PROYECTO DE PLIEGO DE CONDICIONES

PROCESO DE SELECCIÓN ABREVIADA DE MENOR CUANTÍA

Proceso de Contratación: SA-024-2026

OBJETO:

"ADQUIRIR E IMPLEMENTAR UN SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (Endpoint Detection and Response), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL). PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN."

Medellín, 28 de septiembre de 2026

INTRODUCCIÓN

EL INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN - INDER, en adelante la "Entidad", pone a disposición de los interesados el Proyecto de Pliego de Condiciones para la selección del Contratista encargado de ejecutar el Contrato de prestación de servicios, cuyo objeto es ***"*ADQUIRIR E IMPLEMENTAR UN SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (Endpoint Detection and Response), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL). PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN*".**

Los Documentos del Proceso, que incluyen los estudios y documentos previos, el estudio del sector, así como cualquiera de sus Anexos, están a disposición del público en el Sistema Electrónico de Contratación Pública –SECOP–.

La selección del Contratista se realizará a través del Proceso de Contratación de selección abreviada de menor cuantía **SA-024-2026**

La Entidad evaluará las ofertas con base en las reglas establecidas en el Pliego de Condiciones y en la normativa aplicable.

Todas las personas y organizaciones interesadas en hacer control social al Proceso de Contratación, en cualquiera de sus fases o etapas pueden presentar las recomendaciones que consideren convenientes, intervenir en las audiencias y consultar los Documentos del Proceso en los términos previstos en el inciso 3 del artículo 66 de la Ley 80 de 1993 y el artículo 2.2.1.1.1.2.1 del Decreto 1082 de 2015.

I. ASPECTOS GENERALES

A. INSTRUCCIÓN PRELIMINAR

1. El proponente no podrá estar incurso dentro de las causales de inhabilidad o incompatibilidad previstas en el ordenamiento legal colombiano, para contratar con el Estado.
2. El proponente deberá conocer el Pliego de Condiciones y las normas que regulan la contratación de las entidades públicas y en especial todos los aspectos que puedan influir en la elaboración de su propuesta.
3. Los proponentes están en la obligación de actuar objetiva e imparcialmente; por lo que en todo momento deberán primar los intereses de la Entidad, asegurando así no incurrir en conflicto de intereses. En consecuencia, los proponentes evitarán dar lugar a situaciones en que se pongan en conflicto con sus obligaciones previas o vigentes, con respecto a las actividades que desarrollan o desarrollarán con terceros en ejercicio de su actividad profesional y/o comercial, o con su futura participación en el proceso de selección o en la ejecución de otros contratos. Por lo anterior, el proponente al momento de presentar su propuesta, deberá declarar que él, sus directivos y el equipo de trabajo, con el que se ejecutará el objeto contractual, no se encuentra incurso en conflicto de intereses.
4. Los proponentes deberán darle estricto cumplimiento a las previsiones y exigencias indicadas en los pliegos de condiciones, pues, estos últimos forman parte esencial del contrato; son la fuente de derechos y obligaciones de las partes y elemento fundamental para su interpretación e integración, pues contienen la voluntad de la administración a la que se someten los proponentes durante los procesos de selección y el oferente favorecido durante el mismo lapso y, más allá, durante la vida del contrato.
5. La presentación de la propuesta constituye evidencia de que se estudió el pliego de condiciones, los anexos y demás documentos; que se recibieron las aclaraciones necesarias sobre las inquietudes o dudas previamente consultadas y se acepta que, el mismo, es completo compatible y adecuado para identificar bienes o servicios que se contratarán.
6. La presentación de la propuesta indica igualmente que el proponente está enterado a satisfacción en cuanto al alcance del objeto a contratar y que ha tenido en cuenta todo lo anterior, para definir las obligaciones que se adquieren en virtud del contrato que se celebrará.
7. Los proponentes por la sola presentación de su propuesta, autorizan a la Entidad a verificar toda la información que en ella suministren.
8. Toda consulta deberá formularse por escrito en el Portal Único de Contratación Pública - SECOP II www.colombiacompra.gov.co, no se atenderán consultas personales ni telefónicas. Las respuestas a las consultas se harán igualmente mediante escrito suscrito por el competente y dadas a conocer por publicación en el Portal Único de Contratación Pública SECOP II.

9. En caso de persona jurídica, la propuesta debe ser presentada por quien tenga la representación legal de la persona jurídica y/o se encuentre facultado para tal fin. Su nombre será verificado con el que aparece en la cédula de ciudadanía y el certificado de existencia y representación legal. Si usa una sigla ésta debe estar debidamente autorizada.
10. Corresponde al proponente enterarse en forma suficiente de las condiciones particulares de ejecución, resolver previamente las inquietudes que le suscite este pliego de condiciones, según el caso. Por los principios de lealtad procesal y buena fe, deberá advertir a la Administración los errores o inconsistencias que advierta en este documento.
11. Cuando la propuesta contenga información o documentos que tengan el carácter de reservados, de acuerdo con la ley colombiana, el proponente deberá hacer manifestación expresa de tal circunstancia en la carta de presentación de la oferta soportándolo legalmente. En caso de no hacerlo se entenderá que toda la información allí contenida es pública.

B. INVITACIÓN A LAS VEEDURÍAS CIUDADANAS

En cumplimiento de lo dispuesto en el inciso 3 del artículo 66 de la Ley 80 de 1993 El Instituto de Deportes y Recreación – INDER -, invita a todas las personas y organizaciones interesadas en hacer control social al presente Proceso de Contratación, en **cualquiera** de sus fases o etapas, a que presenten las recomendaciones que consideren convenientes, intervengan en las audiencias y a que consulten los Documentos del Proceso en el SECOP II.

C. COMPROMISO ANTICORRUPCIÓN

En el evento de conocerse casos especiales de corrupción en las Entidades del Estado, se debe reportar el hecho al Programa Presidencial “Lucha contra la Corrupción” a través de: los números telefónicos: (1) 560 1095, (1) 565 76 49, (1) 562 41 28; vía fax al número telefónico: (1) 565 86 71; la línea transparente del programa, a los números telefónicos: 01 8000 913 040 o (1) 560 75 56; en el correo electrónico: webmaster@anticorrupción.gov.co; al sitio de denuncias del programa, en el Portal de Internet: www.anticorrupción.gov.co; correspondencia o personalmente, en la dirección Carrera 8 No 7–27, Bogotá, D.C.

D. TRANSPARENCIA

El INDER Medellín, garantiza a los interesados en el proceso, que la selección que nos ocupa se realizará siempre de conformidad con la normatividad vigente, las Leyes 80 de 1993, 1150 de 2007,1474 de 2011, la Ley 2069 de 2020, Decreto 1082 de 2015, Decreto 1860 de 2021 y todas las leyes y decretos que regulen la materia.

Es por ello que, en las distintas etapas del proceso contractual, los interesados cuentan con plenas garantías materializadas en el derecho a conocer y controvertir los distintos informes, conceptos y decisiones que se adopten y publiquen en desarrollo del proceso.

Así mismo, se deja constancia que las actuaciones del INDER MEDELLIN dentro de este proceso contractual son públicas y los expedientes que las contengan estarán abiertos al público. INDER MEDELLÍN expedirá copias del proceso contractual a solicitud y costas del solicitante, incluyendo copia de las propuestas, respetando la reserva de que gocen legalmente algunos documentos.

El INDER MEDELLÍN, consagra en el proyecto de pliego de condiciones requisitos objetivos y necesarios para participar del proceso, que además permitirán garantizar la selección objetiva a través de parámetros justos, claros y completos, precisando las condiciones de costo y calidad de los bienes y servicios necesarios para la ejecución del contrato de manera objetiva.

Por lo anterior, el presente proceso se hará con plena observancia del principio de transparencia, materializado en los diferentes actos u actuaciones administrativas generadas por la Entidad, desde la fase pre-contractual hasta la pos-contractual serán motivadas (Artículo 24, Numeral 7 de la Ley 80 de 1993).

E. COMUNICACIONES

Las comunicaciones en el marco del presente Proceso de Contratación deben hacerse por medio del canal que la plataforma SECOP II destinada para tal fin.

En caso de indisponibilidad de la plataforma del SECOP II, que impida a los interesados presentar su propuesta, deberán atender los lineamientos definidos por Colombia Compra Eficiente, en la "Guía para actuar ante una indisponibilidad del SECOP II" y, para los efectos allí indicados, el correo habilitado por la entidad para del proceso es santiago.restrepov@inder.gov.co

Las comunicaciones y solicitudes enviadas al INSTITUTO DE DEPORTES Y RECREACIÓN – INDER -, por canales distintos a los mencionados, sólo serán tenidas en cuenta para los propósitos del Proceso de Contratación cuando sean radicadas a través del canal que corresponda.

F. INFORMACIÓN INEXACTA

La Entidad se reserva el derecho de verificar integralmente la información aportada por el Proponente. Para esto, se puede acudir a las autoridades, personas, empresas o entidades respectivas. Cuando exista inconsistencia entre la información suministrada por el Proponente y la verificada por la Entidad, la información que se pretende demostrar se entenderá como no acreditada.
La Entidad remitirá copias a las autoridades competentes en aquellos eventos en los cuales la información aportada tenga inconsistencias sobre las cuales pueda existir una posible falsedad, sin que el Proponente haya demostrado lo contrario, y rechazará la oferta.

G. INFORMACIÓN RESERVADA

Si dentro de la propuesta el Proponente incluye información que conforme con la ley colombiana tiene el carácter de información reservada, este debe manifestar esta circunstancia con claridad y precisión en el "Formato 1 – Carta de Presentación de la Oferta", identificando el documento o información que considera goza de reserva, citando expresamente la disposición legal que lo ampara. Sin perjuicio de lo anterior y para evaluar las propuestas, la Entidad se reserva el derecho de dar a conocer la mencionada información a sus funcionarios, empleados, contratistas, agentes o asesores.

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

H. IDIOMA

La propuesta, correspondencia y todos los documentos intercambiados entre los proponentes y el Instituto de Deportes y Recreación – INDER -, deberán estar escritos en idioma castellano. Los documentos de apoyo y el material proporcionado por el proponente adjunto a la propuesta pueden estar en otro idioma, siempre y cuando se acompañen de una traducción apropiada al castellano.

Para efectos de interpretación de la propuesta prevalecerá el texto en castellano.

I. LEGALIZACIÓN DE DOCUMENTOS OTORGADOS EN EL EXTERIOR

Los documentos otorgados en el exterior, que no estén en idioma castellano, deberán presentarse legalizados y acompañados de una traducción oficial de dicho idioma al español. Los documentos otorgados en el exterior deberán presentarse legalizados o apostillados en la forma prevista en las normas vigentes sobre la materia, en especial en los artículos 74 y 251 del Código General del Proceso, Artículo 480 del Código de Comercio, en el inciso 2º, numeral

22.4, del artículo 22 de la Ley 80 de 1993 y en la Resolución 2201 del 22 de julio de 1997 proferida por el Ministerio de Relaciones Exteriores de Colombia.

J. CONSULARIZACIÓN

De conformidad con lo previsto por el artículo 480 del Código de Comercio, "*los documentos otorgados en el exterior se autenticarán por los funcionarios competentes para ello en el respectivo país, y la firma de tales funcionarios lo será a su vez por el cónsul colombiano o, a falta de Este, por el de una nación amiga, sin perjuicio de lo establecido en convenios internacionales sobre el régimen de los poderes*". Tratándose de sociedades, expresa, además, el citado artículo del Código de Comercio que "*al autenticar los documentos a que se refiere este artículo los cónsules harán constar que existe la sociedad y ejerce su objeto conforme a las leyes del respectivo país*".

Surtido el trámite señalado en el presente numeral, estos documentos deberán ser presentados ante el Ministerio de Relaciones Exteriores de Colombia (Oficina de Legalizaciones ubicada en la Av. Carrera 19 N° 98-03 Edificio Torre 100 Piso 6, Bogotá D.C.) para la correspondiente legalización de la firma del cónsul y demás trámites pertinentes.

K. APOSTILLA

Cuando se trate de documentos de naturaleza pública otorgados en el exterior, no se requerirá del trámite de consularización, siempre que provengan de uno de los países signatarios de la Convención de La Haya del 5 de octubre de 1961, sobre abolición del requisito de legalización para documentos públicos extranjeros, aprobada por la Ley 455 de 1998. En este caso solo será exigible el trámite de apostilla, el cual consiste en el certificado mediante el cual se avala la autenticidad de la firma y el título a que ha actuado la persona firmante del documento y que se surte ante la autoridad competente en el país de origen.

Si el trámite de apostilla está dado en idioma distinto del castellano, deberá presentarse acompañada de una traducción oficial de dicho idioma al español y la firma del traductor, legalizada de conformidad con las normas vigentes.

Para cualquier duda relacionada con estos trámites de legalización y apostilla, puede consultarse la página web:
http://www.cancilleria.gov.co/tramites_servicios/apostilla_legalizacion

L. CONVERSIÓN DE MONEDAS

Los Proponentes deben presentar sus estados financieros en la moneda legal del país en el cual fueron emitidos y adicionalmente en pesos colombianos.

M. RÉGIMEN LEGAL

De conformidad con el artículo 13 de la Ley 80 de 1993, el proceso de selección, el contrato y su liquidación, se regirán por las disposiciones comerciales y civiles pertinentes, salvo en las materias particularmente reguladas en el Estatuto General de Contratación (Ley 80 de 1993, la Ley 1150 de 2007 y Decreto 1082 de 2015).

Si existiera contradicción entre el pliego y la ley, primará lo establecido en la ley. Cuando se llegaren a presentar vacíos en el pliego de condiciones, éstos se suplirán con el Estatuto General de Contratación y Decretos Reglamentarios, y si los vacíos continúan, éstos se suplirán con las normas del Código de Comercio y Código Civil.

N. CONSULTA Y PUBLICIDAD DEL PROCESO

De conformidad con el artículo 2.2.1.1.2.1.4 del Decreto 1082 de 2015; el proyecto de pliego de condiciones se publicará mínimo con cinco (5) días hábiles de antelación a la apertura del presente proceso en la plataforma SECOP II a partir de la fecha señalada en el cronograma del proceso.

Durante este término, los posibles oferentes y la ciudadanía en general, podrán formular observaciones mediante el canal de observaciones que la plataforma SECOP II tiene habilitada para tal fin, indicando con claridad que se trata de observaciones a este proceso contractual.

De conformidad con el artículo 2.2.1.1.1.7.1 del Decreto 1082 de 2015; el proyecto de pliego de condiciones se publicará en la plataforma SECOP II a partir de la fecha señalada en el cronograma del proceso.

Dentro del plazo del proceso cualquier interesado podrá solicitar por escrito otras aclaraciones que no hubieren sido resueltas. Dicha solicitud deberá hacerse mediante el canal de observaciones que la plataforma SECOP II tiene habilitada para tal fin.

Si estas observaciones son acogidas en la etapa previa, se reflejarán en el pliego de condiciones definitivo, en el caso de que se considere la procedencia de las aclaraciones u observaciones luego de publicar el pliego de condiciones definitivo, se elaborará la Adenda correspondiente, la cual será publicada en la página Web del Portal Único de Contratación; a partir de su publicación se entenderá conocidas por los interesados; todo ello en virtud del principio de economía, que rige los procedimientos contractuales.

En caso de considerarlo necesario, la Entidad podrá expedir adendas para modificar el cronograma, una vez vencido el término para la presentación de las ofertas y antes de la adjudicación del contrato.
El Instituto de Deportes y Recreación – INDER -, para efectos de garantizar la igualdad entre los proponentes, la publicidad en las decisiones de la administración y la economía, en el presente procedimiento de selección, publicará en la plataforma SECOP II, las respuestas a las observaciones presentadas, que no modifiquen el Pliego de Condiciones. Para ello basta ingresar a la página citada, y ubicar el contenido de este proceso. A medida que se reciban observaciones de los proponentes, éstas se ingresarán en forma consecutiva y serán publicadas en aquel sitio Web.

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

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

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

O. ELABORACIÓN Y PRESENTACIÓN DE LA OFERTA

El Proponente tiene la responsabilidad y carga de presentar su oferta en forma completa e íntegra, esto es, respondiendo todos los puntos del Pliego de Condiciones y adjuntando los documentos de soporte o prueba de las condiciones que pretenda hacer valer en el proceso.

De conformidad con el parágrafo 4 del artículo 2 de la Ley 1150 de 2007, el derecho de participación es gratuito.

P. CIERRE DEL PROCESO Y APERTURA DE OFERTAS

Se entienden recibidas por la Entidad las ofertas que se encuentren en la plataforma del SECOP II a la fecha y hora indicada en el Cronograma del Proceso de Contratación. Después de este momento el SECOP II no permitirá recibir más propuestas por excederse del tiempo señalado en el Cronograma.

Vencido el término para presentar ofertas, la Entidad Estatal debe realizar la apertura de los sobres y publicar la lista de oferentes. Luego de la apertura las propuestas son públicas y cualquier persona puede consultarlas. La Entidad Estatal dará a conocer las ofertas radicadas en el Proceso de Contratación haciendo clic en la opción “publicar ofertas” para que sean visibles a todos los Proponentes.

Se darán por no presentadas las Propuestas que no hayan sido entregadas en la plataforma y en el plazo previsto para ello en el Pliego de Condiciones. No se tendrán como recibidas las ofertas allegadas por medios distintos al SECOP II o que no sean presentadas de conformidad con los Términos y Condiciones de Uso del SECOP II.

Sin embargo, cuando haya una indisponibilidad del SECOP II, la cual hubiese sido confirmada por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente mediante certificado de indisponibilidad, la Entidad Estatal puede recibir ofertas en los términos y condiciones establecidos en el “Protocolo para actuar ante una indisponibilidad del SECOP II” o en el documento que Colombia Compra Eficiente determine para ello. [Puede consultarlo en el siguiente enlace: https://www.colombiacompra.gov.co/secop-ii/indisponibilidad-en-el-secop-ii].

Q. INFORME DE EVALUACIÓN

En la fecha establecida en el Cronograma, la Entidad publicará el informe de evaluación de los documentos e información de los requisitos habilitantes. El informe permanecerá publicado en el SECOP II y a disposición de los interesados durante tres (3) días hábiles, término hasta el cual los Proponentes podrán hacer las observaciones que consideren y entregar los documentos y la información solicitada por la Entidad, salvo que ya lo hubieren hecho en un momento anterior, de conformidad con el mismo numeral citado.

En virtud del principio de transparencia, la Entidad motivará de forma detallada y precisa el informe de evaluación explicando el rechazo de las ofertas y los documentos que se necesitan subsanar -en caso de que no se hayan subsanado durante la evaluación-.

Con posterioridad al vencimiento del plazo para presentar observaciones y a más tardar el día antes de la adjudicación, hasta las 11:59 p.m. de acuerdo con lo señalado en el Cronograma, la Entidad debe publicar el informe final de evaluación, en caso de que el inicial hubiese tenido variaciones.

