CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA-CVC
SELECCIÓN ABREVIADA MENOR CUANTÍA No. 38 – 2021

PLIEGO DE CONDICIONES ELECTRONICO

"ADQUISICION, IMPLEMENTACIÓN Y SOPORTE TECNICO DE NIVEL 3 DE LICENCIAS ANTIVIRUS PARA LA CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA"

SANTIAGO DE CALI
DICIEMBRE 9 DE 2021

Corporación Autónoma Regional del Valle del Cauca

INTRODUCCIÓN

Publicidad y principio de transparencia. En cumplimiento de la Ley 80 de 1993, la Ley 1150 de 2007, el Decreto 1082 de 2015 y lo dispuesto en la materia por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente, la CVC presenta a los oferentes el presente Pliego de Condiciones con sus correspondientes anexos, el cual contiene la información, las condiciones y los requisitos que deben cumplir cada uno de los partícipes en el proceso y cuando corresponda, al futuro contratista; en virtud de ello, el Pliego de Condiciones es ley para las partes.

Estudio y documentos previos. Son el soporte para la elaboración del Pliego de Condiciones y el Contrato y deben permanecer a disposición del público durante el proceso de contratación.

Observaciones al pliego de condiciones. Cualquier interesado puede presentar observaciones y/o aclaraciones al presente documento en las diferentes etapas del proceso, por ello la CVC agradece las sugerencias y observaciones realizadas de manera respetuosa que contribuyan a la confección objetiva del pliego, en aras de lograr la consecución de los fines esenciales del Estado consagrados en la Constitución Política.

Derechos y deberes de los proponentes y contratistas. Colaboraran con las entidades contratantes en lo que sea necesario para que el objeto contratado se cumpla y que este sea de la mejor calidad; obraran con lealtad y buena fe en las distintas etapas del proceso contractual, evitando las dilaciones y entrabamientos que pudieran presentarse.

Principio de responsabilidad. Responderán tanto los oferentes como el contratista por haber ocultado a la CVC al proponer o contratar, inhabilidades, incompatibilidades o prohibiciones, o por haber suministrado información con presuntas irregularidades.

Del deber de la selección objetiva. En los pliegos de condiciones se indicarán los requisitos objetivos necesarios para participar en el correspondiente proceso de selección, para lo cual se confeccionarán reglas objetivas, justas, claras y completas, las cuales permitirán la confección de ofrecimientos de la misma índole, asegurarán una escogencia objetiva y evitarán la declaratoria del proceso.

Obligatoriedad de acatar protocolos de indisponibilidad del SECOP II. El protocolo está dirigido a los usuarios del SECOP II en los eventos en los que la plataforma presente Falla General o Particular que interrumpa el normal desarrollo de los procesos de contratación.

Corporación Autónoma Regional del Valle del Cauca

CAPITULO I.
ASPECTOS GENERALES

A. Control social - veedurías ciudadanas y la participación comunitaria. La CVC brindará especial apoyo y colaboración a las personas y asociaciones que emprendan campañas de control y vigilancia de la gestión pública contractual y oportunamente suministrará la documentación e información que requieran para el cumplimiento de tales labores, la Ley 1712 de 2014, ley de transparencia y acceso a la información pública, cuerpo normativo de carácter estatutario, que regula particularidades al acceso a la información pública producida por la Entidad.

B. Secretaria de Transparencia. En el evento de conocerse casos especiales de corrupción en la CVC, por ser entidad del Estado, se debe reportar lo sucedido al Programa Presidencial "Lucha contra la Corrupción".

C. Costos derivados de participar en el proceso de contratación. Los costos y gastos en que los interesados o proponentes incurran con ocasión del análisis de los documentos del proceso, la presentación de observaciones, la preparación y presentación de las ofertas, y cualquier otro costo o gasto relacionado con la participación en el Proceso de Contratación estará a cargo exclusivo de los interesados y proponentes.

D. Comunicaciones. Las comunicaciones en el marco del Proceso de Contratación deben hacerse a través de la plataforma del SECOP II, de acuerdo a lo establecido en el cronograma.

La comunicación debe contener: (a) el número del presente Proceso de Contratación; (b) los datos del remitente que incluyen nombre, dirección física, dirección electrónica y teléfono; (c) identificación de los anexos presentados con la comunicación.

Las comunicaciones y solicitudes enviadas por canales distintos a los mencionados no serán tenidas en cuenta para los propósitos del Proceso de Contratación.

