAD puede no aceptar la propuesta o no contratar cuando:

a) Ninguna de las que se presenten cumpla los requisitos sustanciales exigidos para el efecto en la solicitud de oferta.
b) Ninguna de las propuestas sea conveniente para la entidad, por razón de factores objetivos en cuanto al costo de estas o a la calidad que ofrecen.

5.6. DECLARATORIA DE DESIERTA

LA UNIVERSIDAD puede a discrecionalidad no aceptar la propuesta o no contratar:

a) Cuando ninguna de las que se presenten cumpla los requisitos sustanciales exigidos para el efecto en la solicitud de oferta.
b) Cuando se presenten factores que impidan la comparación objetiva de las propuestas.
c) Cuando no se presente oferta.
d) Cuando se evidencie que la UNIVERSIDAD fue inducida en error por los oferentes habilitados

6.1. SUSCRIPCIÓN DEL CONTRATO

El proponente será informado de la adjudicación del contrato por parte de la UNIVERSIDAD, mediante comunicación escrita por correo electrónico a la cuenta consignada en el ANEXO 1 y, para lo cual se le allegará la minuta del contrato, debidamente suscrita por la Universidad.

Una vez decepcionada la comunicación, el contratista deberá proceder la suscripción y remisión del contrato, en un plazo máximo de dos (02) días hábiles, contados a partir del día siguiente de la fecha de recibo, por correo electrónico a la dirección que se indique al momento de comunicar la minuta contractual.

6.2. PERFECCIONAMIENTO Y EJECUCIÓN

El contrato quedará perfeccionado con la suscripción de este por las partes contratantes y para su ejecución requiere de la aprobación de las garantías parte de la Oficina Jurídica de la Universidad y la expedición del registro presupuestal.

6.3. GARANTÍA ÚNICA A FAVOR DE LA UNIVERSIDAD COLEGIO MAYOR DE CUNDINAMARCA

EL CONTRATISTA se obliga dentro de los tres (3) días hábiles siguientes al perfeccionamiento del contrato, a constituir a favor de la Universidad la garantía única, otorgada a través de una compañía de seguros que ampare los siguientes riesgos:

CLASE DE RIESGO	%	SOBRE EL VALOR	VIGENCIA
Cumplimiento	20	Total, del contrato	Se extenderá por el tiempo de ejecución del Contrato y cuatro (4) meses más.
Calidad del servicio	20	Total, del contrato	Se extenderá por el tiempo de ejecución del Contrato y un (1) año más
Calidad y correcto funcionamiento de los bienes y equipos suministrados	20	Total del contrato	Se extenderá por el tiempo de ejecución del Contrato y seis (6) meses más.
Pago de salarios, prestaciones sociales e indemnizaciones laborales	5	Total, del contrato	Se extenderá por el tiempo de ejecución del Contrato y tres (3) años más

Nota 1: Las pólizas suscritas por el tomador, deben expresamente señalar que se **EXPIDEN A FAVOR DE ENTIDADES PÚBLICAS CON RÉGIMEN PRIVADO DE CONTRATACIÓN**, dado que la Universidad no está sometida al régimen de contratación estatal.

Nota 2: El Contratista debe allegar constancia o recibo del pago de la prima correspondiente o incluirse constancia de que la garantía no expirará por falta de pago de la prima ni por revocación unilateral.
En caso de que se requiera adicionar, prorrogar o suspender el contrato resultante, o en cualquier otro evento necesario, el CONTRATISTA se obliga a modificarlas garantías de acuerdo con las normas legales vigentes establecidas en la presente invitación.

Nota 3: Para efectos del amparo de calidad del servicio, se considerará además de las coberturas establecidas en las condiciones generales, el acompañamiento del contratista ante el Comité Institucional de Gestión y Desempeño de la Universidad, como ante el Archivo General de la Nación, atendiendo los ajustes que se soliciten desde esas instancias.

6.4. CESIÓN DEL CONTRATO

El contratista no podrá ceder el contrato sin el consentimiento previo y escrito del Representante Legal de la UNIVERSIDAD, pudiendo éste negar la autorización de la cesión.

6.5. SUPERVISIÓN

La Supervisión del contrato resultante, estará a cargo del Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones o quien haga sus veces, quien tendrá las obligaciones propias del supervisor de acuerdo con el acuerdo 027 de 2023 – Manual de Contratación de la Unicolmayor, sin que la Supervisión releve al Contratista de sus responsabilidades.

6.6. DESCUENTOS DE LEY

LA UNIVERSIDAD practicará los descuentos legales a que haya lugar en los porcentajes que rijan al momento del pago, de acuerdo con las normas vigentes en dicho momento.

Si el OFERENTE no manifiesta tener la calidad de autorretenedor, de acuerdo con las normas vigentes, la UNIVERSIDAD efectuará al momento del pago los descuentos por concepto de retención en la fuente por cada factura, de acuerdo con los porcentajes que rijan en la fecha de pago, al tenor de las disposiciones tributarias vigentes.

6.7 VIGENCIA

La vigencia contrato resultante, será por el termino de ejecución estipulado más seis (6) meses, contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del

CONTRATO.

6.8 TERMINO PARA LIQUIDAR

Si derivado de esta invitación llega a suscribirse un contrato, una vez terminado el mismo, se procederá a su liquidación por parte de LA UNIVERSIDAD, mediante acta en la cual constarán las sumas de dinero recibidas por el contratista y la efectiva prestación del servicio. En el acta se hará constar el cumplimiento de las obligaciones a cargo de cada una de las partes, de acuerdo con lo estipulado en el contrato.

El acta llevará la firma del supervisor del contrato y el contratista. Si este último no se presenta a la liquidación, o las partes no llegan a un acuerdo sobre el contenido de esta, será suscrita directa y unilateralmente por LA UNIVERSIDAD.

El contrato resultante de esta invitación deberá ser liquidado máximo dentro de los seis (06) meses siguientes a la fecha determinación de este.

Términos de referencia aprobados de conformidad con el acuerdo 027 de 2022 y los procedimientos internos