R. PROPUESTAS PARCIALES

No se admitirán propuestas parciales.

S. LIMITACIÓN A MIPYME

Respecto del proceso de contratación No. SA-024-2026, conforme con el artículo 12 de la Ley 1150 de 2007, modificado por el artículo 34 de la Ley 2069 de 2020, reglamentado por el artículo 2.2.1.2.4.2.2. y siguientes del Decreto 1082 de 2015, modificado por el Decreto 1860 de 2021, en razón de la modalidad de selección aplicable -Licitación pública- y al valor establecido para su Presupuesto oficial -el cual excede el rango de Ciento veinticinco mil dólares de los Estados Unidos de América (US$125.000)-, no resulta aplicable lo consagrado en la normatividad en comento, y por tanto, **NO ES SUSCEPTIBLE DE SER LIMITADO A MIPYMES** (Micro, Pequeñas y Medianas empresas), ya que no se cumple con los parámetros descritos en la normativa"

T. REGLAS DE SUBSANABILIDAD, EXPLICACIONES Y ACLARACIONES

En caso de identificar inconsistencias o errores en los documentos con los cuales el proponente acredite el cumplimiento de los requisitos habilitantes, el Comité de Estructuración y Evaluación podrá solicitar al proponente en el término legal aclarar, aportar, completar o corregir dichos documentos.
En consecuencia, se rechazarán las ofertas de quienes no aclaren, completen o corrijan la información para acreditar los requisitos habilitantes en el plazo otorgado por la Ley.

En todo proceso de selección de contratistas primará lo sustancial sobre lo formal. En consecuencia, no podrá rechazarse una propuesta por la ausencia de requisitos o la falta de documentos que verifiquen las condiciones del proponente o soporten el contenido de la oferta, y que no constituyan los factores de escogencia establecidos por el INDER MEDELLÍN en el pliego de condiciones.

De conformidad con el parágrafo 1 ° del artículo 5, de la Ley 1150 de 2007, modificado por el parágrafo 1 del artículo 5 de la ley 1882 de 2018: "*La ausencia de requisitos o la falta de documentos referentes a la futura contratación o al proponente, no necesarios para la comparación de las propuestas no servirán de título suficiente para el rechazo de los ofrecimientos hechos. En consecuencia, todos aquellos requisitos de la propuesta que no afecten la asignación de puntaje, deberán ser solicitados por las entidades estatales y deberán ser entregados por los proponentes hasta el término de traslado del informe de evaluación que corresponda a cada modalidad de selección, salvo lo dispuesto para el proceso de Mínima Cuantía y para el proceso de selección a través del sistema de subasta. Serán rechazadas las ofertas de aquellos proponentes que no suministren la información y la documentación solicitada por la entidad estatal hasta el plazo anteriormente señalado.*

Durante el término otorgado para subsanar las ofertas, los proponentes no podrán acreditar circunstancias ocurridas con posterioridad al cierre del proceso."

De igual manera, se recuerda lo establecido por los parágrafos 3 y 4 del artículo 5 de la ley 1882 de 2018, que para el efecto establece que:
"*Parágrafo 3. La no entrega de la garantía de seriedad junto con la propuesta no será subsanable.*"
"*Parágrafo 4. En aquellos procesos de selección en los que se utilice el mecanismo de subasta, los documentos referentes a la futura contratación o al proponente, no necesarios para la comparación de las propuestas, deberán ser solicitados hasta el momento previo a su realización*"

Tales requisitos o documentos podrán ser requeridos por la Entidad en el plazo señalado en el cronograma del proceso de selección.

Para efectos de subsanar los documentos habilitantes, el INDER MEDELLÍN, se tendrá como plazo el indicado en el cronograma del proceso.

U. CRONOGRAMA DEL PROCESO

PUBLICACIÓN DEL AVISO DE CONVOCATORIA, ESTUDIOS PREVIOS Y PUBLICACIÓN DEL PROYECTO DE PLIEGO DE CONDICIONES.	28 de septiembre de 2026.
OBSERVACIONES AL PROYECTO DE PLIEGO DE CONDICIONES	Hasta el 5 de octubre de 2026.
RESPUESTA A OBSERVACIONES AL PROYECTO DE PLIEGO DE CONDICIONES	Hasta el 6 de octubre de 2026.

MANIFESTACIÓN DE INTERÉS PARA LIMITAR LA CONVOCATORIA EXCLUSIVAMENTE A MIPYMES	Hasta el 6 de octubre de 2026.
RESOLUCIÓN DE APERTURA DEL PROCESO DE SELECCIÓN	Hasta el 7 de octubre de 2026.
PUBLICACIÓN DEL PLIEGOS DE CONDICIONES DEFINITIVO	Hasta el 7 de octubre de 2026.
PLAZO PARA MANIFESTACIÓN INTERÉS SECOP II	Hasta el 13 de octubre de 2026.
AUDIENCIA DE SORTEO Y PUBLICACIÓN DE LA LISTA DE PRECALIFICADOS	La Entidad NO hará sorteo.
OBSERVACIONES AL PLIEGO DE CONDICIONES DEFINITIVO	Hasta el 13 de octubre de 2026.
PUBLICACION DE LAS RESPUESTAS A OBSERVACIONES AL PLIEGO DE CONDICIONES DEFINITIVO	Hasta el 14 de octubre de 2026.
PLAZO MÁXIMO PARA PUBLICAR ADENDAS	Hasta el 14 de octubre de 2026.
ENTREGA DE PROPUESTAS	El 16 de octubre de 2026, a través de la plataforma SECOP II.
PUBLICACIÓN INFORME DE EVALUACIÓN PRELIMINAR	Hasta el 20 de octubre de 2026.
TRASLADO PARA OBSERVACIONES AL INFORME CONSOLIDADO DE EVALUACION Y FECHA PARA PRESENTAR LOS DOCUMENTOS Y LA INFORMACION SOLICITADA POR LA ENTIDAD	Hasta el 23 de octubre de 2026.
TERMINO PARA RESPONDER OBSERVACIONES Y ASIGNAR PUNTAJES	Hasta el 26 de octubre de 2026.
RESOLUCIÓN DE ADJUDICACIÓN DEL CONTRATO O DECLARATORIA DE DESIERTO	Hasta el 28 de octubre de 2026.

V. MANIFESTACIÓN DE INTERES PARA PARTICIPAR EN EL PROCESO

Los oferentes deberán realizar su manifestación de interés a través de la herramienta dispuesta para ello en la plataforma SECOP II.

W. CAUSALES DE RECHAZO

Son causales de rechazo de las propuestas las siguientes:

A. Que el proponente o alguno de los integrantes del proponente plural esté incurso en causal de inhabilidad, incompatibilidad o prohibición previstas en la legislación para contratar.

B. Que el proponente o alguno de los integrantes del proponente plural esté reportado en el Boletín de Responsables Fiscales que administra la Contraloría General de la República.
C. Que la persona jurídica proponente individual o integrante del proponente plural esté incursa en la situación descrita en el numeral 1 del artículo 38 de la Ley 1116 de 2006, relacionada con la disolución de la persona jurídica.
D. Si la propuesta se presenta en forma extemporánea o en un lugar y fecha diferente al establecido en el pliego de condiciones y en el cronograma del SECOP.
E. Que el proponente no aclare, subsane o aporte documentos necesarios para cumplir un requisito habilitante, o aportándolos no lo haga de forma correcta, en los términos establecidos en la sección.
F. Que el proponente aporte información inexacta sobre la cual pueda existir una posible falsedad en los términos de la selección.
G. Que el proponente se encuentre incurso en un conflicto de intereses previsto en una norma de rango constitucional o legal.
H. Cuando se presenten inconsistencias, inexactitudes o inconformidades entre la información o documentación allegada por el proponente y lo verificado por la entidad, sin perjuicio de las acciones legales que puedan iniciarse por este hecho.
I. Cuando el oferente: persona jurídica, persona natural, consorcio o unión temporal presente más de una propuesta para este mismo proceso.
J. Cuando uno o más socios de la persona jurídica proponente o su representante legal, se presenten como personas naturales en este mismo proceso.
K. Cuando se presenten dos (2) o más propuestas por el mismo oferente, bajo el mismo nombre o con nombres diferentes
L. Que el objeto social del proponente o el de alguno de sus integrantes no le permita ejecutar el objeto del contrato.
M. No ofrecer u ofrecer cero (0) en el valor de un precio unitario.
N. Superar el valor unitario de alguno o algunos de los ítems ofrecidos con respecto al valor establecido para cada ítem del presupuesto oficial (si aplica).
O. Cuando se presente propuesta condicionada para la aceptación de la oferta.
P. Presentar la oferta extemporáneamente.
Q. No presentar oferta económica (si aplica).
R. Cuando se determine que el valor total de la oferta es artificialmente bajo, de acuerdo con lo establecido en la sección.
S. Cuando se presenten propuestas parciales y esta posibilidad no haya sido establecida en la invitación pública.
T. Ofrecer un plazo mayor al previsto por la entidad en la sección.
U. Cuando una misma persona natural o jurídica, o integrante de un proponente plural, presente o haga parte en más de una propuesta para el mismo proceso. En tal caso todas las propuestas serán rechazadas.
V. Cuando el representante legal de la persona jurídica tenga limitaciones para comprometer a la sociedad y no cuente con la autorización suficiente del órgano social.

W. Cuando existan varias propuestas presentadas por el mismo proponente o por interpuesta persona, natural o jurídica, individualmente o formando parte de un consorcio o unión temporal para la misma convocatoria.
X. Cuando el proponente no allegue, o allegue de manera incompleta o ilegible a la Entidad, en el tiempo establecido por ella, los documentos o aclaraciones solicitados para subsanar la información requerida para verificar los requisitos habilitantes o de comparación de las ofertas.
Y. Cuando la oferta sea incompleta o parcial; esto es, cuando no cumpla lo especificado o no incluya algún documento que, de acuerdo con los Pliegos de condiciones, se requiera adjuntar, y dicha deficiencia impida la comparación objetiva con otras ofertas, en los términos del artículo 5 de la Ley 1150 de 2007, modificado por el artículo 5° de la Ley 1882 de 2018.
Z. Cuando el valor presentado por los proponentes supere el presupuesto oficial por ítems o total, incluso después de realizadas las correcciones aritméticas.
AA. Si después de efectuada la corrección aritmética, si hubiere lugar a ello, la diferencia entre el valor original y el valor corregido de la propuesta supera el cero punto cinco por ciento (0.5%) del valor original.
BB. Cuando la oferta no sea presentada de conformidad con lo estipulado en la guía para presentar oferta en el SECOP II emitida por Colombia Compra Eficiente.
CC. Cuando el valor presentado por los proponentes supere el presupuesto oficial por ítems o total, incluso después de realizadas las correcciones aritméticas.
DD. Si después de efectuada la corrección aritmética, si hubiere lugar a ello, la diferencia entre el valor original y el valor corregido de la propuesta supera el cero punto cinco por ciento (0.5%) del valor original.
EE. Cuando la propuesta sea artificialmente baja a consideración del Comité evaluador una vez agotado lo contemplado en el artículo 2.2.1.1.2.2.4 del Decreto 1082 de 2015.
FF. Cuando se compruebe que la información suministrada por los oferentes, sea contradictoria y no corresponda en algún aspecto a la verdad, o sea artificiosamente incompleta.
GG. Cuando se adicione, suprima, modifique, o altere uno o varios de los ítems, o no se oferten las cantidades del ANEXO 3, o cuando se modifique una cantidad o unidad del mismo anexo.
HH. Cuando verificada la propuesta se considere que el precio ofertado en la propuesta resulte artificialmente bajo y analizadas las explicaciones del proponente, el INDER considere con fundamentos objetivos y razonables que esa propuesta económica pone en riesgo el proceso y el cumplimiento de las obligaciones contractuales en caso de resultar favorecido con la adjudicación. Lo anterior aplica igualmente para el caso de oferta única que haya cumplido con los requisitos habilitantes.
II. Cuando un proponente, persona natural o el representante legal de la persona jurídica o del consorcio o unión temporal, se encuentre reportado en el boletín de antecedentes disciplinarios con sanción de destitución.

JJ. Cuando el proponente persona natural o representante legal de la persona jurídica o del consorcio unión temporal, según el caso, registre antecedentes judiciales consistentes en sentencia judicial condenatoria con pena accesoria de interdicción de derechos y funciones públicas.
KK. Cuando el proceso se limite a Mipyme y se presenten ofertas de empresas que no acrediten tal condición.
LL. Cuando la oferta de un proponente plural sea presentada desde el perfil de uno de sus integrantes y no como lo indica la guía para presentar oferta en el SECOP II, es decir desde el perfil que se debe crear para el oferente plural.
MM. Las demás previstas en la ley.

X. CAUSALES PARA DECLARAR DESIERTO EL PROCESO DE SELECCIÓN

La entidad podrá declarar desierto el procedimiento de selección cuando:

A. No se presenten ofertas.
B. Ninguna oferta resulte hábil, por no cumplir las exigencias de la Invitación.
C. Existan causas o motivos que impidan la escogencia objetiva del proponente.
D. Lo contemple la ley.

Y. RETIRO DE LA PROPUESTA

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

Si la oferta se presenta a través de SECOP II, el proponente debe seguir el proceso indicado en la “Guía rápida para la presentación de ofertas en SECOP II”. Una vez se cumpla la fecha de cierre del proceso la plataforma del SECOP II bloquea a los proveedores la opción del retiro de ofertas. En este sentido, basta el retiro de la oferta en la plataforma del SECOP II, sin necesidad de enviar una solicitud a la entidad.

Z. NORMAS DE INTERPRETACIÓN DEL PLIEGO DE CONDICIONES

Este Pliego de Condiciones debe interpretarse como un todo y sus disposiciones no deben entenderse de manera separada de lo que indica su contexto general. Por lo tanto, se considera integrada la información incluida en los Documentos del Proceso que lo acompañan y las Adendas que se expidan.

Además, se seguirán los siguientes criterios para la interpretación y entendimiento del Pliego de Condiciones:

A. El orden de los numerales, capítulos y cláusulas de este Pliego de Condiciones no deben interpretarse como un grado de prelación entre los mismos.
B. Los títulos de los numerales y capítulos utilizados en este pliego solo sirven como referencia y no afectan la interpretación de su contenido.
C. Las palabras en singular se entenderán también en plural y viceversa, cuando lo exija el contexto; y las palabras en género femenino, se entenderán en género masculino y viceversa, cuando el contexto lo requiera.
D. Los plazos en días establecidos en este Pliego de Condiciones se entienden como hábiles, salvo que de manera expresa la ley o la Entidad indique que se trata de calendario o de meses. Cuando el vencimiento de un plazo corresponda a un día no hábil o no laboral para la Entidad este se trasladará al día hábil siguiente.
E. Las palabras definidas en este Pliego de Condiciones deben entenderse en dicho sentido.
F. Las referencias a normas jurídicas incluyen las disposiciones que las modifiquen, adicionen, sustituyan o complementen.
G. Este pliego se interpretará, además, en lo pertinente, de conformidad con las reglas del Código Civil definidas en los artículos 1618 a 1624.

AA. PRECIO ARTIFICIALMENTE BAJO

Si de acuerdo con la información obtenida por la Entidad Estatal en su deber de análisis de que trata el artículo 2.2.1.1.2.2.4 del Decreto 1082 de 2015, el valor de una oferta parece artificialmente bajo, la Entidad Estatal debe requerir al oferente para que explique las razones que sustentan el valor ofrecido. Analizadas las explicaciones, el comité evaluador, o quien haga la evaluación de las ofertas, debe recomendar rechazar la oferta o continuar con el análisis de la misma en la evaluación de las ofertas.

Cuando el valor de la oferta sobre la cual la Entidad Estatal tuvo dudas sobre su valor responde a circunstancias objetivas del oferente y de su oferta, que no ponen en riesgo el cumplimiento del contrato si este es adjudicado a tal oferta, la Entidad Estatal debe continuar con su análisis en el proceso de evaluación de ofertas.

SC-SC CER203995 CO-SA CER307282
Calle 47D N.º 75-276, barrio Velódromo PBX: (604) 369 90 00
Correo: atencion.ciudadano@inder.gov.co | www.inder.gov.co
NIT: 800194096-0 | Código Postal 0500304
Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

1. CAPÍTULO II. ELABORACIÓN Y PRESENTACIÓN DE LA OFERTA

1.1. *OBJETO, PRESUPUESTO OFICIAL, PLAZO Y UBICACIÓN*

El objeto, Presupuesto Oficial, plazo y ubicación del proyecto objeto del Proceso de Contratación se identifican en la siguiente tabla:

Objeto del proyecto	Plazo del Contrato	Valor Presupuesto Oficial (pesos incluido IVA)	Lugar(es) de ejecución del Contrato
"ADQUIRIR E IMPLEMENTAR UN SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (Endpoint Detection and Response), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL). PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN."	Desde la firma del acta de inicio hasta el 31 de diciembre de 2026	OCHOCIENTOS VÉINTISEIS MILLONES QUINIENTOS SETENTA MIL PESOS M.L ($826.570.000)	En la ciudad de Medellín, Antioquia En Las Instalaciones del INDER Medellín

PARÁGRAFO: A más tardar el 15 de noviembre de 2026, el contratista deberá haber culminado las actividades de diagnóstico, instalación, configuración y parametrización, de manera que la solución se encuentre completamente implementada y en operación.

El plazo comprendido entre el 15 de noviembre y el 31 de diciembre de 2026 estará destinado a la ejecución de actividades posteriores a la implementación, tales como la elaboración de informes, actividades derivadas de la puesta en funcionamiento de la solución y verificaciones necesarias para la autorización de pago.

A partir del 31 de diciembre de 2026 y hasta el la finalización de la vigencia de las licencias, el contratista deberá continuar prestando de forma ininterrumpida, todos los servicios

contratados y previstos en las especificaciones técnicas incluyendo garantía, soporte, mantenimiento, disponibilidad, actividades con alcance dentro de la vigencia de las licencias y las demás obligaciones detalladas en las especificaciones técnicas, obligaciones específicas y garantizando el correcto funcionamiento de la solución durante todo el período de prestación del servicio correspondiente a 1 año.

FORMA DE PAGO:

El INSTITUTO DE DEPORTES Y RECREACION DE MEDELLIN - INDER MEDELLÍN pagará en un solo contado una vez se dé el cumplimiento de todas las actividades necesarias para la configuración, instalación, puesta en funcionamiento y verificación del sistema de ciberseguridad, incluyendo las respectivas pruebas de funcionamiento y la entrega del informe de instalación. Lo anterior deberá estar revisado y ser recibido a satisfacción por parte del supervisor y del apoyo técnico antes de dicha fecha, con el fin de garantizar que las licencias puedan iniciar su vigencia el 15 de noviembre de 2026.

El pago de la factura estará sujeto a las políticas y las disposiciones de Tesorería y según disponibilidad del Plan Anualizado de Caja- PAC.