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

En el caso de documentos especializados, como por ejemplo, especificaciones o fichas técnicas, que en el mercado sean de amplia utilización y aceptación en idioma distinto al castellano, los proponentes deben aportar dichos documentos en su lengua original acompañados de una traducción simple al castellano.

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

Para efectos del trámite de apostilla y/o legalización de documentos otorgados en el exterior se debe tener en cuenta lo establecido en la Resolución No. 10547 del 14 de diciembre de 2018, “Por la cual se adopta el procedimiento para apostillar y/o legalizar documentos”, expedida por el Ministerio de Relaciones Exteriores de la República de Colombia.

Las Entidades Estatales solamente pueden exigir la legalización de acuerdo con la Convención de la Apostilla o la legalización de documentos públicos otorgados en el extranjero. Este tipo de legalización no es procedente para los documentos privados.

Cuando en un Proceso de Contratación un proponente presenta un documento público legalizado de acuerdo con la Convención de la Apostilla, la Entidad Estatal no debe solicitar legalizaciones, autenticaciones o ratificaciones adicionales de ninguna autoridad nacional o extranjera, puesto que el trámite de la Apostilla es suficiente para certificar por sí mismo la autenticidad.

De acuerdo con el Manual para el Funcionamiento Práctico de la Convención de la Apostilla, el país de origen del documento puede tener una autoridad que verifica y certifica ciertos documentos públicos (autoridad intermedia) y otra autoridad centralizadora que es quien emite la Apostilla. En consecuencia, las Entidades Estatales deben aceptar la Apostilla expedida por la autoridad centralizadora correspondiente.

G. Moneda. Los Proponentes deben presentar sus ofertas en pesos colombianos. Los valores de los documentos aportados en la propuesta deberán ser presentados en pesos colombianos.

Cuando un valor esté expresado en monedas extranjeras este deberá convertirse a pesos colombianos, teniendo en cuenta lo siguiente: **I.** Si los valores de un contrato están expresados originalmente en Dólares de los Estados Unidos de América, los valores se convertirán a pesos colombianos, utilizando para ello el valor correspondiente al promedio entre la TRM de la fecha de inicio del contrato y la TRM de la fecha de terminación del contrato. Para esto el Proponente deberá indicar la tasa representativa del mercado utilizada para la conversión de cada contrato en la Matriz No. 1 – Experiencia; la TRM utilizada deberá ser la certificada por la Superintendencia Financiera de Colombia. **II.** Si los valores del contrato están expresados originalmente en una moneda diferente a Dólares de los Estados Unidos de América, estos deberán convertirse inicialmente a esta moneda, utilizando para ello el valor correspondiente al promedio entre la tasa de cambio de la fecha de inicio del contrato y la tasa de cambio de la fecha de terminación del contrato. Para tales efectos, se deberá utilizar la información certificada por el Banco de la República. [Para el cálculo se recomienda acudir al siguiente link: https://www.oanda.com/lang/es/currency/converter/] Hecho esto, se procederá en la forma señalada en el numeral anterior. **III**. Si los valores de los estados financieros están expresados originalmente en Dólares de los Estados Unidos de América, el Proponente y la Entidad tendrán en cuenta la tasa representativa del mercado vigente certificada por la Superintendencia Financiera de Colombia de la fecha de expedición de los estados financieros. **IV.** Si los valores de los Estados Financieros están expresados originalmente en una moneda diferente a US$, estos deberán convertirse inicialmente a Dólares de los Estados Unidos de América utilizando para ello el valor correspondiente a la fecha de expedición de los estados financieros. Para verificar la tasa de cambio entre la moneda y el US$, el Proponente deberá utilizar la página web https://www.oanda.com/lang/es/currency/converter/. Hecho esto, se procederá en la forma señalada en el numeral III.

H. Conversión a Salarios Mínimos Mensuales Legales Vigentes (SMMLV). Cuando los Documentos del Proceso señalen que un valor debe expresarse en Salarios Mínimos Mensuales Legales Vigentes (SMMLV) deberá seguirse el siguiente proceso: **I.** Los valores convertidos a pesos colombianos, aplicando el proceso descrito anteriormente, o cuya moneda de origen sea el peso deberán ser convertidos a SMMLV, para lo cual se deberán emplear los valores históricos de SMMLV señalados por el Banco de la República (http://www.banrep.gov.co/es/mercado-laboral/salarios), del año correspondiente a la fecha de terminación del contrato. **II.** En relación con los valores convertidos a SMMLV, se deberán aproximar a la unidad más próxima de la siguiente forma: hacia arriba para valores mayores o iguales a cero punto cinco (0.5) y hacia abajo para valores menores a cero punto cinco (0.5).