La factura deberá ser presentada de forma electrónica, la cual debe cumplir como mínimo, los requisitos de las normas fiscales establecidas en el artículo 616-1 del Estatuto Tributario, o en su defecto la factura de venta presentada en original y con copia, la cual debe cumplir como mínimo, los requisitos de las normas fiscales establecidas en el artículo 617 del Estatuto Tributario. La fecha de la factura debe corresponder al mes de su elaboración, y en ella constará el número del contrato, el concepto del bien o servicio que se está cobrando y el nombre del Supervisor designado o funcionario responsable.

Una vez sea recibido a satisfacción área financiera solicitará una pro forma de la factura, una vez se autorice la pro forma de la factura, el contratista deberá subir la copia a la plataforma de CCE utilizada y enviar el comprobante al área financiera, posteriormente enviar la factura al correo facturacion@inder.gov.co. independientemente al envió de la factura electrónica, se deberán enviar los documentos soporte de la factura, certificado de paz y salvo de seguridad social y parafiscal, copia de la tarjeta profesional del revisor fiscal y certificado de antecedentes disciplinarios expedido por la Junta Central de Contadores no superior a 90 días, o cualquier otro que la supervisión del contrato considere.

El Contratista deberá informar al INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN - INDER, la cuenta bancaria (corriente o de ahorros), abierta a su nombre, en la cual le serán consignados o transferidos electrónicamente, los pagos que, por este concepto, le efectúe el Instituto.

De conformidad con el artículo 23 de la Ley 1150 de 2007, el contratista, deberá acreditar que se encuentra al día en el pago de aportes parafiscales relativos al Sistema de Seguridad Social Integral, así como los propios del SENA, ICBF y Cajas de Compensación Familiar, cuando corresponda. Esta información deberá ser acreditada por el CONTRATISTA para cada pago a efectuar, situación que deberá ser verificada por el Supervisor del INDER Medellín, pena de incurrir en causal de mala conducta.

Además, deberá acreditar que se encuentra al día en el pago de las obligaciones adquiridas con los proveedores, con quien tenga relación comercial emanada de la ejecución del contrato suscrito con el INDER.

Si el contratista no se encuentra a paz y salvo con el INDER, con la suscripción del contrato, autoriza para que la Tesorería del Instituto, en el momento de un pago, automáticamente y sin previo aviso realice el correspondiente cruce de cuentas, para compensar los valores que tenga en mora por cualquier concepto.

En el evento en que el contratista pretenda hacer cesión de derechos económicos o cualquier otro negocio jurídico financiero que conlleve a que los pagos derivados de la ejecución del contrato se hagan a terceras personas o a un patrimonio autónomo constituido por el contratista, deberá mediar autorización de la Entidad, previa acreditación de encontrarse a paz y salvo con proveedores y subcontratistas con quienes tenga relación comercial emanada de la ejecución del contrato.

Los recursos no ejecutados durante el plazo contractual serán reembolsados administrativamente al rubro y/o rubros respectivos.

Los recursos no ejecutados en la presente vigencia se someterán a las autorizaciones respectivas del consejo distrital de política fiscal CODFIS, para el visto bueno de constitución de reservas presupuestales y por ende los pagos estarán sujetos a la incorporación de estas al presupuesto del Instituto en la siguiente vigencia.

ALCANCE DEL OBJETO CONTRACTUAL. ESPECIFICACIONES TÉCNICAS:

La entidad requiere **ADQUIRIR E IMPLEMENTAR UN SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (Endpoint Detection and Response), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL) PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN.** Los servicios deben ser desplegados en nube y estar relacionados bajo una sola marca y deberán ser administrados mediante una sola interfaz de administración.

ALCANCE DE LA CAPACIDAD OPERATIVA DEL SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR, PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF.

Las soluciones deberán proporcionar de manera coherente y completamente interoperable capacidades de protección para Endpoints y servidores mediante EDR, correo electrónico, espacios de trabajo colaborativo, y sitios web, permitiendo la prevención, detección y respuesta ante amenazas de seguridad, así como el análisis y gestión de eventos e incidentes de seguridad, garantizando la trazabilidad de las acciones de protección y respuesta.

La solución deberá disponer de mecanismos de gestión centralizada que faciliten la operación, monitoreo y administración de los componentes de seguridad desde una interfaz unificada o integrada. Asimismo, deberá contar con garantía y soporte del fabricante y cumplir con las siguientes capacidades técnicas:

DIMENSIONAMIENTO DE LA SOLUCIÓN: A continuación, se realiza una discriminación de las especificaciones técnicas requeridas para satisfacer el objeto contractual:

I. **WAF (WEB APPLICATION FIREWALL)**:

La plataforma deberá ser desplegada y administrada en nube. Soportar la protección de aplicaciones institucionales expuestas a internet en entornos de computación en la nube, garantizando operación continua, escalabilidad automática, alta disponibilidad y balanceo de carga, bajo arquitectura de capa siete (HTTP/HTTPS). Estas capacidades deberán permitir la inspección, prevención y mitigación de ataques contra aplicaciones, la aplicación de políticas de seguridad administradas, así como la capacidad para auditoría, análisis forense y trazabilidad del tráfico. Para este propósito, la plataforma deberá soportar, como mínimo, una capacidad equivalente a la siguiente.

Con el fin de que los Proponentes tengan un panorama claro acerca del estado actual del consumo del WAF, se procede a brindar la siguiente información:

Datos actuales

- throughput promedio últimos 6 meses: 3.1 MB/s

- RPS promedio últimos 6 meses: 100
- Crecimiento últimos dos años 2 MB/s
- Sitios Web protegidos: 10.
- Transferencia total mensual: 8 TB
- Pico máximo últimos 6 meses 12.42 MB/s

Con la finalidad de que el Contratista que resulte adjudicado pueda solventar los picos de consumo, se recomienda presupuestar el consumo diario descrito a continuación:

- Se solicita un throughput promedio de 14.3 MB/s. Este se calcula de la siguiente manera: redondeamos el actual throughput a 3,5 MB/s en promedio y sumamos un crecimiento proyectado de 2 MB/s para los próximos 12 meses, esta suma da como resultado 5.5 MB/s al cual le sumamos 160 % de holgura para atender variaciones o picos de consumo durante la vigencia del servicio.

Pormenorización de los Datos de Requerimiento Mínimo Exigido:

- throughput promedio = (3.5+2) x 2.6) = 14.3MB/s
- Sitios Web a proteger: 10 sitos.
- Transferencia mensual mínima: 15 TB
- Conexiones persistentes requeridas 12.500 (si aplica)
- Validación del servicio: La solución debe estar en capacidad en realizar chequeos de salud (health checks) a servicios y/o aplicaciones, con el fin de detectar de forma proactiva el estado de los diferentes componentes de los servicios, para reaccionar de forma proactiva a una posible falla o indisponibilidad.

El INDER protegerá máximo 10 sitios web de su propiedad. Esta es una cantidad fija que ya incorpora el crecimiento máximo proyectado por la Entidad para el periodo de ejecución de las licencias, por lo que no se presentará incremento superior a 10 sitios durante la vigencia de la licencia.

El Contratista deberá prever, presupuestar y garantizar la capacidad mínima requerida y antes referenciada. De esta manera podrá atender eventuales incrementos en el consumo del WAF durante la ejecución del contrato, asegurando la continuidad de la protección de seguridad sin generar costos adicionales para el INDER Medellín por encima del presupuesto adjudicado. Para tal efecto, se recomienda considerar en su propuesta económica el consumo total diario estimado descrito.

El contratista también podrá proponer estrategias, mecanismos, políticas de usabilidad de los datos con la finalidad de disminuir los riesgos de picos en las transferencias.

II. PROTECCIÓN ENDPOINTS Y SERVIDORES.

Para el dimensionamiento de esta solución, la Entidad suministra los siguientes parámetros:

- Número de EndPoints existentes, número de servidores existentes y número de licencias endpoints de reserva.

El licenciamiento para 1.020 EndPoints y servidores no tendrá crecimiento durante la vigencia de las licencias, esta cantidad es fija y ya contempla el incremento máximo proyectado de equipos para el periodo de la vigencia de las licencias. La cantidad comprende 900 EndPoints, 20 servidores on premise y 100 licencias para respaldar el posible crecimiento proyectado de los EndPoints.

III. PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS.

Para el dimensionamiento de esta solución, la Entidad suministra los siguientes parámetros:

El INDER Medellín cuenta con M365, Se debe tener presente que el INDER actualmente cuenta con 2.300 cuentas de usuario de correo electrónico, que corresponden a una cantidad fija que no tendrá crecimiento durante la ejecución del contrato y la vigencia de las licencias, toda vez que este número ya considera el margen máximo de usuarios previsto por la Entidad.

Importante: Se aceptarán soluciones de cualquier fabricante, siempre que la totalidad de los componentes, funcionalidades y módulos que conformen la solución ofertada sean provistos por un único fabricante.

INICIO DE LA VIGENCIA DE LAS LICENCIAS

El Contratista deberá realizar, con anterioridad al 15 de noviembre de 2026, todas las actividades necesarias para la configuración, instalación, puesta en funcionamiento y verificación del sistema de ciberseguridad, incluyendo las respectivas pruebas de

funcionamiento y la entrega del informe de instalación. Lo anterior deberá revisado y ser recibido a satisfacción por parte del supervisor y del apoyo técnico antes de dicha fecha, con el fin de garantizar que las licencias puedan iniciar su vigencia el 15 de noviembre de 2026. De cualquier forma, la vigencia no deberá iniciar sin el recibido a satisfacción.

IV. **IMPLEMENTACIÓN Y SOPORTE TÉCNICO.**

La Entidad requiere Soporte Técnico durante 12 meses de la Plataforma de Ciberseguridad, la cual deberá contar como mínimo con las siguientes características:

1- Actualizaciones y mantenimiento de producto o Compatibilidad con nuevos sistemas operativos, acceso a versiones nuevas sin costo adicional dentro de la vigencia.
2- Deberá incluir atención remota telefónica 24/7, asistencia para configuración y despliegue, guías técnicas, manuales y base de conocimientos y SLA (acuerdo de nivel de servicio).
3- Deberá contar con medios de escalamiento que deberá corresponder como mínimo a una Plataforma helpdesk con usuario y contraseña.
4- Transferencia de Conocimiento: La actividad de transferencia de conocimiento inicial sobre uso del producto deberá ser como mínimo de 20 horas que será prestado a mínimo tres Contratista que forman parte del Equipo Técnico del INDER. La capacitación o actividad de transferencia del conocimiento deberá contar dentro de sus temáticas con las siguientes: a) laboratorios de aprendizaje de uso de la solución para administradores o equipos técnicos, documentación de mejores prácticas; b) Interfaz de administración
5- Recuperación, restablecimiento o migración sin costo adicional, en caso de que aplique.

En materia de implementación deberá realizar todas las actividades necesarias para la configuración, instalación, puesta en funcionamiento y verificación del sistema de ciberseguridad, incluyendo las respectivas pruebas de funcionamiento y la entrega del informe de instalación con el protocolo y resultados de pruebas realizadas. Lo anterior deberá ser recibido a satisfacción por parte del supervisor y del apoyo técnico.

DETALLES TÉCNICOS DE LOS SERVICIOS A CONTRATAR POR PARTE DEL INSTITUTO DE DEPORTS Y RECREACIÓN:

La solución deberá disponer de mecanismos de gestión centralizada que faciliten la operación, monitoreo y administración de los componentes de seguridad desde una sola

interfaz unificada o integrada. Asimismo, deberá contar con garantía y soporte del fabricante y cumplir con las siguientes capacidades técnicas:

Todas las características descritas a continuación son referencia al resultado esperado al implementar toda la solución mas no a una marca en específico, y sin restringir a una única forma de obtener el resultado final esperado, por lo cual se informa que sin importar el mecanismo que cada fabricante utiliza, la solución deberá permitir implementar todos los controles descritos.

1. PROTECCIÓN ENDPOINTS Y SERVIDORES	
La Entidad solicita una solución que provea la seguridad de las estaciones de trabajo y servidores mediante prevención, detección y respuesta ante amenazas en el EndPoint, que incluya protección contra malware, ransomware, amenazas sin archivo residentes en memoria, explotación de vulnerabilidades, robo de credenciales y uso malicioso de herramientas legítimas del sistema operativo, gestionada desde una sola interfaz.	
Cantidad	1020
Vigencia	12 Meses
Medida	Unidad
#	**Requerimiento Técnico Mínimo (de obligatorio cumplimiento)**
	GENERALIDADES
1.1	La Entidad requiere del licenciamiento de la solución EDR para 1020 dispositivos. **SERVIDORES ON-PREMISES (20)** Protección de servidores de centro de datos con diferentes sistemas operativos en cualquier versión: • Windows server 2008 • Windows server 2012 • Windows server 2016 • Windows server 2022 • Windows server 2025 • Linux Ubuntu 22.04 • CentOS 8 **ENDPOINTS (900)** • Debe tener compatibilidad Multiplataforma principalmente Windows, macOS en cualquier versión. **RESERVA ENDPOINTS (100)** • Debe tener compatibilidad Multiplataforma principalmente Windows, macOS en cualquier versión.
1.2	La solución de EDR debe proporcionar a la Entidad un conjunto de protecciones tanto en pre-ejecución —antes de que la amenaza tenga capacidad de comprometer el sistema— como en post-ejecución —cuando la amenaza ya interactúa con el servidor o la estación de trabajo—, con capacidad de respuesta en tiempo real. La capa de pre-ejecución debe incorporar un motor de prevención basado en aprendizaje automático, capaz de emitir un veredicto sobre archivos no vistos previamente sin depender exclusivamente de firmas, operando de forma local en el agente para mantener la protección en equipos desconectados de la red. La capa de post-ejecución debe operar mediante análisis de comportamiento en tiempo de ejecución, con capacidad de bloquear comunicaciones salientes a nivel de proceso, impedir el acceso malicioso al sistema de archivos y al registro, y detener el cifrado por ransomware, incluso en equipos sin conectividad con la consola de gestión.
2	**FUNCIONALIDADES DE PREVENCIÓN**

2.1	El EDR debe utilizar un motor antivirus de aprendizaje automático para detener la ejecución previa de malware. Esta capacidad NGAV viene integrada en un agente único y ligero, lo que permite a los usuarios asignar protección antimalware a cualquier grupo de terminales sin necesidad de ninguna solución adicional.
2.2	Disponer de aprendizaje automático, NGAV basado en kernel y Machine learning (ML)
2.3	Enriquecer los eventos de seguridad con información de inteligencia de amenazas proveniente de una base de datos en la nube actualizada de forma continua, incluyendo reputación de archivos, dominios y direcciones IP.
2.4	Mantener la capacidad de prevención y detección en equipos sin conectividad con la consola de gestión o con los servicios en la nube del fabricante, conservando la telemetría localmente y sincronizándola al restablecerse la conexión.
2.5	Proporcionar un control de dispositivos de almacenamiento extraíble (**Almacenamiento USB, Pendrive, Periféricos externos**), sobre estaciones de trabajo Windows, con políticas asignables de forma diferenciada por grupo de equipos. La solución debe permitir el bloqueo del uso de dispositivos por categoría (**Almacenamiento USB, Dispositivos móviles, Unidades ópticas, impresoras escáner, Dispositivos de interfaz HID, dongles, y los que pertenezcan en esta categorías**), y disponer de un mecanismo de autorización granular que habilite dispositivos específicos mediante su fabricante, descripción o número de serie, o una combinación de estos criterios. Todo intento de uso de dispositivo extraíble debe generar un evento registrado y consultable en la consola de gestión.
2.6	La solución debe reducir el ruido operativo mediante: clasificación automática del veredicto de cada evento, con historial y reclasificación posterior; agrupación de eventos relacionados en un incidente único; y excepciones granulares —acotables por proceso, ruta y grupo de equipos— que supriman detecciones equivalentes sin recurrir a exclusiones amplias.
2.7	La solución deberá evaluar vulnerabilidades en sistemas operativos y aplicaciones de EndPoints Windows, Windows Server y Linux, identificando CVE/CVSS, activos afectados y nivel de riesgo, y proporcionando mecanismos de mitigación como virtual patching mientras se realiza el parcheo definitivo.
3	**FUNCIONALIDADES DE DESCUBRIMIENTO**
3.1	El EDR debe contar con un sistema automatizado de control de políticas de superficie de ataques, con evaluaciones y descubrimiento de vulnerabilidades que permiten al personal encargado de la seguridad dar gestión.
3.2	Descubrir y controlar dispositivos no autorizados (por ejemplo, dispositivos no protegidos o no administrados) y detectar dispositivos IoT.
3.3	Realizar un seguimiento de aplicaciones ejecutadas, y su clasificación de seguridad.
3.4	Descubrir y mitigar las vulnerabilidades del sistema y las aplicaciones con parches virtuales, mediante el análisis de sus comunicaciones e inhabilitando el acceso a su comunicación con el exterior.
3.5	Al descubrir las vulnerabilidades debe mostrar la clasificación de reputación y el detalle de los códigos CVE aplicables
3.6	Reducir la superficie de ataque con políticas proactivas basadas en niveles de riesgo.
4	**FUNCIONALIDADES DE DETECCIÓN Y PROTECCIÓN**
4.1	El EDR debe detectar y desactivar el malware así sean amenazas del tipo sin archivos o file-less y otros ataques avanzados en tiempo real para proteger los datos y evitar brechas en la seguridad en la entidad. Tan pronto como el EDR detecte flujos y comportamientos sospechosos, inmediatamente debe desactivar las amenazas potenciales, bloquear las comunicaciones salientes y el acceso al sistema de archivos desde esos procesos sospechosos, por otro lado debe evitar la exfiltración de datos, las comunicaciones de comando y control (C&C), la manipulación de archivos y el cifrado de ransomware. Al mismo tiempo, el backend del EDR debe continuar recopilando evidencias adicionales, enriqueciendo los datos de eventos y clasificando los incidentes para aplicar de forma automatizada una estrategia de respuesta a incidentes, permitiendo así automáticamente la continuidad del negocio incluso en dispositivos ya comprometidos cumpliendo como mínimo con los siguientes ítems:
4.2	Detección basada en el análisis del comportamiento en tiempo de ejecución con visibilidad a nivel de kernel sobre los procesos y actividades del EndPoint, capaz de identificar técnicas de infiltración sigilosa, ataques residentes en memoria, ataques basados en scripts y uso malicioso de herramientas y binarios legítimos del sistema operativo (living off the land).