En caso de que el Proponente aporte certificaciones en las que no se indique el día, sino solamente el mes y el año se procederá así: Fecha (mes, año) de suscripción y/o inicio del contrato: se tendrá en cuenta el último día del mes que se encuentre señalado en la certificación. Fecha (mes, año) de terminación del contrato: se tendrá en cuenta el primer día del mes que se encuentre señalado en la certificación.

I. Modalidad del proceso de selección y su justificación. Teniendo en cuenta la naturaleza del objeto contractual, las circunstancias de la contratación y la cuantía del contrato a celebrar, se determina que la modalidad de selección que se debe adelantar es la de Licitación Pública, en virtud de lo consagrado en el artículo 2 de la Ley 1150 de 2007 que establece: *"(...) la escogencia del contratista se efectuará por regla general través de licitación pública, con las excepciones que se señalan en los numerales 2, 3 y 4 del presente artículo (...)"*

La no relación o enunciación de una cualquiera de las normas que rigen la materia no será excusa para que el proponente no cumpla con las obligaciones contenidas en ellas y por parte de la CVC, para no exigir su cumplimiento; así no aparezca transcrita en el Pliego de Condiciones o en el contrato.

J. Forma de adjudicación. La CVC realizará adjudicación total del proceso de contratación por Licitación Pública; por lo cual no se aceptarán ofertas parciales.

K. Acuerdos comerciales. Los Acuerdos Comerciales son tratados internacionales vigentes celebrados entre Estados, los cuales incluyen obligaciones y derechos en materia de compras públicas en los cuales existe como mínimo el compromiso de trato nacional para los proponentes, bienes y servicios del Estado con el que se firma el Acuerdo Comercial.

La CVC, debe cumplir en sus Procesos de Contratación con las obligaciones incluidas en los Acuerdos Comerciales. Cualquier proponente tiene el derecho a exigir el cumplimiento de los Acuerdos Comerciales cuando estos son aplicables a los Procesos de Contratación. Este también es un derecho de los proponentes frente a los Procesos de Contratación que adelantan los Estados con los cuales Colombia ha suscrito Acuerdos Comerciales.

La lista de Acuerdos Comerciales aplicables al Proceso de Contratación es la siguiente tabla:

Acuerdo Comercial		Entidad Estatal Cubierta	Presupuesto del Proceso de Contratación superior al umbral del Acuerdo Comercial	Excepción Aplicable al Proceso de Contratación	Proceso de Contratación cubierto por el Acuerdo Comercial
		Si/No	Si/No	Si/No	Si/No
Alianza Pacífico	Chile	NO	-	-	-
	México	NO	-	-	-
	Perú	NO	-	-	-
Canadá		NO	-	-	-
Chile		NO	-	-	-
Corea		NO	-	-	-
Costa Rica		NO	-	-	-
Estados AELC		NO	-	-	-
Estados Unidos		NO	-	-	-
México		SI	NO	NO	NO
Triángulo Norte	El Salvador	SI	SI	NO	SI
	Guatemala	SI	SI	NO	SI
	Honduras	NO	NO	NO	NO
Unión Europea		NO	-	-	-
Comunidad Andina		SI	-	-	SI

Acuerdos Comerciales aplicables en el Proceso de Contratación Fuente Colombia

Por lo anterior, existe la posibilidad de que en el proceso precontractual puedan participar nacionales de Salvador, Guatemala y miembros de la Comunidad Andina.

I. DEFINICIONES.

Las expresiones utilizadas en el presente Contrato con mayúscula inicial deben ser entendidas con el significado que se asigna a continuación. Los términos definidos son utilizados en singular y en plural de acuerdo con el contexto en el cual son utilizados. Otros términos utilizados con mayúscula inicial deben ser entendidos de acuerdo con la definición contenida en el Decreto 1082 de 2015 y de acuerdo al significado establecido en los pliegos de condiciones. Los términos no definidos en los documentos referenciados o en la presente cláusula, deben entenderse de acuerdo con su significado natural y obvio.

II. OBJETO A CONTRATAR.

Consiste en la: **"ADQUISICION, IMPLEMENTACIÓN Y SOPORTE TECNICO DE NIVEL 3 DE LICENCIAS ANTIVIRUS PARA LA CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA"**

la descripción técnica del objeto a contratar se encuentra en el Anexo No. 1 - Anexo Técnico del Proyecto Pliego de Condiciones.

A. Clasificación UNSPSC. El objeto del presente Proceso de Contratación está identificado en el Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC) con el cuarto nivel de ser posible o de lo contrario se clasificará en el tercer nivel, como se indica a continuación:

UNSPC	NOMBRE
43222500	Equipo de seguridad de red
43233200	Software de seguridad y protección
43232700	Software de aplicaciones de red
81111800	Servicios de sistemas y administración de componentes de sistemas
81112200	Mantenimiento y soporte de software

B. Valor Estimado del Contrato. El valor del presente proceso será el que resulte del ofertado por el proponente y evaluado por LA CVC incluido el impuesto del IVA; valor que incluye todos los gastos e impuestos en que el Contratista pueda incurrir para la legalización y la ejecución del objeto del contrato.

C. Presupuesto oficial y disponibilidad presupuestal. El presupuesto estimado asciende a la suma de CIENTO SESENTA Y UN MILLONES CUATROCIENTOS OCHENTA Y CINCO MIL CIENTO CINCUENTA Y SEIS PESOS MONEDA CORRIENTE ($161.485.156) incluido el impuesto del IVA y todos los costos directos e indirectos y demás impuestos, tasas y contribuciones a que hubiere lugar el cual se encuentra respaldado por el certificado de disponibilidad presupuestal No. 2832 expedido el 02 de diciembre de 2021 por el Coordinador del grupo de presupuesto.

El presente proceso para la publicación del proyecto pliego de condiciones se atempera a lo dispuesto en el Parágrafo del Art. 6 Ley 1882 del 2018, que dispone que no es obligatorio contar con disponibilidad presupuestal.

A Continuación, se resume la localización de los recursos que apalancan el proceso:

Localización de los recursos en el Presupuesto de la CVC:

FUNCIONAMIENTO Área: 0500300 - Oficina de Tecnologías de Información - TODAS LAS CUENCAS - VALLE DEL CAUCA Proceso 0720-Gestión de Tecnologías de Información y Telecomunicaciones Subproceso: 0940-Administración y Soporte de Infraestructura Tecnológica y de Telecomunicaciones VIGENCIA PRESUPUESTAL 2021					
Actividad	**Concepto**	**Fuente**	**Valor**	**IVA (19%)**	**Total**
005	Soporte, mantenimiento y actualización de sistemas de información.	1251- Excedentes financieros-rendimientos Financieros Imputación: 000072009400052115 Concepto de gasto: Honorarios	$22.608.963	$4.295.703	$26.904.666
		Imputación: 000072009400055189 Concepto de gasto: Paquetes de Software	$113.092.849	$21.487.641	$134.580.490
			$131.701.812	**$25.783.344**	**$161.485.156**

Forma de pago. Los pagos por concepto de entrega de bienes o servicios se realizarán de la siguiente manera:

No.	Valor	Descripción entrega
1	$134.580.490	Un pago contra entrega de los certificados de propiedad de las licencias Antivirus y XDR que hacen parte de esta contratación en el almacén general de la CVC, previa autorización del Supervisor del contrato
2	$26.904.666	Un pago a la entrega del acta de recibo a satisfacción de la implementación y puesta en marcha de los elementos de antivirus y XDR y el cumplimiento de las obligaciones del contratista con respecto a los servicios, previa autorización del Supervisor del contrato

El Contratista deberá presentar certificación emitida por el Revisor Fiscal o Representante legal según el caso, en donde conste que la firma se encuentra al día en el pago de salarios, pago de aportes a sus empleados a los sistemas generales de seguridad social, (Salud, Pensión y Riesgos Profesionales) y aportes parafiscales (Cajas de Compensación Familiar, SENA, ICBF, subsidio familiar y subsidio de transporte). De igual forma debe presentarse fotocopia SIMPLE, de la planilla de la totalidad de los operarios que laboran en la ejecución del presente objeto contractual.

Todo pago del contrato estará sujeto a la suscripción del acta de entrega y recibo a satisfacción por parte del supervisor y el contratista.