4.3	Debe Proporcionar protección en los procesos en ejecución, el inicio y parada de procesos, y en las interacciones entre procesos, así como frente a actividades sospechosas asociadas a librerías (archivos DLL en el caso de sistemas operativos Windows).
4.4	Debe poder Detener las amenazas en tiempo real y eliminar el tiempo de permanencia de dichas amenazas en la organización, incluso en los endpoints desconectados de la red corporativa.
4.5	Debe Bloquear las comunicaciones de forma granular a nivel de proceso, evitando exfiltraciones de datos, movimientos laterales y conexión con redes de comando y control.
4.6	Debe Impedir a los procesos maliciosos el acceso a los sistemas de ficheros, protegiendo frente a cifrados de ransomware, y la creación/modificación/eliminación maliciosa de archivos y/o registros.
4.7	Debe permitir definir listas de permitidos y denegados mediante criterios de identificación de archivos y aplicaciones que incluyan, como mínimo: hash del archivo, nombre y ruta de ubicación, y firma digital del editor, admitiendo para este último criterio la identificación por certificado, por huella digital del certificado o por nombre del firmante.
4.8	Debe Proporcionar la capacidad para marcar, tanto manual como automáticamente, determinada actividad como falso positivo, evitando además que ocurran detecciones similares.
4.9	La solución deberá conservar los eventos de seguridad y la telemetría de actividad del endpoint durante un período mínimo de noventa (90) días, disponibles para análisis retrospectivo mediante consultas estructuradas sobre la totalidad del período retenido.
4.10	La solución debe revalidar el veredicto de los eventos de seguridad mediante un análisis posterior en el servicio en la nube del fabricante, que incorpore inteligencia de amenazas. Cada reclasificación debe registrarse en un historial auditable, y las acciones de respuesta automatizada deben basarse en el veredicto final.
5	**FUNCIONALIDADES DE PROTECCIÓN CONTRA RANSOMWARE**
5.1	La solución de EDR debe contar con políticas predefinidas y exclusivas para la prevención de secuestro de información por ataques de ransomware, por lo cual debe incluir más de 30 estrategias de protección diferentes. Dichas estrategias deben incluir como mínimo:
5.2	1. Debug de Procesos.
5.3	2. Código dinámico.
5.4	3. Formato de archivo ejecutable incorrecto
5.5	4. Una pila con código ejecutable
5.6	5. El programa ejecutado no tiene instalador
5.7	6. Programa crítico falso.
5.8	7. Empaquetador falso.
5.9	8. File Encryptor.
5.10	9. Proceso oculto.
5.11	10. Ejecutable inyectado.
5.12	11. Proceso inyectado.
5.13	12. Hilo inyectado.
5.14	13. Suma de comprobación no válida.
5.15	14. Ejecución no válida.
5.16	15. Puntero no válido.
5.17	16. Inyección de kernel.
5.18	17. Empaquetador conocido.
5.19	18. Archivo malicioso detectado.
5.20	19. Proceso malicioso.
5.21	20. Ejecutable modificado.
5.22	21. Stack Parcialmente asignado.
5.23	22. Exploit de escalamiento de privilegios.
5.24	23. Proceso vacío.
5.25	24. Manipulación de pilas.
5.26	25. Aplicación sospechosa.
5.27	26. Empaquetador sospechoso.
5.28	27. Ejecutable manipulado.

5.29	28. Ejecutable no confirmado.
5.30	29. Ejecutable sin asignar.
5.31	30. Código grabable.
6	**FUNCIONALIDADES DE REMEDIACIÓN**
6.1	La Solución de EDR propuesta debe orquestar operaciones de respuesta a incidentes utilizando playbooks predefinidos en la solución, optimizando sí la respuesta a incidentes y los procesos de remediación, revirtiendo de modo automático los cambios maliciosos realizados por amenazas ya contenidas, en un único dispositivo o en dispositivos distribuidos a lo largo del entorno de la entidad, las características de remediación deben cumplir como mínimo con los siguientes requerimientos:
6.2	Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta.
6.3	La solución debe permitir definir playbooks de respuesta configurables por clasificación de evento y por grupo de dispositivos, con acciones ejecutables de forma automática o previa aprobación del analista.
6.4	Debe optimizar los recursos de seguridad, automatizando las acciones de respuesta a incidentes, como la eliminación de archivos, la finalización de procesos maliciosos, la reversión de cambios persistentes, la notificación a los usuarios, el aislamiento de aplicaciones y dispositivos, y la integración con una plataforma de ITMS para apertura de tickets.
6.5	Debe permitir la respuesta a incidentes basada en el contexto utilizando la clasificación de incidentes y los sujetos de los ataques (como por ejemplo, grupos de estaciones de trabajo).
6.6	Visibilidad completa de la cadena de ataque y de los cambios realizados en el sistema, con representación gráfica de la secuencia de procesos involucrados desde el origen.
6.7	Reversión automatizada de cambios de persistencia introducidos por la amenaza, incluyendo entradas de registro, tareas programadas y servicios creados o modificados.
6.8	Debe realizar la contención y respuesta de forma automática
6.9	Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta.
7	**FUNCIONALIDADES DE INVESTIGACIÓN**
7.1	La solución de EDR debe enriquecer automáticamente los registros de los eventos con información detallada sobre el malware antes y después de la infección, para realizar análisis forenses en los endpoints infiltrados. Su interfaz guiada debe proporcionar una guía útil, mejores prácticas y sugerir los próximos pasos lógicos a los analistas de seguridad, estas características de investigación deben cumplir como mínimo con los siguientes requerimientos:
7.2	Debe tener la capacidad de contención automática de la amenaza debe permitir que el análisis forense posterior se realice sin presión de tiempo, manteniendo el equipo operativo.
7.3	Debe contar con la capacidad de visualización de la cadena de ataque completa con identificación del origen de la infección (paciente cero), disponible incluso cuando el dispositivo se encuentre fuera de línea.
7.4	Debe conservar instantáneas de memoria, de los ataques sin archivo o file-less para la búsqueda de amenazas basada en memoria.
7.5	La interfaz grafica debe mostrar explicaciones claras por qué el evento está marcado como sospechoso o malicioso, enumera el marco de ataque MITRE correspondiente, así como el siguiente paso lógico para la investigación forense.
8	**FUNCIONALIDADES DE EDR**
8.1	La solución de EDR debe disponer de capacidades de integración con otras plataformas de seguridad del ecosistema de la Entidad, ya sea mediante conectores nativos preconfigurados por el fabricante o mediante interfaces de programación de aplicaciones (API) documentadas públicamente. La integración deberá permitir, como mínimo, el intercambio bidireccional de información de eventos e indicadores de compromiso, y la ejecución de acciones de respuesta coordinada. El proponente deberá acreditar, mediante documentación técnica oficial del fabricante, la disponibilidad de la integración para cada una de las siguientes categorías de solución:
8.2	1. Next Generation Firewall de la Entidad
8.3	2. Control de Acceso a la Red.

8.4	3. Análisis dinámico de archivos en entorno aislado SandBoxing.
8.5	4. Plataformas de engaño (deception) o honeypots
8.6	5. Correlacionador de Eventos, SIEM.
8.7	6. Plataforma de Orquestación, automatización y respuesta a incidentes, SOAR.
8.8	7. Plataforma de Análisis de comportamiento de usuario UEBA
8.9	8. Plataforma de Manejo de Identidades, IAM
8.10	Debe contar con la funcionalidad de INVESTIGACIÓN IMPULSADA POR INTELIGENCIA ARTIFICIAL
8.11	Debe contar con la funcionalidad de RESPUESTA AUTOMATIZADA
9	**COMPONENTES DE LA SOLUCIÓN DE EDR**
9.1	La plataforma de seguridad del endpoint EDR debe ser una arquitectura distribuida, la cual debe constar de una agente en software el cual debe ser compatible con los siguientes sistemas operativos y entornos, en versiones de 32 y 64 bits:
9.2	Windows: XP SP2/SP3, 7, 8, 8.1 y 10.
9.3	Windows Server: 2003 R2 SP2, 2008 R2 SP2, 2012, 2012 R2, 2016 y 2019.
9.4	MacOS: Yosemite (10.10), El Captain (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) y Catalina (10.15).
9.5	Linux: Redhat Enterprise Linux and CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 and 7.7, y Ubuntu LTS 16.04.5, 16.04.6, 18.04.2 server, en 64-bit.
9.6	Entornos VDI: VMware Horizons 6 y 7, y Citrix Desktop 7.
9.7	En cuanto al hardware, se debe ser un agente muy ligero; el cual no debe requerir más de 100MB de memoria RAM, y 20MB de espacio en disco.
9.8	Adicional la solución debe permitir ser desplegada de cualquiera de las siguientes maneras:
9.9	Nube: En la Nube del Fabricante.
9.10	On-Premise: En el Datacenter de la entidad.
9.11	Hibrida: En Nube y On-premise.
9.12	AirGapped o Sistemas Cerrados.
9.13	El producto debe incluir servicios de mejores prácticas implementadas por personal de servicios de Fabrica o un partner de servicios autorizado por Fabrica
10	**Servicios Profesionales**
10.1	La solución debe ofrecer transferencia de conocimiento en la fase de implementación sin cargo adicional.
10.2	El servicio de atención al cliente deberá estar disponible las 24 horas del día, los 7 días de la semana por correo electrónico, chat y teléfono.
10.3	El soporte del servicio debe entregarse por 12 meses

2. PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS		
La Entidad solicita una solución que provea la seguridad del sitio de trabajo a través de protección del correo electrónico, plataformas de colaboración, que incluya protección contra phishing, ransomware, ataques de día cero y apropiaciones de cuentas en una sola consola.		
Cantidad		2300
Vigencia		12 Meses
Medida		Unidad
#	**Categoría**	**Requerimiento Técnico Mínimo (de obligatorio cumplimiento)**
1	**Protección de correo electrónico.**	
1.1	**Escaneo de correo electrónico**	La solución debe analizar dinámicamente el 100% de los correos electrónicos
1.2		La solución debe analizar todas las URL y archivos adjuntos de los correos electrónicos entrantes
1.3		La solución debe escanear dinámicamente los correos electrónicos a una velocidad media de 15 segundos

1.4		El administrador de la solución debe estar en capacidad de acceder automáticamente a los detalles del análisis para ver las razones exactas por las que se marca un correo electrónico como malicioso
1.5		La solución debe proteger activamente contra el spam
1.6		La solución debe identificar amenazas después de la entrega de correo. Debe estar en capacidad de notificar a los usuarios y recuperar correos electrónicos maliciosos de sus bandejas de entrada para ponerlos en cuarentena automáticamente
1.7	**Identificación de amenazas**	La solución debe utilizar fuentes de inteligencia sobre amenazas para identificar amenazas conocidas
1.8		La solución debe utilizar capacidades internas de búsqueda de amenazas asistidas por humanos
1.9		La solución debe escanear los correos electrónicos de forma estática utilizando motores Antivirus
1.10		La solución debe utilizar herramientas para identificar firmas muy complejas
1.11	**Amenazas avanzadas**	La solución debe proteger contra los ataques de phishing a través del reconocimiento de imágenes, el análisis de texto y los evaluadores de reputación
1.12		La solución debe proteger contra los ataques BEC cuando se realizan comprobaciones SPF, DKIM y DMARC
1.13		La solución debe proteger contra los ataques de suplantación de identidad mediante el uso de técnicas para descubrir la suplantación de nombres de visualización y la suplantación de VIP
1.14		La solución debe proteger contra ataques de día cero y día N al inspeccionar datos a nivel de CPU
1.15		La solución debe detectar ATO mediante la observación de anomalías en el comportamiento del usuario
1.16	**Manejo de URL**	La solución debe hacer clic y escanear activamente las direcciones URL para identificar enlaces maliciosos antes de que lleguen al buzón del usuario final
1.17	**Sandbox**	La solución contar con la tecnología Sandbox para identificar archivos maliciosos
1.18		La solución debe utilizar datos de nivel de CPU para inspeccionar el flujo de ejecución de archivos
1.19		La solución debe mantener la integridad de los archivos durante los análisis, evitando alterar la estructura de los archivos
1.20		La solución debe identificar vulnerabilidades de daño en la memoria
1.21		La solución debe detectar errores lógicos y macros dentro de los documentos
1.22	**Gestión de archivos**	La solución debe escanear cientos de tipos de archivos diferentes
1.23		La solución debe descomprimir el contenido de forma recursiva, buscando enlaces y archivos incrustados para escanear
1.24		La tecnología de la solución para escanear enlaces y archivos incrustados debe tener al menos 7 capas de profundidad
1.25		La solución debe analizar contenido protegido con contraseña al entregarse el password
1.26		La solución debe analizar archivos comprimidos/comprimidos
1.27	**Situación del mercado**	La solución debe estar en la Guía de mercado de Gartner para la seguridad del correo electrónico
1.28		La solución debe estar catalogada en los tres primeros lugares en la evaluación de SE Labs.
2	**Protección de herramientas de colaboración**	
2.1	**Protección de Herramientas de colaboración**	La solución debe ser compatible con Slack, Microsoft 365 (Teams, One Drive, SharePoint), Google Drive, Box, Salesforce, Dropbox, Zendesk, AWS S3 Buckets y otras aplicaciones usando APIs.

2.2		La solución debe detectar y bloquear archivos maliciosos, URLs, y ataques avanzados en las soluciones protegidas
2.3		La solución debe tener la capacidad de integrarse a un servicio de Incident&Response (IR) para evaluar casos particulares o solicitados por el usuario final.
2.4		Debe escanear el 100% de los datos
2.5		La solución debe evaluar los correos y URLs que se envíen por las plataformas evaluadas
2.6		El servicio debe tener un Objetivo de nivel de servicio de mínimo 99.98%
2.7		Debe proveer servicios de Análisis de amenazas, Análisis dinámico y estático de archivos, protección de toma de cuenta (mínimo MS365)
3	**Uso**	
3.1	**Duración**	La solución debe ser nativa de la nube y está totalmente alojada en la nube
3.2		La solución debe actualizarse automáticamente
3.3		La solución debe satisfacer las necesidades de escalamiento de licenciamiento de un cliente sin afectar la experiencia del usuario ni requerir la compra de equipos adicionales
3.4	**Instalación**	La solución debe permitir la implementación en modo de prevención de amenazas, evitando las amenazas antes de que lleguen a los usuarios finales
3.5		La solución debe permitir ser implementada en modo CCO/Journaling, así como en línea para una protección completa en M365 como mínimo
3.6		La solución debe permitir la implementación para los usuarios a través de una invitación por correo electrónico
3.7		La solución debe ser implementada automáticamente con la integración de Office 365
3.8	**Integración**	La solución debe tener la posibilidad de conectarse a través de API a otras aplicaciones
3.9		La solución debe integrarse con Office 365 a través de API sin necesidad de cambiar el registro MX
3.10		La solución debe poderse ajustar a las políticas e integrarse a un SIEM, y no requiere cambios en la infraestructura e integración vía REST APIs
3.11		La solución debe estar en capacidad de exportar registros en tiempo real a un SIEM
3.12		La solución debe estar en capacidad de integrarse con gestores de Identidades a través de SAML
3.13		Los usuarios se deben asignan automáticamente permisos a roles y grupos en función de un esquema RBAC
3.14		La solución debe estar en capacidad mediante licencias adicionales de proteger el uso del cliente del almacenamiento compartido, las herramientas de colaboración y el navegador
3.15	**Gestión de datos**	La solución debe cifrar los datos en reposo con AES-256 y en tránsito con TLS 1.2+
3.16		Las claves de cifrado deben estar protegidas con soluciones como AWS KMS
3.17		La solución debe cumplir con: SOC2, GDPR, HIPAA, ISO 27001
3.18		La solución debe estar alojada en servidores separados ubicados en Europa, EE. UU. y APAC para garantizar resiliencia del servicio
3.19	**Gestión**	La solución debe proporcionar un panel de administración informativo que muestre datos de incidentes, informes y políticas
3.20		la solución debe tener la opción de incluir en las listas negras o blancas en función de la IP, las URL, los dominios, los remitentes, los tipos de archivos, etc.

3.21		La solución debe registrar las acciones del usuario, como los intentos de inicio de sesión, los cambios en el veredicto, la publicación de correos electrónicos y las solicitudes de investigación
3.22		El cliente debe estar en capacidad de personalizar los banners y las alertas de advertencia y traducirlos a otros idiomas como español, inglés y portugués
3.23		La solución debe tener una forma que el usuario reporte un presunto falso positivo o falso negativo para que la solución la revise y de su veredicto
3.24		La solución debe enviar informes y resúmenes de acciones a los usuarios
4	**Servicio**	
4.1	**Soporte al cliente**	La solución debe ofrecer transferencia de conocimiento en la fase de implementación sin cargo adicional.
4.2		El servicio de atención al cliente deberá estar disponible las 24 horas del día, los 7 días de la semana por correo electrónico, chat y teléfono.
4.4	**Duración**	El soporte del servicio debe entregarse por 12 meses.

3. WAF (WEB APPLICATION FIREWALL)		
La entidad requiere una solución unificada para proteger aplicaciones web (**10 sitios máximo**) y debe permitir APIs, optimizar el rendimiento y simplificar la gestión en entornos híbridos y multi-nube, que cumpla con los siguientes requerimientos		
Cantidad		1
Vigencia		12 Meses
Medida		Unidad
#	**Categoría**	**Requerimiento Técnico Mínimo (de obligatorio cumplimiento)**
1	**CARACTERÍSTICA/FUNCIONALIDAD**	
1.1	**Seguridad de Aplicaciones Web y API (WAF y API Security):**	Protección contra ataques de día cero mediante aprendizaje automático dual.
1.2		Eliminación de falsos positivos analizando y filtrando tráfico antes de llegar a las aplicaciones.
1.3		Protección contra los riesgos principales de OWASP Top 10.
1.4		Actualizaciones automáticas con inteligencia de amenazas en tiempo real.
1.5		Configuración simplificada a través de una interfaz intuitiva.
1.6		Protección basada en firmas.
1.7		Inteligencia de amenazas IP.
1.8		Inteligencia GEO-IP.
1.9		Reglas de seguridad personalizadas.
1.10		Cumplimiento de HTTP.
1.11		Protección de URL, parámetros y CORS.
1.12		Protección de cookies.
1.13		Prevención de fugas de información.
1.14		Antivirus para cargas de archivos.
1.15		Sandbox para cargas de archivos.
1.16		Protección contra ataques de día cero basada en aprendizaje automático.
1.17		Cumplimiento de esquemas (Open API, XML, JSON).
1.18		API Gateway.
1.19		Protección de API móviles.
1.20		Descubrimiento, catálogo de PII y protección basada en aprendizaje automático.
1.21		Protección de encabezados HTTP.
1.22		Protección contra CSRF y ataques Man-in-the-Browser (MiTB).
1.23		Detección basada en comportamiento mediante análisis biométrico y de comportamiento.

1.24	**Protección Avanzada contra Bots:**	Perfilado avanzado de dispositivos para bloquear ataques de bots.
1.25		Identificación y bloqueo de rastreadores web no deseados y amenazas automatizadas.
1.26		Análisis en tiempo real e histórico del tráfico y actividades de bots.
1.27		Protección avanzada contra bots (detección biométrica, firma y engaño).
1.28	**Balanceo de Carga Global de Servidores:**	Balanceo de carga basado en DNS para distribuir tráfico entre múltiples centros de datos.
1.29		Distribución geográfica del tráfico según métricas de salud y ubicación.
1.30		Integración sencilla con la plataforma de Protección Web.
1.31		Alta disponibilidad incluso durante interrupciones regionales.
1.32		Capacidad para realizar chequeos de salud (health checks) sobre servicios y aplicaciones, permitiendo identificar el estado operativo de sus componentes, detectar de manera anticipada posibles fallas o indisponibilidades y generar acciones de respuesta proactiva.
1.33	**Análisis de Amenazas:**	Identificación de patrones de ataque ocultos mediante correlación de eventos basada en IA.
1.34		Visibilidad en tiempo real de eventos de seguridad en toda la infraestructura.
1.35		Respuesta proactiva a incidentes con inteligencia de amenazas y flujos de trabajo automatizados.
1.36		Reducción de la fatiga de alertas consolidando múltiples alertas en incidentes significativos.
1.37	**Automatización**	Automatización de tareas de seguridad como actualizaciones de políticas y correcciones de configuración.
1.38		Priorización de amenazas de alto riesgo y caza adaptativa de amenazas.
1.39		Enriquecimiento de inteligencia de amenazas para mejorar la defensa proactiva.
1.40	**Protección contra Toma de Cuentas:**	Seguimiento de usuarios.
1.41		Protección contra fijación de sesiones.
1.42		Defensa contra relleno de credenciales.
1.43	**Protección contra DDoS:**	Mitigación de DDoS en capas 3-4.
1.44		Mitigación de DDoS en capa 7.
1.45	**Entrega de Aplicaciones:**	Certificados SSL automáticos y personalizados.
1.46		Autenticación de clientes/Mutual TLS.
1.47		Red de entrega de contenido (CDN).
1.48		CDN GEO limitado.
1.49		Balanceo de carga y monitoreo de salud de servidores.
1.50		Enrutamiento de contenido del servidor de origen.
1.51		Sala de espera.
1.52	**Escaneo DAST:**	Evaluación de vulnerabilidades.
1.53		Escaneo de API.
1.54	**Reportes y Análisis:**	Registros de ataques.
1.55		Notificaciones de alertas.
1.56		Integración con SIEM.
1.57		Enmascaramiento de datos sensibles en registros.
1.58		Análisis de registros en tiempo real e históricos.
1.59		Dashboards e informes.
1.60		Registros de tráfico.
1.61		Análisis de amenazas con IA.
1.62	**Gestión:**	Control de acceso basado en roles.
1.63		Soporte para inicio de sesión único (SSO).
1.64		Soporte API.

1.65	**Servicios:**	La solución debe ofrecer transferencia de conocimiento en la fase de implementación sin cargo adicional.
1.66		El servicio de atención al cliente deberá estar disponible las 24 horas del día, los 7 días de la semana por correo electrónico, chat y teléfono.
1.67		El servicio soporte debe entregarse por 12 meses

4. **IMPLEMENTACIÓN Y SOPORTE TÉCNICO**	
4.1	• La Entidad requiere Soporte Técnico durante 12 meses de la Plataforma de Ciberseguridad, la cual deberá contar como mínimo con las siguientes características: o Actualizaciones y mantenimiento de producto o Compatibilidad con nuevos sistemas operativos, acceso a versiones nuevas sin costo adicional dentro de la vigencia. o Deberá incluir atención remota telefónica 24/7, asistencia para configuración y despliegue, guías técnicas, manuales y base de conocimientos y SLA (acuerdo de nivel de servicio). o Deberá contar con medios de escalamiento que deberá corresponder como mínimo a una Plataforma helpdesk con usuario y contraseña. o Transferencia de Conocimiento: La actividad de transferencia de conocimiento inicial sobre uso del producto deberá ser como mínimo de 20 horas que será prestado a mínimo tres Contratista que forman parte del Equipo Técnico del INDER. La capacitación o actividad de transferencia del conocimiento deberá contar dentro de sus temáticas con las siguientes: a) laboratorios de aprendizaje de uso de la solución para administradores o equipos técnicos, documentación de mejores prácticas; b) Interfaz de administración. o Recuperación, restablecimiento o migración sin costo adicional, en caso de que aplique.
4.2	• Realizar todas las actividades necesarias para la configuración, instalación, puesta en funcionamiento y verificación del sistema de ciberseguridad, incluyendo las respectivas pruebas de funcionamiento y la entrega del informe de instalación con el protocolo y resultados de pruebas realizadas. Lo anterior deberá ser recibido a satisfacción por parte del supervisor y del apoyo técnico.

- Todas las actividades, comunicaciones y documentos relacionados con el proceso de contratación y la ejecución del contrato deberán realizarse y presentarse en idioma castellano.
- Todos los componentes deber ser del mismo fabricante.
- La vigencia de la solución de seguridad debe iniciar a partir de la entrega a satisfacción y estar activa por 12 meses.
- Las licencias de la plataforma de seguridad deben ser en la última versión publicada por el fabricante y deben quedar a nombre del INDER Medellín.
- La plataforma de seguridad debe contar con acceso a actualizaciones periódicas para la protección contra nuevas amenazas.
- La garantía comercial del fabricante: El licenciamiento de los productos tendrá una vigencia de doce (12) meses, durante los cuales deberá mantenerse vigente el soporte del fabricante. El fabricante deberá garantizar la disponibilidad de soporte

técnico 24x7, permitiendo la apertura y atención de casos de soporte durante todo el periodo de vigencia del licenciamiento

ACTIVIDADES A EJECUTAR POR EL CONTRATISTA:

Estas actividades son transversales durante la vigencia del contrato y de las licencias.

Prestación de servicios profesionales especializados para la implementación, configuración, puesta en operación, transferencia de conocimiento y soporte técnico de las soluciones de ciberseguridad adquiridas, durante la vigencia del contrato y de las licencias de la siguiente forma**:**

1. Una vez suscrita el Acta de Inicio por las partes, el Contratista deberá realizar un análisis del nivel de seguridad actual del INDER Medellín y presentar los resultados de dicho examen al Instituto, el cual deberá ser entregado mediante un informe por escrito a más tardar 15 días calendario contados a partir de la suscripción del Acta de Inicio.
2. Con anterioridad al 15 de noviembre de 2026, el Contratista deberá proceder con la Instalación, configuración y puesta en marcha de las soluciones definidas (EDR, PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS Y WAF) en el presente alcance:
    a. Despliegue del 40% de los 1020 agentes en los EndPoint.
    b. Despliegue de agentes en 5 de los 20 para servidores.
    c. Despliegue de la solución WAF con la configuración de las políticas de protección para 10 sitios Web.
    d. Despliegue y configuración de la protección para 2300 buzones de correo y herramientas colaborativas.
    e. Configuración de la interfaz de administración e integración de los servicios.

3. Con anterioridad al 15 de noviembre de 2026, deberá alinear la solución de seguridad según las políticas de ciberseguridad del INDER Medellín.
4. Transferencia de conocimiento a 3 integrantes del personal técnico del INDER Medellín sobre la administración del **SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR, PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF**.
5. Envió de Campañas de entrenamiento para usuarios finales en la identificación de situaciones de riesgo, “Boletines de sensibilización de Ciberseguridad” a través de correo electrónico, a los usuarios del instituto (gestionado y coordinado entre el oferente y la coordinación de TI.).

6. Capacitación virtual (dos al año), sobre concienciación en ciberseguridad para usuarios finales durante la vigencia de las licencias, entregar evidencia documentada que incluya el contenido o protocolo de la actividad una vez sea realizada.
7. Durante la vigencia de las licencias y a solicitud del apoyo técnico del instituto, realizar una evaluación de ciberseguridad basado en algún framework cómo: NIST, ISO 27001 o CIS Controls. Entregar evidencia documentada que incluya alcance, criterios de severidad, protocolo y demás contenido de la actividad una vez sea realizada.

OBLIGACIONES DEL CONTRATISTA.

GENERALES:

1. Realizar las actividades necesarias para el cumplimiento del objeto del contrato a entera satisfacción, así como las demás actividades que relacionadas con el objeto del mismo sean necesarias para lograr los fines buscados.
2. Cumplir con las especificaciones técnicas solicitadas para el desarrollo del contrato.
3. Velar por el cumplimiento del plazo establecido para la ejecución del objeto contractual.
4. Atender las consultas que la Contratante o el Supervisor hagan sobre los servicios prestados.
5. Participar en la elaboración de la liquidación respectiva en el término que se ha establecido, cuando aplique.
6. Mantener vigentes las garantías otorgadas, en caso de que procedan.
7. Cumplir con todas las obligaciones laborales, de Seguridad Social, ARL y el pago de las obligaciones Parafiscales vigentes de los empleados y/o contratistas que utilice en el desarrollo del objeto contractual, y con las obligaciones del Sistema de Gestión de Seguridad y Salud en el Trabajo de conformidad con lo señalado en el Decreto 1072 del 2015.
8. Respetar los buenos usos sociales, la cultura ciudadana y las buenas costumbres en la ejecución contractual.
9. Dar aplicación a los principios de seguridad, confidencialidad, disponibilidad, acceso y circulación restringida respecto de la información y datos a que tenga acceso con ocasión del desarrollo del objeto contractual.

OBLIGACIONES ESPECÍFICAS

1. Dentro de los primeros 3 días hábiles posteriores a la fecha de inicio del contrato, el contratista deberá asistir a una reunión presencial o virtual para socializar requisitos exigidos por INDER Medellín, obligaciones establecidas por INDER Medellín y dudas del contratista.
2. Cumplir con los requisitos técnicos y actividades descritas en el anexo técnico y ESPECIFICACIONES TÉCNICAS del Estudio Previo. Entregable: Informe técnico de entrega final, el cual debe contener cada ítem indicar actividad realizada o licencia entregada.
3. Mediante carta firmada por el Representante Legal, Informar detalladamente el alcance de la garantía del fabricante y soporte técnico adquirido para los servicios contratados, la cual debe coincidir con las características mencionadas en las especificaciones técnicas.
   Entregable: Carta firmada por el representante legal.
4. El contrista deberá brindar el soporte técnico, de conformidad con las condiciones y alcance establecidos en la carta de garantía, cuando sea requerido por la supervisión durante la vigencia de la plataforma adquirida.
5. El contratista deberá presentar un informe cuantitativo del desempeño de toda la solución de seguridad con periodicidad mensual durante la vigencia de la plataforma adquirida.
   Entregable: Carta firmada por el representante legal con este compromiso.
6. El contratista deberá entregar de forma digital, la evidencia de las licencias(s) de la plataforma a nombre del INDER Medellín.
7. Deberá contar con un sistema de escalamiento de solicitudes, medios de contacto y SLA. Entregable: Incluir esta información en el informe técnico de entrega final.
8. El contratista deberá desarrollar cronogramas, planes de trabajo e implementación, procedimientos y contenidos que sean necesarios para la correcta ejecución de todas las actividades que conlleve el proyecto.
9. Durante la vigencia de las licencias, realizar dos (2) pruebas de penetración, en las fechas que sean determinadas y solicitadas por el apoyo técnico designado por la Entidad, quien comunicará oportunamente al contratista los momentos en los cuales deberán ejecutarse dichas pruebas, una vez realizada cada prueba deberá entregar el informe al instituto con todo el protocolo realizado.

1.2.*DOCUMENTOS DEL PROCESO*

Los Documentos del Proceso son los señalados tanto en el capítulo IX. Así mismo, los estudios y documentos previos del presente y el anexo de glosario aplicable en el sector que corresponde, y los enunciados en el artículo 2.2.1.1.1.3.1 del Decreto 1082 de 2015.

1.3. *COMUNICACIONES Y OBSERVACIONES AL PROCESO*

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

Las respuestas se comunicarán a través de la plataforma del SECOP II de acuerdo con el Manual de Uso y Condiciones de la plataforma.Cuando el Proponente registre el certificado de indisponibilidad de la plataforma, la Entidad pondrá a disposición el siguiente correo: santiago.restrepov@inder.gov.co

1.4. *CLASIFICADOR DE BIENES Y SERVICIOS DE NACIONES UNIDAS (UNSPSC)*

El bien o servicio objeto del Proceso de Contratación está codificada en el Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC), como se indica en la siguiente tabla:

Tipo	Código	Nombre Producto
Clase	43233200	Software de seguridad y protección
Clase	43222500	Equipo de seguridad de red
Clase	81111800	Servicios de sistemas y administración de componentes de sistemas
Clase	81112200	Mantenimiento y soporte de software

1.5. *RECURSOS QUE RESPALDAN LA CONTRATACIÓN*

Para respaldar el compromiso derivado del Proceso de Contratación, se cuenta con el siguiente Certificado de Disponibilidad Presupuestal:

DISPONIBILIDAD	FECHA CDP	VALOR DISP	POSICIÓN DOCUMENTO	DESCRIPCION POSICIÓN PRESUPUESTAL	CENTRO GESTOR	FONDO
1160015664	22.05.2026	800.589.423 COP	001	2320201004	905924008103	911070126
1160015679	02.06.2026	32.272.427 COP	001	2320201004	905924008103	911070126

AREA FUNCIONAL	PROYECTO	NOMBRE RUBRO PRESUPUESTAL	MONTO RECUERSOS (APRO.INICIAL)	TIPO DE GASTO	ORIGEN DEL PRESUPUESTO

45991000.0254.99	9240081	Fortalecimiento de infraestructura tecnológica	$ 3.273.495.941	Inversión	R.Ordinarios Mpio
45991000.0254.99	9240081	Fortalecimiento de infraestructura tecnológica	$ 3.273.495.941	Inversión	R.Ordinarios Mpio

La necesidad se encuentra incluida en el Plan Anual de Adquisiciones de la Entidad.

2. CAPÍTULO II. REQUISITOS HABILITANTES Y SU VERIFICACIÓN

EXPERIENCIA DEL PROPONENTE:

Todos los documentos deben ser presentados de forma individual (no unificar todo en un solo pdf).

Se tendrá como experiencia general mínima habilitante del proponente la acreditación de máximo dos (2) certificados de contratos ejecutados, terminados y liquidados por el proponente, que el valor sumado de los contratos y expresado en salarios mínimos mensuales legales vigentes (SMMLV) sea igual o superior al presupuesto oficial expresado en (SMMLV), es decir, igual o superior a 472

Los contratos deben encontrarse en el RUP del Proponente y debe relacionarlos en el Formato 3 (Experiencia del Proponente). El Proponente deberá presentar ambos documentos (RUP y Formato 3) para participar del Proceso.

Cada contrato acreditado debe estar identificado al menos en tres (03) de los códigos del clasificador de bienes y servicios de Naciones Unidas a nivel de clase señalados en el siguiente cuadro:

CLASIFICACIÓN	SEGMENTO	FAMILIA	CLASE
43233200	Tecnología de la Información, Radiodifusión y Telecomunicaciones	Software	Software de seguridad y protección
43222500	Tecnología de la Información, Radiodifusión y Telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipo de seguridad de red

81111800	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas
81112200	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Mantenimiento y soporte de software

Para la certificación se admite, acta de liquidación o recibido a satisfacción y deberán cumplir con los siguientes requisitos:

a. Fecha de expedición
b. Razón social del contratante
c. Razón del social del contratista con Nit
d. Teléfonos del contratante (si es empresa privada)
e. Valor final del contrato, expresado en pesos colombianos o SMMLV
f. Fecha de inicio y terminación del contrato.
i. Objeto del contrato, este debe tener relación con el suministro e implementación de soluciones, tecnologías o servicios especializados de ciberseguridad, destinados a fortalecer la protección y seguridad de infraestructuras tecnológicas.

El proponente deberá aportar un certificado expedido por el o los fabricante(s) de la solución, dirigido a la Entidad donde se especifique que cuenta con un nivel de partner o canal en la categoría más alta dentro del programa de canales del fabricante y su fecha de expedición no podrá ser superior a treinta (30) días calendario contados a partir del cierre del proceso de selección.

La o las certificación(es) deberá(n) demostrar que el o (los) oferente(s) cuenta(n) con mínimo una (1) especialidad del o los fabricante(s) consultable en el sitio web del o los fabricante (s).

La Entidad se reserva el derecho de verificar las certificaciones aportadas o de solicitar los respectivos documentos que soporten la certificación.

PERSONAL PROFESIONAL REQUERIDO

Esta documentación será evaluada en la etapa de requisitos habilitantes.

El personal profesional requerido debe estar vinculado con la empresa interesada en el proceso y demostrar su vinculación de mínimo los últimos 3 meses.

El contratista debe contar con un equipo mínimo de trabajo de 4 integrantes para la ejecución del proyecto, el cual debe estar conformado de la siguiente manera:

ROL	DESCRIPCIÓN
Un (1) Gerente de Proyecto.	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática **Experiencia general:** Debe contar con mínimo diez (10) años de experiencia general, contados a partir de la expedición de la matrícula profesional. **Título de Posgrado en:** Especialización o Maestría en áreas relacionadas con su carrera profesional Debe acreditar mediante una certificación, que tiene fundamentos en ciberseguridad, esta debe ser emitida por el fabricante. Debe acreditar mediante una certificación vigente, conocimientos a nivel profesional en gestión de proyectos. **Experiencia específica:** Especifica mínima de ocho (8) años gerenciando y/o coordinando proyectos en temas relacionados con seguridad de la información y/o seguridad informática.

Un (1) Ingeniero de Soporte	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática **Experiencia general:** mínimo tres (3) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. **Título de Posgrado:** Especialización o maestría en seguridad informática o ciberseguridad Debe estar Certificado como profesional en seguridad de redes por el fabricante y debe estar vigente Debe acreditar mediante una certificación que cuenta con conocimientos para brindar soluciones de seguridad de redes y debe estar vigente y debe ser emitida por el fabricante. Experiencia específica: Mínimo Dos (2) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad.
Un (1) Especialista en Ciberseguridad:	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática **Experiencia general:** Mínimo cinco (5) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. **Título de Posgrado:** Especialización o maestría en seguridad informática o ciberseguridad Debe acreditar mediante una certificación que cuenta con conocimientos para brindar soluciones de seguridad de

	redes, debe estar vigente y debe ser emitida por el fabricante. Debe contar con certificación de EH-Ethical Hacker vigente. **Experiencia específica:** Mínimo Dos (2) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad.
Un (1) Ingeniero de apoyo a la implementación WAF	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática. **Experiencia general:** Mínimo tres (3) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. Debe contar con certificación como Profesional de seguridad en nube emitida por el fabricante. **Experiencia específica:** Mínimo un (1) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad

Documentación para entregar

- Cedula de ciudadanía
- Hoja de vida del profesional
- Diploma de título Profesional
- Tarjeta Profesional con Certificación de vigencia
- Certificaciones que acrediten experiencia especifica
- Certificaciones acreditadas de especialista o maestría en las áreas solicitadas, según aplique.
- Certificaciones técnicas solicitadas en cada uno de los perfiles
- Planilla de seguridad social u otro documento que acredite la vinculación con la empresa interesada en el proceso.

Teniendo en cuenta que el personal propuesto es objeto de verificación dentro de los requisitos habilitantes, las hojas de vida y el personal acreditado por el proponente durante el proceso de selección no podrán ser sustituidos. En consecuencia, en caso de resultar adjudicado, el contratista deberá garantizar que el personal presentado y aprobado durante la etapa de selección sea el mismo que ejecute el proyecto.

La Entidad verificará los requisitos habilitantes dentro del término señalado en el Cronograma del Pliego de Condiciones, de acuerdo con los soportes documentales.

Los requisitos habilitantes serán objeto de verificación. Por lo tanto, si la propuesta cumple con todos los aspectos se evaluarán como *"cumple"*. En caso contrario, se evaluará como *"no cumple"*.

De conformidad con la normativa aplicable, la Entidad realizará la verificación de requisitos habilitantes de los Proponentes (personas naturales o jurídicas nacionales o extranjeras domiciliadas o con sucursal en Colombia, Consorcios o Uniones Temporales) con base en la información contenida en el RUP y los documentos señalados en los Pliegos de Condiciones.

2.1. *GENERALIDADES*

A. Únicamente se consideran habilitados aquellos Proponentes que cumplan todos los requisitos habilitantes, según lo señalado en el Pliego de Condiciones.

B. En el caso de Proponentes Plurales, los requisitos habilitantes serán acreditados por cada uno de los integrantes de la figura asociativa, salvo que se entienda algo distinto y, en todo caso, se realizará de acuerdo con las reglas del Pliego de Condiciones.

C. Todos los proponentes deben diligenciar el Formato 3 – Experiencia y los Proponentes extranjeros sin domicilio o sin sucursal en Colombia deben diligenciar adicionalmente el Formato 4 – Capacidad financiera y organizacional para extranjeros y adjuntar los soportes que ahí se definen.

D. Los Proponentes obligados a estar inscritos en el Registro Único de Proponentes (RUP), deben aportar el certificado con fecha de expedición no mayor a treinta (30) días calendario anteriores a la fecha de cierre del Proceso de Contratación. En caso de modificarse la fecha de cierre del proceso, se tendrá como referencia para

establecer el plazo de vigencia del certificado la originalmente indicada en el Pliego de Condiciones.

2.2. *CAPACIDAD JURÍDICA*

Los interesados podrán participar como Proponentes bajo alguna de las siguientes modalidades siempre y cuando cumplan los requisitos exigidos en el Pliego de Condiciones:

A. Individualmente como: a) persona natural nacional o extranjera, b) persona jurídica nacional o extranjera.
B. Conjuntamente, como Proponentes Plurales en cualquiera de las formas de asociación previstas en el artículo 7 de la Ley 80 de 1993.

Los Proponentes deben:

A. Tener capacidad jurídica para la presentación de la oferta.
B. Tener capacidad jurídica para la celebración y ejecución del Contrato.
C. No estar incursos en ninguna de las circunstancias de inhabilidad, incompatibilidad, conflicto de interés o prohibición para contratar previstas en la Constitución y en la ley, incluyendo la causal establecida en el numeral 1.14 del Pliego de Condiciones.
D. No estar reportados en el último boletín de responsables fiscales vigentes publicado por la Contraloría General de la República. Esta disposición aplica para el Proponente e integrantes de un Proponente Plural con domicilio en Colombia. Tratándose de Proponentes Extranjeros sin domicilio o sin sucursal en Colombia, deben declarar que no son responsables fiscales por actividades ejercidas en Colombia en el pasado y que no tienen sanciones vigentes en Colombia que impliquen inhabilidad para contratar con el Estado.

La Entidad debe consultar los antecedentes judiciales en línea en los registros de las bases de datos, al igual que los antecedentes fiscales acorde con el artículo 60 de la Ley 610 de 2000, los antecedentes disciplinarios conforme con el artículo 1 de la Ley 1238 de 2008 y el Registro Nacional de Medidas Correctivas del Ministerio de Defensa Nacional – Policía Nacional, de acuerdo con lo dispuesto en el artículo 184 de la Ley 1801 de 2016 – Código Nacional de Seguridad y Convivencia Ciudadana–.

2.2.1 CARTA DE PRESENTACIÓN DE LA OFERTA

El Proponente presentará el Formato 1 – Carta de Presentación de la Oferta, el cual debe estar firmado por la persona natural o por el representante legal del Proponente individual o Plural, o por el apoderado.

La carta de presentación debe suscribirse. Con la firma de este documento se entiende que el proponente conoce y acepta las obligaciones del Anexo 3 – Pacto de Transparencia y, por lo tanto, no será necesaria la entrega de este documento al momento de presentar la oferta.

El Proponente debe diligenciar los Formatos. Todos los espacios en blanco deben diligenciarse con la información solicitada.

2.2.2EXISTENCIA Y REPRESENTACIÓN LEGAL

La existencia y representación legal de los Proponentes individuales o integrantes de los Proponentes Plurales se acreditará de acuerdo con las siguientes reglas:

2.2.2.1 PERSONAS NATURALES

Deben presentar los siguientes documentos en copia simple:

A. Persona natural de nacionalidad colombiana: cédula de ciudadanía.

B. Persona natural extranjera con residencia en Colombia: cédula de extranjería vigente.

C. Persona natural extranjera sin domicilio en Colombia: pasaporte.

2.2.2.2 PERSONAS JURÍDICAS

Deben presentar los siguientes documentos:

A. Persona jurídica nacional o extranjera con sucursal en Colombia:

I. Certificado de existencia y representación legal expedido por la Cámara de Comercio o autoridad competente, en el que se verificará:

a. Fecha de expedición del certificado no mayor a treinta (30) días calendario anteriores a la fecha de cierre del Proceso de Contratación. En caso de modificarse la fecha de cierre del proceso, se tendrá como referencia para establecer el plazo de vigencia del certificado de existencia y representación legal la originalmente fijada en el Pliego de Condiciones.

b. Que el objeto de la sociedad permita ejecutar las actividades descritas en el objeto del Proceso de Contratación.

c. Las personas jurídicas nacionales y extranjeras deberán acreditar que su duración no será inferior a la del plazo del contrato y un año más.

d. Si el representante legal de la sociedad tiene restricciones para contraer obligaciones en nombre de la misma, deberá acreditar su capacidad a través de una autorización suficiente otorgada por el órgano social competente respectivo para cada caso.

e. El nombramiento del revisor fiscal en caso de que deba contar con uno.

II. Certificación del revisor fiscal en caso de ser sociedad anónima colombiana, en la que conste si es abierta o cerrada.

III. Fotocopia del documento de identificación del representante legal.

En el caso de las sucursales de las personas jurídicas extranjeras y como quiera que la sucursal en Colombia no es una persona jurídica diferente a la matriz, se tendrá en cuenta la fecha de constitución de esta última.

Si la oferta es suscrita por una persona jurídica extranjera a través de la Sucursal debidamente constituida en Colombia, deberá acreditar la existencia de la Sucursal y la capacidad jurídica de su representante o apoderado, mediante la presentación del certificado del Registro Único de Proponentes (RUP) y el certificado de existencia y representación legal con fecha de expedición máximo de 30 días calendario antes de la fecha de cierre de este procedimiento de selección por la Cámara de Comercio. Cuando el representante legal de la Sucursal tenga restricciones para contraer obligaciones, deberá acreditar autorización suficiente del órgano social respectivo para contraer obligaciones en nombre de la sociedad. La ausencia definitiva de autorización suficiente o el no aporte de dicho documento una vez solicitado por la Entidad, determinará la falta de capacidad jurídica para presentar la oferta

B. Persona jurídica extranjera sin Sucursal o domicilio en Colombia: Documentos que acredite la existencia y representación legal de la sociedad extranjera, presentados de conformidad con lo establecido en el Pliego de Condiciones, en el que debe constar, como mínimo, los siguientes aspectos:

I. Nombre o razón social completa.

II. Nombre del representante legal o de la persona facultada para comprometer a la persona jurídica.

III. Que el objeto de la sociedad permita ejecutar las actividades descritas en el objeto del Proceso de Contratación.

IV. Facultades del representante legal o de la persona designada para comprometer a la persona jurídica, en la que se señale expresamente que el representante no tiene limitaciones para contraer obligaciones en nombre de la misma o aportando la autorización o documento correspondiente del órgano social competente para cada caso.

V. Tipo, número y fecha del documento de constitución o creación.

VI. Fecha y clase de documento por el cual se reconoce la personería jurídica.

VII. Acreditar que su duración no será inferior a la del plazo del contrato y un año más.

VIII. Fotocopia del documento de identificación del representante legal.

Si no existiera ninguna autoridad o entidad que certifique la totalidad de la información de existencia y representación legal, el Proponente o integrante extranjero del Proponente Plural deberá presentar una declaración juramentada de una persona con capacidad jurídica para vincular y representar a la sociedad en la que conste que: i) no existe autoridad u organismo que certifique lo solicitado en este numeral; ii) la información requerida en el presente literal, y iii) la capacidad jurídica para vincular y representar a la sociedad de la persona que efectúa la declaración, así como de las demás personas que puedan representar y vincular a la sociedad, si las hay.

C. Entidades Estatales: Deben presentar los siguientes documentos para acreditar su existencia:

Acto de creación de la Entidad Estatal. Este puede ser ley, decreto, ordenanza, acuerdo o certificado de existencia y representación legal (este último no mayor a treinta (30) días calendario anteriores a la fecha de cierre del proceso de selección) o documento equivalente que permita conocer la naturaleza jurídica, funciones, órganos de dirección o régimen jurídico de contratación de la Entidad Estatal.

NOTA: En el último evento indicado en el párrafo anterior, relacionado con las personas jurídicas no obligadas a aportar el certificado de existencia y representación legal, deberán

aportar un documento equivalente que acredite su existencia, junto con los documentos que demuestren la capacidad del representante legal de la Entidad o sociedad a contratar, en el cual se verificará:

- Fecha de expedición del documento equivalente que acredite su existencia que no sea mayor a treinta (30) días calendario anteriores a la fecha de cierre del Proceso de Contratación.
- Que el objeto incluya las actividades principales objeto del proceso.
- La duración deberá ser por lo menos igual al plazo estimado del contrato y un (1) año más.
- Para efectos del Pliego de Condiciones, el plazo de ejecución del Contrato será el indicado en el numeral “1.1 Objeto, presupuesto oficial, plazo y ubicación”.
- Si el representante legal tiene restricciones para contraer obligaciones en nombre de la misma, deberá acreditar autorización suficiente del órgano competente para contraer obligaciones en nombre de la sociedad o de la Entidad.
- La ausencia definitiva de autorización suficiente o el no aporte de dicho documento una vez solicitado por la Entidad, determinará la falta de capacidad jurídica para presentar la oferta, y por tanto su rechazo.
- El nombramiento del revisor fiscal en caso de que esté obligado a tenerlo.

2.2.2.3 PROPONENTES PLURALES

El documento de conformación de proponentes plurales debe:

A. Acreditar la existencia del Proponente Plural y clasificarlo en Unión Temporal o en Consorcio. En este documento los integrantes deben expresar su intención de conformar el Proponente Plural. En caso de que no exista precisión sobre el tipo de asociación se solicitará aclaración. Los Proponentes deben incluir como mínimo la información requerida en el Formato 2 – Conformación de Proponente Plural (Formato 2A – Consorcios) (Formato 2B – Uniones Temporales). Los Proponentes podrán incorporar información adicional que no contradiga lo dispuesto en los Documentos del Proceso de Contratación.

B. Acreditar el nombramiento de un representante y un suplente, este último en caso de considerarlo conveniente, cuya designación deberá quedar definida en el Formato 2 – Conformación de Proponente Plural (Formato 2A – Consorcios) (Formato 2B – Uniones Temporales), de las personas naturales y/o jurídicas asociadas. Estos tendrán facultades suficientes para la representación sin limitaciones de los integrantes, en todos los aspectos que se requieran para presentar la oferta, suscribir y ejecutar el contrato, así como la facultad para firmar el acta de terminación y liquidación.

C. Aportar copia del documento de identificación del representante principal y suplente del Proponente Plural, en caso de que se haya nombrado este último.

D. Acreditar que la vigencia del Proponente Plural no sea inferior a la del plazo del Contrato y un año adicional. Para efectos de la evaluación, este plazo será contado a partir de la fecha del cierre del Proceso de Contratación.

E. El Proponente Plural debe señalar expresamente cuál es el porcentaje de participación de cada uno de sus integrantes. La sumatoria de este porcentaje no podrá ser diferente al 100 %.

F. En la etapa contractual, no podrán ser modificados los porcentajes de participación sin el consentimiento previo de la Entidad. En todo caso, en la etapa precontractual no será posible modificar los porcentajes de los integrantes del Proponente Plural después de la fecha del cierre del Proceso de Contratación

Dicho documento debe estar firmado por todos los integrantes del Proponente Plural y en el caso del integrante persona jurídica, por el representante legal de dicha persona, o por el apoderado de cualquiera de los anteriores.

2.2.3 REGISTRO ÚNICO DE PROPONENTES (RUP)

Los Proponentes obligados a estar inscritos en el Registro Único de Proponentes (RUP), deben aportar el certificado con fecha de expedición no mayor a treinta (30) días calendario anteriores a la fecha de cierre del Proceso de Contratación. En caso de modificarse la fecha de cierre del proceso, se tendrá como referencia para establecer el plazo de vigencia del certificado la originalmente indicada en el Pliego de Condiciones.

2.2.4 CERTIFICACIÓN DE PAGOS DE SEGURIDAD SOCIAL Y APORTES LEGALES

2.2.4.1 PERSONAS JURÍDICAS

El Proponente persona jurídica debe presentar el Formato 6 – Pagos de seguridad social y aportes legales suscrito por el revisor fiscal, de acuerdo con los requerimientos de ley o por el representante legal, bajo la gravedad del juramento, cuando no se requiera revisor fiscal, en el que conste el pago de los aportes de sus empleados a los sistemas de salud, riesgos laborales, pensiones y aportes a las cajas de compensación familiar, al Instituto Colombiano de Bienestar Familiar, al Servicio Nacional de Aprendizaje.

La Entidad no exigirá las planillas de pago. Bastará el certificado suscrito por el revisor fiscal, en los casos requeridos por la ley, o por el representante legal que así lo acredite.
Cuando la persona jurídica está exonerada en los términos previstos en el artículo 65 de la Ley 1819 de 2016 debe indicarlo en el Formato 6 – Pagos de seguridad social y aportes legales.

Esta misma previsión aplica para las personas jurídicas extranjeras con domicilio o Sucursal en Colombia, las cuales deben acreditar este requisito respecto del personal vinculado en Colombia.

2.2.4.2 PERSONAS NATURALES

El Proponente persona natural debe acreditar la afiliación a los sistemas de seguridad social en salud y pensiones, aportando los certificados de afiliación respectivos o con el certificado de pago de la correspondiente planilla, pero no será obligatoria la presentación de este último.

Los certificados de afiliación deben presentarse con fecha de expedición no mayor a treinta (30) días calendario anteriores al cierre del Proceso de Contratación. En caso de modificarse la fecha de cierre del Proceso de Contratación, se tendrá como referencia para establecer el plazo de vigencia de los certificados de afiliación la originalmente contemplada en el Pliego de Condiciones.

La persona natural que reúna los requisitos para acceder a la pensión de vejez o se pensione por invalidez o anticipadamente, presentará el certificado que lo acredite y, además, la afiliación al sistema de salud.

Esta misma previsión aplica para las personas naturales extranjeras con domicilio en Colombia las cuales deberán acreditar este requisito respecto del personal vinculado en Colombia.

2.2.4.3 PROPONENTES PLURALES

Cada uno de los integrantes del Proponente Plural debe acreditar por separado los requisitos de que tratan los numerales anteriores.

2.2.4.4 SEGURIDAD SOCIAL PARA LA SUSCRIPCIÓN DEL CONTRATO

El adjudicatario debe presentar, para la suscripción del respectivo Contrato, ante la dependencia respectiva, la declaración donde acredite el pago correspondiente a seguridad social integral y aportes legales cuando a ello haya lugar.

En caso de que el adjudicatario, persona natural o jurídica, no tenga o haya tenido dentro de los seis (6) meses anteriores a la fecha de firma del Contrato personal a cargo y por ende no esté

obligado a efectuar el pago de aportes legales y seguridad social integral, debe indicar esta circunstancia en la mencionada certificación, bajo la gravedad de juramento.

2.2.4.5 ACREDITACIÓN DEL PAGO AL SISTEMA DE SEGURIDAD SOCIAL DURANTE LA EJECUCIÓN DEL CONTRATO

El Contratista debe acreditar, para que se le realice cada pago del Contrato, que se encuentra al día en los aportes parafiscales relativos al Sistema de Seguridad Social Integral, así como los propios del Sena, ICBF y cajas de compensación familiar, cuando corresponda.

2.2.5 CERTIFICADO DE ANTECEDENTES DISCIPLINARIOS, FISCALES, JUDICIALES, REGISTRO NACIONAL DE MEDIDAS CORRECTIVAS, DELITOS SEXUALES Y DEUDORES DE ALIMENTOS

El INDER verificará los antecedentes fiscales, disciplinarios, penales, y consultará el Registro Nacional de Medidas Correctivas de los oferentes y/o sus representantes legales o apoderados, así mismo, el oferente deberá aportar la consulta de estos tanto para la persona jurídica como para el representante legal cuando aplique o en su defecto persona natural.

Lo anterior, se realizará en los portales:

- www.contraloriagen.gov.co
- www.procuraduria.gov.co
- www.policia.gov.co
- https://srvpsi.policia.gov.co/PSC/frm_cnp_consulta.aspx
- https://inhabilidades.policia.gov.co:8080/.
- https://www.redam.gov.co/modulo-2

CERTIFICADO DE LA CUENTA BANCARIA

Los proponentes deberán aportar certificado de la cuenta bancaria en el que se les pagará en caso de ser adjudicatarios.

EXPERIENCIA:

2.2.6 CARACTERÍSTICAS DE LOS CONTRATOS PRESENTADOS PARA ACREDITAR LA EXPERIENCIA EXIGIDA

Todos los documentos deben ser presentados de forma individual (no unificar todo en un solo pdf).

Se tendrá como experiencia general mínima habilitante del proponente la acreditación de máximo dos (2) certificados de contratos ejecutados, terminados y liquidados por el proponente, que el valor sumado de los contratos y expresado en salarios mínimos mensuales legales vigentes (SMMLV) sea igual o superior al presupuesto oficial expresado en (SMMLV), es decir, igual o superior a 472.

Los contratos deben encontrarse en el RUP del Proponente y debe relacionarlos en el Formato 3 (Experiencia del Proponente). El Proponente deberá presentar ambos documentos (RUP y Formato 3) para participar del Proceso.

El contrato acreditado debe estar identificado al menos en tres (03) de los códigos del clasificador de bienes y servicios de Naciones Unidas a nivel de clase señalados en el siguiente cuadro:

CLASIFICACIÓN	SEGMENTO	FAMILIA	CLASE
43233200	Tecnología de la Información, Radiodifusión y Telecomunicaciones	Software	Software de seguridad y protección
43222500	Tecnología de la Información, Radiodifusión y Telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipo de seguridad de red
81111800	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas
81112200	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Mantenimiento y soporte de software

Para la certificación se admite, acta de liquidación o recibido a satisfacción y deberán cumplir con los siguientes requisitos:

a. Fecha de expedición
b. Razón social del contratante
c. Razón del social del contratista con Nit
d. Teléfonos del contratante (si es empresa privada)
e. Valor final del contrato, expresado en pesos colombianos o SMMLV
f. Fecha de inicio y terminación del contrato.
g. Objeto del contrato, este debe tener relación con el suministro e implementación de soluciones, tecnologías o servicios especializados de ciberseguridad, destinados a fortalecer la protección y seguridad de infraestructuras tecnológicas.

En caso de existir contradicción entre lo relacionado en el formulario y el RUP, prevalecerá la información consignada en el RUP.

Si los contratos fueron ejecutados bajo la modalidad de consorcio o unión temporal, el valor que debe informar el proponente será el correspondiente al porcentaje de participación que hubiere tenido en los mismos, es decir, en el contrato que le dio origen a la experiencia.

En caso de que el proponente no cumpla con la verificación anterior, serán considerados como **NO ADMISIBLES.**

Las certificaciones de experiencia deberán ser expedida por la entidad o empresa contratante de cada uno de ellas, donde se pueda verificar el objeto del contrato o sus obligaciones, y debe tener clara relación con el suministro e implementación de soluciones, tecnologías o servicios especializados de ciberseguridad, destinados a fortalecer la protección y seguridad de infraestructuras tecnológicas.

Las certificaciones deberán ser expedidas por el representante legal o funcionario competente de la respectiva entidad pública o privada contratante.

El proponente deberá aportar un certificado expedido por el o los fabricante(s) de la solución, dirigido a la Entidad donde se especifique que cuenta con un nivel de partner o canal en la categoría más alta dentro del programa de canales del fabricante y su fecha de expedición no podrá ser superior a treinta (30) días calendario contados a partir del cierre del proceso de selección.

PERSONAL PROFESIONAL REQUERIDO.

Esta documentación será evaluada en la etapa de requisitos habilitantes.

El personal profesional requerido debe estar vinculado con la empresa interesada en el proceso y demostrar su vinculación de mínimo los últimos 3 meses.

El contratista debe contar con un equipo mínimo de trabajo de 4 integrantes para la ejecución del proyecto, el cual debe estar conformado de la siguiente manera:

ROL	DESCRIPCIÓN
Un (1) Gerente de Proyecto.	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática **Experiencia general:** Debe contar con mínimo diez (10) años de experiencia general, contados a partir de la expedición de la matrícula profesional. **Título de Posgrado en:** Especialización o Maestría en áreas relacionadas con su carrera profesional Debe acreditar mediante una certificación, que tiene fundamentos en ciberseguridad, esta debe ser emitida por el fabricante. Debe acreditar mediante una certificación vigente, conocimientos a nivel profesional en gestión de proyectos. **Experiencia específica:** Especifica mínima de ocho (8) años gerenciando y/o coordinando proyectos en temas relacionados con seguridad de la información y/o seguridad informática.

Un (1) Ingeniero de Soporte	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática **Experiencia general:** mínimo tres (3) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. **Título de Posgrado:** Especialización o maestría en seguridad informática o ciberseguridad Debe estar Certificado como profesional en seguridad de redes por el fabricante y debe estar vigente Debe acreditar mediante una certificación que cuenta con conocimientos para brindar soluciones de seguridad de redes y debe estar vigente y debe ser emitida por el fabricante. Experiencia específica: Mínimo Dos (2) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad.
Un (1) Especialista en Ciberseguridad:	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática **Experiencia general:** Mínimo cinco (5) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. **Título de Posgrado:** Especialización o maestría en seguridad informática o ciberseguridad Debe acreditar mediante una certificación que cuenta con conocimientos para brindar soluciones de seguridad de

	redes, debe estar vigente y debe ser emitida por el fabricante. Debe contar con certificación de EH-Ethical Hacker vigente. **Experiencia específica:** Mínimo Dos (2) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad.
Un (1) Ingeniero de apoyo a la implementación WAF	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática. **Experiencia general:** Mínimo tres (3) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. Debe contar con certificación como Profesional de seguridad en nube emitida por el fabricante. **Experiencia específica:** Mínimo un (1) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad

Documentación para entregar

- Cedula de ciudadanía
- Hoja de vida del profesional
- Diploma de título Profesional
- Tarjeta Profesional con Certificación de vigencia
- Certificaciones que acrediten experiencia especifica
- Certificaciones acreditadas de especialista o maestría en las áreas solicitadas, según aplique.
- Certificaciones técnicas solicitadas en cada uno de los perfiles

- Planilla de seguridad social u otro documento que acredite la vinculación con la empresa interesada en el proceso.

Teniendo en cuenta que el personal propuesto es objeto de verificación dentro de los requisitos habilitantes, las hojas de vida y el personal acreditado por el proponente durante el proceso de selección no podrán ser sustituidos. En consecuencia, en caso de resultar adjudicado, el contratista deberá garantizar que el personal presentado y aprobado durante la etapa de selección sea el mismo que ejecute el proyecto.

CRITERIOS DEFERENCIALES DECRETO 1860 DE 2021:

Con fundamento en los artículos 2.2.1.2.4.2.14 y 2.2.1.2.4.2.15 respecto a emprendimientos y empresas de mujeres y en el artículo 2.2.1.2.4.2.18 respecto de las Mipyme, del Decreto 1860 de 2021, las Entidades Estatales establecerán condiciones habilitantes diferenciales que promuevan y faciliten la participación en los procedimientos de selección competitivos. En este sentido, para el presente proceso se establecen los siguientes criterios diferenciales únicamente para la experiencia del proponente:

CRITERIO	PUNTAJE MÁXIMO
VALOR DE LA PROPUESTA	59,5
FACTOR DE CALIDAD	28
ESTIMULO A LA INDUSTRIA NACIONAL	10
PUNTAJE ADICIONAL PARA EMPLEADORES DE PERSONAS CON DISCAPACIDAD Y PARA EMPRENDIMIENTOS Y EMPRESAS DE PERSONAS CON DISCAPACIDAD	2
PUNTAJE ADICIONAL PARA EMPRENDIMIENTOS Y EMPRESAS DE MUJERES (0.25%)	0,25
PUNTAJE ADICIONAL PARA MIPYME EN EL SISTEMA DE COMPRAS PÚBLICAS (0.25%)	0,25
TOTAL	**100**

Experiencia habilitante para emprendimientos y empresas de mujeres

Para la calificación de este aspecto se asignará un puntaje máximo de CERO PUNTO VEINTICINCO (0.25) del valor total de los puntos y se tendrá en cuenta lo establecido en el artículo 2.2.1.2.4.2.15 del Decreto 1082 de 2015, que regula lo relacionado con la adopción de

medidas afirmativas que incentiven la participación de las mujeres en el sistema de compras públicas.

Se asignará el puntaje asignado a este criterio, únicamente a aquellos oferentes que acrediten alguna de las siguientes condiciones:

No	Condición	Medio de Prueba
1	Cuando más del cincuenta por ciento (50%) de las acciones, partes de interés o cuotas de participación de la persona jurídica (proponente) pertenezcan a mujeres y los derechos de propiedad hayan pertenecido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección.	Esta circunstancia se acreditará mediante certificación expedida por el representante legal y el revisor fiscal del proponente, cuando exista de acuerdo con los requerimientos de ley, o el contador, donde conste la distribución de los derechos en la sociedad y el tiempo en el que las mujeres han mantenido su participación.
2	Cuando por lo menos el cincuenta por ciento (50%) de los empleos del nivel directivo[1] de la persona jurídica sean ejercidos por mujeres y éstas hayan estado vinculadas laboralmente a la empresa durante al menos el último año anterior a la fecha de cierre del Proceso de Selección en el mismo cargo u otro del mismo nivel.	Esta circunstancia se acreditará mediante certificación expedida por el representante legal y el revisor fiscal del proponente, cuando exista de acuerdo con los requerimientos de ley, o el contador, donde se señale de manera detallada todas las personas que conforman los cargos de nivel directivo del proponente, el número de mujeres y el tiempo de vinculación. La certificación deberá relacionar el nombre completo y el número de documento de identidad de cada una de las personas que conforman el nivel directivo del proponente. Además, se deberá allegar como soporte, copia de los respectivos documentos de identidad, copia de los contratos de trabajo o certificación laboral con las funciones, así como el certificado de aportes a

[1] Se entenderá como empleos del nivel directivo aquellos cuyas funciones están relacionadas con la dirección de áreas misionales de la empresa y la toma de decisiones a nivel estratégico. En este sentido, serán cargos de nivel directivo los que dentro de la organización de la empresa se encuentran ubicados en un nivel de mando o los que por su jerarquía desempeñan cargos encaminados al cumplimiento de funciones orientadas a representar al empleador.

		seguridad social del último año en el que se demuestren los pagos realizados por el empleador.
3.	Cuando la persona natural sea una mujer y haya ejercido actividades comerciales a través de un establecimiento de comercio durante al menos el último año anterior a la fecha de cierre del proceso de selección.	Esta circunstancia se acreditará mediante la copia de cédula de ciudadanía, la cédula de extranjería o el pasaporte, así como la copia del registro mercantil vigente.
4.	Para las asociaciones y cooperativas, cuando más del cincuenta por ciento (50%) de los asociados sean mujeres y la participación haya correspondido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección.	Esta circunstancia se acreditará mediante certificación expedida por el representante legal.

Las certificaciones de trata el presente artículo deben expedirse bajo la gravedad de juramento con una fecha de máximo treinta (30) días calendario anteriores a la prevista para el cierre del procedimiento de selección.

Para obtener el puntaje previsto en este criterio, en el caso de consorcios y uniones temporales, por lo menos uno de sus integrantes deberá acreditar que (i) es una empresa de mujeres, según alguna de las condiciones antes descritas y que, (ii) tiene una participación igual o superior al diez por ciento (10%) en la figura asociativa.

Experiencia general habilitante para Mipyme

Para la calificación de este aspecto se asignará un puntaje máximo de PUNTO VEINTICINCO (0.25) del valor total de los puntos y se tendrá en cuenta lo establecido en el artículo 2.2.1.2.4.2.18 del Decreto 1082 de 2015, que regula lo relacionado con la adopción de criterios diferenciales para MiPymes domiciliadas en Colombia.

Para acreditar la condición de MiPymes se verificará lo pertinente, en el certificado del Registro Único de Proponentes de los oferentes. de conformidad con el parágrafo primero del artículo 2.2.1.2.4.2.4. del Decreto 1082 de 2015.

Para obtener el puntaje previsto en este criterio, en el caso de consorcios y uniones temporales, por lo menos uno de sus integrantes deberá acreditar la calidad de MiPymes y tiene una participación igual o superior al diez por ciento (10%) en la figura asociativa.

Nota. Este puntaje se otorgará siempre y cuando la convocatoria pública no haya sido limitada a Mipyme conforme a los artículos 2.2.1.2.4.2.2 y 2.2.1.2.4.2.3 del Decreto 1082 de 2015.

VALOR DE LA PROPUESTA

Se asignará el mayor puntaje a la propuesta de menor precio y de forma proporcional a los demás oferentes, de conformidad con la fórmula que se detalla más abajo, para lo cual, el oferente consignará su oferta en el anexo respectivo publicado por la entidad.

El valor que se tomará para efectos de la evaluación, será el corregido por la entidad, si hubo lugar a ello.

PE = 59,5*(Vm /VE)

PE: Puntos del proponente evaluado.

Vm: Valor menor ofertado.

VE: Valor del proponente a evaluar.

Los precios ofrecidos serán fijos no reajustables y deberán ser en cifras enteras sin decimales, en moneda colombiana, para toda la vigencia del contrato.

ser en cifras enteras sin decimales, en moneda colombiana, para toda la vigencia del contrato.

FACTOR DE CALIDAD

Se otorgará puntaje al proponente que ofrezca para la solución, configuración y puesta en funcionamiento de la solución, lo siguiente:

CERTIFICACIONES	PUNTAJE

PLAN DE MEJORA CONTINUA DE LA POSTURA DE CIBERSEGURIDAD El plan deberá estar estructurado a partir de una metodología de evaluación de ciberseguridad reconocida, basada en alguno de los siguientes marcos de referencia: NIST Cybersecurity Framework (CSF), ISO/IEC 27001 o CIS Controls, y deberá contemplar como mínimo: 1. Metodología propuesta para realizar la evaluación de la postura actual de ciberseguridad. 2. Análisis de la postura de ciberseguridad y definición iniciativas de fortalecimiento. 3. Propuesta de acciones de mejora orientadas al fortalecimiento de la postura de ciberseguridad. 4. Definición de responsables, recursos y tiempos estimados para la implementación de las acciones. 5. Sesión de seguimiento y actualización del plan de mejora continua antes de finalizar el contrato. Perfil del profesional que lidera la actividad Esta actividad debe ser liderada por un profesional con: Título profesional: Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Electrónica, Ingeniería de Software o Ingeniería de Telecomunicaciones. Título de posgrado: Especialización o maestría en áreas relacionadas con Seguridad Informática, Ciberseguridad o Seguridad de la Información. Certificaciones vigentes: Una (1) certificación vigente CEH – Certified Ethical Hacker. Una (1) certificación vigente como Lead Cybersecurity Manager en ISO/IEC 27032. Una (1) certificación vigente como Auditor Líder o Auditor Interno en ISO/IEC 27001:2022.	28 puntos

Para la asignación del puntaje por el factor de calidad, el proponente deberá presentar los documentos soporte:

- Cedula de ciudadanía
- Hoja de vida del profesional
- Diploma de título Profesional
- Tarjeta Profesional con Certificación de vigencia
- Certificaciones que acrediten experiencia especifica
- Certificaciones acreditadas de especialista o maestría en las áreas solicitadas.

- Certificaciones técnicas solicitadas del perfil
- Planilla de seguridad social u otro documento que acredite la vinculación con la empresa interesada en el proceso.

El profesional que cumpla con el perfil descrito en este ítem podrá, a su vez, hacer parte del equipo de profesionales exigido, sin que ello constituya impedimento alguno.

ESTIMULO A LA INDUSTRIA NACIONAL (10 PUNTOS)

En aquellos casos en que, de acuerdo con el objeto contractual, no existan bienes colombianos relevantes o no exista oferta nacional de los mismos en el Registro de Productores de Bienes Nacionales, la Entidad Estatal otorgará el puntaje de que trata el inciso primero del artículo 2 de la Ley 816 de 2003 al proponente que vincule el porcentaje mínimo establecido por la Entidad Estatal de empleados o contratistas por prestación de servicios colombianos, que no podrá ser inferior al 40% del total de empleados y contratistas asociados al cumplimiento del contrato.

Para el presente proceso de contratación, la entidad no asignará puntaje por bienes relevantes nacionales. De acuerdo con el Decreto 680 del 22 junio de 2021, la entidad estudió los numerales establecidos en el artículo 2 y en virtud del análisis del sector económico y de los oferentes, se concluyó que este proceso corresponde a servicios, razón por la cual no contiene bienes colombianos relevantes.

Por otra parte, el presupuesto para la presente contratación se encuentra determinado en el Plan Anual de Adquisiciones; de igual manera, se precisa que para el presente proceso de selección no aplica los bienes del registro de productores de bienes nacionales por las razones expuestas ya que este proceso está comprendido en el sector de servicios.

Teniendo en cuenta lo anterior y de acuerdo con el análisis efectuado en el estudio del sector se identificó que los proponentes y el personal que ejecutarán las actividades, son de origen colombiano, razón por la cual, para obtener el puntaje correspondiente al ítem de apoyo a la industria nacional, el recurso humano colombiano o sujeto a trato nacional que se vincule no deberá ser al menor del 40% del total de empleados y contratistas.

Así las cosas, el puntaje para el ítem APOYO A LA INSDUSTRIA NACIONAL, se asignará de la siguiente manera:

CONCEPTO APOYO A LA INDUSTRIA NACIONAL	PUNTAJE

El proponente deberá manifestar bajo la gravedad de juramento que, en caso de resultar adjudicatarios, el recurso humano colombiano o sujeto a trato nacional que vincule o tenga vinculados no será inferior al 40% del total de empleados y contratistas asociados al cumplimiento del contrato	10 PUNTOS

Para el cumplimiento de este requisito calificable el proponente deberá diligenciar el **FORMATO APOYO A LA INDUSTRIA NACIONAL**. Quien no oferte ninguno de los criterios definidos en este numeral, obtendrá cero (0) puntos. Para el cumplimiento de este requisito calificable el proponente deberá diligenciar el formato respectivo y entregarlo con la oferta.

NOTA 1: En el caso que algún profesional o técnico sea extranjero, no se otorgará el puntaje correspondiente.

NOTA 2: En el caso de consorcios o uniones temporales, conformados por participantes nacionales y extranjeros sin derecho a trato nacional, el puntaje se otorgará con la sumatoria del puntaje que obtendría cada uno de sus integrantes en proporción a su porcentaje de participación en la figura asociativa.

Persona natural extranjera residente en Colombia, con la presentación de la visa correspondiente que le permita la ejecución del objeto contractual de conformidad con la ley. La cual deberá ser aportada con la oferta en copia simple.

Persona jurídica constituida en el país, se verificará con el certificado de Cámara y Comercio que el domicilio de la persona jurídica esté dentro del territorio nacional.

Servicios extranjeros con trato nacional

Se asignará puntaje de los servicios nacionales a aquellos servicios que provengan de otros estados (i) con los cuales exista un acuerdo comercial aplicable al proceso de contratación y (ii) respecto de los cuales exista un trato nacional por reciprocidad.

Adicional a lo anterior, para la obtención del puntaje por el factor de Industria Nacional, el proponente Nacional o Extranjero con trato Nacional, deberá presentar el formato debidamente diligenciado y suscrito por la persona natural o representante legal de la persona jurídica o representante legal del proponente plural, según corresponda

PUNTAJE ADICIONAL PARA EMPLEADORES DE PERSONAS CON DISCAPACIDAD Y PARA EMPRENDIMIENTOS Y EMPRESAS DE PERSONAS CON DISCAPACIDAD

Para la calificación de este aspecto se asignará un puntaje máximo de DOS (2) del valor total de los puntos y se tendrá en cuenta lo establecido en el artículo 2.2.1.2.4.2.7.4. **del Decreto 0287 del 2026,** que regula lo relacionado con la adopción de medidas afirmativas que incentiven la participación de las personas con discapacidad en el sistema de compras públicas

2.2.7 CONSIDERACIONES PARA LA VALIDEZ DE LA EXPERIENCIA REQUERIDA

La Entidad tendrá en cuenta los siguientes aspectos para analizar la experiencia requerida:

A. Tratándose de Proponentes Plurales se tendrá en cuenta lo siguiente: i) uno de los integrantes debe aportar como mínimo el cincuenta por ciento (50%) de la experiencia exigida; ii) los demás integrantes deben acreditar al menos el cinco por ciento (5%) de la experiencia requerida; y iii) sin perjuicio de lo anterior, solo uno de los integrantes, si así lo considera pertinente, podrá no acreditar experiencia. En este último caso, el porcentaje de participación del integrante que no aporta experiencia relacionada en la estructura plural no podrá superar el cinco por ciento (5%).

B. Cuando el contrato que se pretende acreditar como experiencia haya sido ejecutado en Consorcio o en Unión Temporal, el porcentaje de participación del integrante será alguno de los documentos válidos para la acreditación de experiencia en caso de que el integrante no esté obligado a tener RUP.

C. Las auto certificaciones no servirán para acreditar la experiencia, ya que con estas no se puede constatar la ejecución de contratos que deben ser certificados por los terceros que recibieron el bien o servicio. Para la aplicación de esta regla, se entiende por auto certificaciones aquellas expedidas por el mismo Proponente, sus representantes o los integrantes del Proponente Plural para acreditar su propia experiencia.

2.2.8 DOCUMENTOS VÁLIDOS PARA LA ACREDITACIÓN DE LA EXPERIENCIA REQUERIDA

En aquellos casos en que por las características del objeto a contratar se requiera verificar información adicional a la contenida en el RUP, el Proponente podrá aportar uno o algunos de los documentos que se establecen a continuación, para que la Entidad realice la verificación en forma directa. Los mismos deberán estar diligenciados y suscritos por el contratante, el Contratista o el interventor, según corresponda. En caso de existir discrepancias entre dos (2) o más documentos aportados por el Proponente para la acreditación de la experiencia, se tendrá en cuenta el orden de prevalencia indicado a continuación:

A. Acta de liquidación.

B. Acta de entrega, terminación, final o de recibo definitivo.

C. Certificación de experiencia. Expedida con posterioridad a la fecha de terminación del Contrato en la que conste el recibo a satisfacción del bien o servicio contratada debidamente suscrita por quien esté en capacidad u obligación de hacerlo.

D. Acta de inicio o la orden de inicio. La misma solo será válida para efectos de acreditar la fecha de inicio.

E. Para los contratos que hayan sido objeto de cesión, el Contrato deberá encontrarse inscrito y clasificado en el RUP o en uno o alguno de los documentos considerados como válidos para la acreditación de experiencia de la persona jurídica o natural cesionaria, según aplique. La experiencia se admitirá para el cesionario y no se reconocerá experiencia alguna al cedente.

2.2.9 PARA SUBCONTRATOS

Para la acreditación de experiencia de subcontratos, cuyo contrato principal fue suscrito con particulares, se aplicarán las disposiciones establecidas en el numeral anterior. Para la acreditación de experiencia de los contratos derivados de contratos suscritos con Entidades Estatales, el Proponente deberá aportar los documentos que se describen a continuación:

A. Certificación del subcontrato. Certificación expedida con posterioridad a la fecha de terminación del subcontrato, la cual debe estar suscrita por el representante legal del Contratista del contrato principal, del Concesionario, o del EPC o Consorcio Constructor. Así mismo, debe contener la información requerida en el numeral 3.3.4 de este Pliego de Condiciones para efectos de constatar la experiencia.

B. Certificación emitida por la Entidad Estatal del contrato principal del cual se derivó el subcontrato.

Para los subcontratos, las actividades subcontratadas solo serán válidas para el subcontratista cuando ambos se presenten de manera separada al Proceso de Contratación; es decir, dichas actividades no serán tenidas en cuenta para efectos de acreditación de experiencia del contratista directo.
En todo caso, la experiencia será válida para quien efectivamente haya ejecutado las actividades exigidas.

REDUCCIÓN DE PUNTAJE POR INCUMPLIMIENTO

En caso de que al proponente o a algún integrante del consorcio o unión temporal se le haya impuesto una o más multas o cláusulas penales durante el último año, contado a partir de la fecha prevista para la presentación de las ofertas, sin importar la cuantía, del total de puntaje obtenido, se realizará un descuento correspondiente al dos por ciento (2%).

Dicha reducción no se aplicará en caso de que los actos administrativos que hayan impuesto las multas sean objeto de medios de control jurisdiccional a través de las acciones previstas en la Ley 1437 de 2011 o las normas que la modifiquen, adicionen o sustituyan; para lo cual el proponente deberá presentar CON LA OFERTA, la demanda debidamente radicada ante la autoridad judicial correspondiente, la cual deberá haberse radicado antes del cierre de presentación de ofertas.

NOTA 1: Para efectos de aplicar lo dispuesto en el artículo 58 de la Ley 2195 de 2022 y parágrafos, las decisiones correspondientes a la imposición de multas o cláusulas penales deben estar en firme e inscritas en el RUP para que sean tenidas en cuenta en el presente proceso de selección, lo anterior de conformidad con lo establecido en el artículo 29 y 83 de la Constitución Política de Colombia, siempre que las mismas se hayan impuesto y publicado después del 18 de enero de 2022.

2.3 CAPACIDAD FINANCIERA

La verificación y evaluación de la capacidad financiera y organizacional se realizará de acuerdo con la información reportada en el formato 4 Capacidad Financiera.

Si el proponente presenta la información financiera en la forma exigida y cuenta con los indicadores de capacidad financiera y capacidad organizacional requeridos, la propuesta será calificada como CUMPLE y estará habilitado.

En el caso que el oferente presente información que no sea clara o no allegara la documentación exigida completa, la entidad podrá solicitarla para que sea aportada durante el término del traslado del informe de evaluación.

a. Capacidad financiera y Capacidad organizacional

Para el presente proceso de contratación se establecen los siguientes indicadores como requisito habilitante para evaluar la capacidad financiera de los proponentes:

CAPACIDAD FINANCIERA			CAPACIDAD ORGANIZACIONAL	
INDICE DE LIQUIDEZ	**NIVEL DE ENDEUDAMIENTO**	**COBERTURA DE INTERESES**	**RENTABILIDAD PATRIMONIO**	**RENTABILIDAD ACTIVO**
Mayor o igual (≥) a **1,03**	Menor o igual (≤) a **0.75**	Mayor o igual (≥) a **1.45**	Mayor o igual (≥) a **0.05**	Mayor o igual (≥) a **0.03**

Las empresas que al cierre de su ejercicio económico no registren Gastos Financieros, y que el resultado del indicador de Cobertura de Intereses resulte indeterminado por la operación matemática de dividir entre cero (0), se considera que cumplen con el requisito y se habilitan dentro del proceso de verificación de requisitos habilitantes.

Criterio financiero y organizacional diferencial para Mipymes:

Con fundamento en los artículos 2.2.1.2.4.2.14 y 2.2.1.2.4.2.15 respecto a emprendimientos y empresas de mujeres y en el artículo 2.2.1.2.4.2.18 respecto de las Mipyme, del Decreto 1860 de 2021, las Entidades Estatales establecerán condiciones habilitantes diferenciales que promuevan y faciliten la participación en los procedimientos de selección competitivos. En este sentido, para el presente proceso se establecen los siguientes criterios diferenciales únicamente para la experiencia del proponente:

En el marco del presente proceso se definen los siguientes indicadores de capacidad financiera y organizacional, como incentivo que busca fomentar la participación de las emprendimientos, empresas de mujeres y Mipyme en el sistema de compras y contratación pública:

CAPACIDAD FINANCIERA			CAPACIDAD ORGANIZACIONAL	
INDICE DE LIQUIDEZ	**NIVEL DE ENDEUDAMIENTO**	**COBERTURA DE INTERESES**	**RENTABILIDAD PATRIMONIO**	**RENTABILIDAD ACTIVO**
Mayor o igual (≥) a **1,0**	Menor o igual (≤) a **0,75**	Mayor o igual (≥) a **1,3**	Mayor o igual (≥) a **0,04**	Mayor o igual (≥) a **0,02**

Consideraciones para acreditar la capacidad financiera y capacidad organizacional de personas naturales o jurídicas extranjeras sin domicilio o sucursal en Colombia

Para garantizar la participación de las Personas Extranjeras no inscritas en el Registro Único de Proponentes por no tener domicilio o sucursal en el país, a estas no se les podrá exigir el requisito de inscripción en el Registro Único de Proponentes. En consecuencia, los citados oferentes deberán aportar la información antes solicitada (indicadores) para verificar su capacidad financiera. Las personas extranjeras deberán presentar la certificación firmada por el Representante Legal, acompañada de traducción simple al idioma español, con los valores re-expresados a la moneda funcional colombiana (peso colombiano), a la tasa de cambio de la fecha de cierre de los mismos, avalados con la firma de un Contador Público con Tarjeta Profesional expedida por la Junta Central de Contadores de Colombia y certificado de vigencia de inscripción y antecedentes disciplinarios.

El Instituto de Deportes y Recreación de Medellín INDER se reserva la facultad de solicitar información adicional, con el fin de verificar y/o aclarar los datos reportados en los certificados requeridos.

2.4 PERSONAS NATURALES O JURÍDICAS NACIONALES Y EXTRANJERAS CON DOMICILIO O SUCURSAL EN COLOMBIA

La evaluación financiera y organizacional de las propuestas se efectuará a partir de la información contenida en el RUP vigente y en firme. En tal sentido, la evaluación de la capacidad financiera se realizará de acuerdo con la información reportada en el RUP, según las disposiciones establecidas en la Subsección 5, de la Sección 1, del Capítulo 1, del Título 1, de la Parte 2 del Decreto 1082 de 2015, o las normas que las modifiquen, adicionen o sustituyan, por lo que se tomará la información financiera del mejor año fiscal que se refleje en el registro del Proponente y que esté vigente y en firme.

Los Proponentes extranjeros sin domicilio o Sucursal en Colombia no están obligados a tener RUP y por tanto la verificación de esta información procederá en los términos definidos en el siguiente numeral.

2.4.1 PERSONAS NATURALES O JURÍDICAS EXTRANJERAS SIN DOMICILIO O SUCURSAL EN COLOMBIA

Los Proponentes extranjeros sin domicilio o Sucursal en Colombia deberán allegar la siguiente información financiera de conformidad con la legislación propia del país de origen. Los valores deben: (i) presentarse en Pesos Colombianos; (ii) convertirse a la tasa de cambio de la fecha de corte de los mismos y (iii) estar avalados con la firma de quien se encuentre en obligación de hacerlo de acuerdo con la normativa del país de origen.

1. El estado de situación financiera (balance general) y estado de resultado integral (estado de resultados), acompañados por el informe de auditoría (sí aplica según la legislación de origen) con traducción simple al español de acuerdo con las normas NIIF.

2. Copia de la tarjeta profesional del contador público o revisor fiscal y certificado de antecedentes disciplinarios vigente expedido por la autoridad competente de quien realiza la conversión.

3. El Formato 4 – Capacidad financiera y organizacional para extranjeros diligenciado. En caso de presentarse discrepancias entre la información consignada en el Formato 4 – Capacidad financiera y organizacional para extranjeros y los documentos señalados en el literal A, prevalecerá la información consignada en los estados financieros incluidos en la oferta.

Las fechas de corte de los documentos señalados en el literal A será [la Entidad establecerá las fechas de corte de acuerdo con lo contemplado en la Subsección 5, de la Sección 1, del Capítulo 1, del Título 1, de la Parte 2 del Decreto 1082 de 2015 o las normas que las modifiquen, adicionen o sustituyan. En tal sentido, se tomará la información de acuerdo con el mejor año fiscal del Proponente], acompañado del Informe de Auditoría, salvo que se acredite en debida forma que la legislación propia del país de origen fije una fecha de corte diferente a la prevista en este pliego.

Si alguno de estos requerimientos no aplica en el país del domicilio del Proponente extranjero, el representante legal o el apoderado en Colombia deberán hacerlo constar bajo la gravedad de juramento en el Formato 4 – Capacidad financiera y organizacional para extranjeros. El Proponente podrá acreditar este requisito con un documento que así lo certifique emitido por una firma de auditoría externa.

Si los valores de los estados financieros están expresados originalmente en una moneda diferente a Dólares de los Estados Unidos de América, estos deberán convertirse a Pesos en los términos definidos el presente documento.

CAPÍTULO VII. GARANTÍAS

6.1 GARANTÍA DE SERIEDAD DE LA OFERTA

El Proponente debe presentar con la propuesta una Garantía de seriedad de la oferta que cumpla con los parámetros, condiciones y requisitos que se indican en este numeral. Cualquier error o imprecisión en el texto de la Garantía presentada será susceptible de aclaración por el Proponente hasta el término de traslado del informe de evaluación. Sin embargo, la no entrega de la Garantía no es subsanable y se rechazará la oferta.

Las características de las Garantías son las siguientes:

Característica	Condición
Clase	Cualquiera de las clases permitidas por el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015, a saber: (i) contrato de seguro contenido en una póliza, (ii) patrimonio autónomo y (iii) garantía bancaria.
Asegurado/ beneficiario	INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN - INDER identificada con el NIT 800.194.096-0
Amparos	La sanción derivada del incumplimiento del ofrecimiento en los eventos señalados en el artículo 2.2.1.2.3.1.6 del Decreto 1082 de 2015.
Vigencia	3 meses contados a partir de la fecha de cierre del Proceso de Contratación.
Valor asegurado	Diez por ciento (10 %) del Presupuesto Oficial del Proceso de Contratación
Tomador	• Para las personas jurídicas: la Garantía deberá tomarse con el nombre o razón social y tipo societario que figura en el certificado de existencia y representación legal expedido por la cámara de comercio respectiva, y no solo con su sigla, a no ser que en el referido documento se exprese que la sociedad podrá denominarse de esa manera. • Para los Proponentes Plurales: la Garantía deberá ser otorgada por todos los integrantes del Proponente Plural, para lo cual se tendrá que relacionar claramente los integrantes, su identificación y porcentaje de participación.

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

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

6.2. GARANTÍAS DEL CONTRATO

Para cubrir cualquier hecho constitutivo de incumplimiento, el Contratista deberá presentar la Garantía de cumplimiento en original a la Entidad dentro de los tres (3) días hábiles siguientes

contados a partir de la firma del Contrato y requerirá la aprobación de la Entidad. Esta Garantía tendrá las siguientes características:

<table>
<tr><th>CARACTERÍSTICA</th><th>CONDICIÓN</th></tr>
<tr><td>Clase</td><td>Cualquiera de las clases permitidas por el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015, a saber: (i) Contrato de seguro contenido en una póliza para Entidades Estatales, (ii) patrimonio autónomo, (iii) Garantía bancaria.</td></tr>
<tr><td>Asegurado/ beneficiario</td><td>INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN – INDER, identificada con el NIT 800.194.096-0.</td></tr>
<tr><td>Amparos, vigencia y valores asegurados</td><td>
<table>
<tr><th>AMPARO</th><th>VIGENCIA</th><th>VALOR ASEGURADO</th></tr>
<tr><td>Cumplimiento general del Contrato y el pago de las multas y la cláusula penal pecuniaria que se le impongan</td><td>Plazo del contrato y 1 año más.</td><td>Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato.</td></tr>
<tr><td>Calidad del servicio</td><td>Plazo del contrato y un (1) año más.</td><td>Por una cuantía equivalente al cinco por ciento (5%) del valor total del contrato.</td></tr>
<tr><td>Pago de salarios, prestaciones sociales legales e indemnizaciones laborales</td><td>Plazo del contrato y tres (3) años más</td><td>Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato.</td></tr>
</table>
</td></tr>
<tr><td>Tomador</td><td>A. Para las personas jurídicas: la Garantía deberá tomarse con el nombre o razón social y tipo societario que figura en el certificado de existencia y representación legal expedido por la cámara de comercio respectiva, y no sólo con su sigla, a no ser que en el referido documento se exprese que la sociedad podrá denominarse de esa manera.
B. No se aceptan Garantías a nombre del representante legal o de alguno de los integrantes del Consorcio o de la Unión Temporal. Cuando el Contratista sea una Unión Temporal o Consorcio, se debe incluir el nombre, el NIT y el porcentaje de participación de cada uno de los integrantes.</td></tr>
</table>

	C.	Para el Contratista conformado por un Proponente Plural (Unión Temporal o Consorcio): la Garantía deberá ser otorgada por todos los integrantes del Contratista, para lo cual se deberá relacionar claramente los integrantes, su identificación y porcentaje de participación, quienes para todos los efectos serán los otorgantes de esta.
Información necesaria dentro de la póliza	D. E. F. G.	Número y año del Contrato Objeto del Contrato Firma del representante legal del Contratista En caso de no usar centavos, los valores deben aproximarse al mayor Ej. Cumplimiento si el valor a asegurar es $14.980.420,20 aproximar a $14.980.421.

NOTA 1: La garantía de CUMPLIMIENTO deberá constituirse de la siguiente manera:
Tomador: Contratista;
Asegurado: El contratista y el INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN – INDER.
Beneficiarios: El INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN – INDER.

El Contratista está obligado a restablecer el valor de la Garantía cuando esta se vea reducida por razón de las reclamaciones que efectúe la Entidad, así como, a ampliar las Garantías en los eventos de adición y/o prórroga del Contrato. El no restablecimiento de la Garantía por parte del Contratista o su no adición o prórroga, según el caso, constituye causal de incumplimiento del Contrato y se iniciarán los procesos sancionatorios a que haya lugar.

7.CAPÍTULO VIII. MINUTA Y CONDICIONES DEL CONTRATO

Las condiciones de ejecución del Contrato están previstas en el Anexo 4 – Minuta del contrato. Dentro de estas condiciones se incluye la forma de pago, obligaciones y derechos generales del Contratista, obligaciones de la Entidad, garantías, multas, cláusula penal y otras condiciones particulares aplicables al negocio jurídico a celebrar.

El Proponente adjudicatario debe presentar el Registro Único Tributario—RUT y demás documentos necesarios para la celebración del Contrato al momento de la firma.

8. CAPÍTULO IX. LISTADO DE ANEXOS, FORMATOS, MATRICES Y FORMULARIOS

8.1 ANEXOS

1. Anexo 3 – Pacto de Transparencia
2. Anexo 4 – Minuta del Contrato

8.2 FORMATOS

1. Formato 1 – Carta de presentación de la oferta
2. Formato 2 – Conformación de Proponente plural (Formato 2A- Consorcios) (Formato 2B- UT)
3. Formato 3 – Experiencia
4. Formato 4 – Capacidad financiera y organizacional
5. Formato 6 – Pagos de seguridad social y aportes legales
6. Formato 10- Factores de desempate
7. Formato - APOYO A LA INDUSTRIA NACIONAL

7.3 MATRICES

1. Matriz 2 – Riesgos