Las facturas que presente el CONTRATISTA para llevar a cabo cualquier cobro inherente al contrato, deben cumplir con todos los requisitos establecidos por la Dirección de Impuestos Nacionales de Colombia DIAN. En el evento que la CVC reporte cualquier novedad en dicho documento el CONTRATISTA tendrá la obligación de realizar las correcciones pertinentes a fin de dar continuidad al proceso de pago. No se realizarán pagos que no cumplan con el lleno de los requisitos legales.

La CVC efectuará Los reconocimientos o descuentos a que haya lugar proporcional al monto de cada factura. Si la factura no ha sido bien elaborada o si le faltan los documentos de soporte, el término para el pago sólo empezará a contarse desde la fecha en que quede corregida la factura o desde aquélla en que se haya aportado el último de los documentos. Todas las demoras que se presenten por estos conceptos serán responsabilidad del contratista, quien no tendrá por ello derecho al pago de intereses o compensación de ninguna naturaleza.

La CVC ha establecido el recibo de facturas de proveedores los primeros veinte (20) días calendario de cada mes. El contratista deberá radicar sus facturas teniendo en cuenta este término.

D. Plazo. El plazo de ejecución del presente es a partir de la firma del Acta de Inicio hasta el 31 de diciembre de 2021.

E. Lugar de ejecución. El presente tendrá como lugar de ejecución el Edificio Principal de la Corporación

MUNICIPIO	SEDE	DIRECCION	TIPO OFICINA
Cali	Sede Principal	Carrera 56 # 11 -36	Principal
Dagua	Pacifico Este	Calle 10 #12-60	DAR
Buenaventura	Pacifico Oeste	Cra 2A # 2-09. Edf. Raul Becerra Pisos 2 y 3	DAR
Palmira	Sur Oriente	Calle 32 #25-16	DAR
Buga	Centro Sur	Inst. de Piscicultura carretera a la Habana contiguo al Batallón Palacé	DAR
Tuluá	Centro Norte	Cra.27A #42-432	DAR
La Unión	Brut	Calle 16 #3-278	DAR
Cartago	Norte	Cra 4 #9-73 piso 4 Edif.Torre San Francisco	DAR

Sevilla	UGC Municipio de Sevilla	Carrera 48 No. 54 – 10 Barrio Siracusa	Subsede
Calima Darién	UGC Municipio Calima Darién	Calle 6 No 10 -01	Subsede
Ginebra	UGC Municipio Ginebra	Calle 9 No. 7SN – 120 – Centro Minero Aurifero	Subsede
Jamundí	Jamundí	Calle 10 No. 12 – 25 Piso 1	Subsede
Palmira	Aeropuerto Alfonso Bonilla Aragón	Antigua Oficina ICA por la Secretaria de Salud	Subsede
Palmira	San Emigdio	Vereda la Zapata Corregimiento Potrerillo Vereda San Emigdio	Subsede
Cremal	UGC Anchicayá Alto	Calle 10 # 6-37 Tel 2533245	Subsede
Riofrío	Dar Centro Sur	Carrera 9 - 402	Subsede
Yumbo	Dar Sur Occidente	Calle 2 No 3-22 Barrio Belalcázar	Subsede
Palmira	Vivero San Emigdio	Corregimiento: Potrerillo Vereda: San Emigdio (2) 6206600 Ext. 1307 Latitud: 03.54757N Longitud:076.20250W	Subsede

III. CONVOCATORIA LIMITADA A MIPYMES

De conformidad con lo establecido en el artículo 84 de la Ley 2069 de 2020 y concepto de Colombia Compra Eficiente: […], además de la perdida de fuerza ejecutoria del artículo 2.2.1.2.4.2.2. del Decreto 1082 de 2015, por la desaparición de su fundamento de derecho, se advierte una manifiesta oposición entre dicho enunciado normativo y el nuevo contenido del artículo 12 de la Ley 1150 de 2007, modificado por el artículo 34 de la Ley 2069 de 2020.

Ante esta esta contradicción, se debe aplicar la consecuencia jurídica prevista en el artículo 84 de la Ley 2069 de 2020, según la cual esta deroga "…*todas las disposiciones que le sean contrarias"*. Entonces, puede afirmarse que, además del decaimiento del artículo 2.2.1.2.4.2.2. del Decreto 1082 de 2015, debe entenderse derogado y mientras no sea reglamentado por el Gobierno Nacional, para el caso que nos ocupa**, la convocatoria no se limitará a MiPymes.**

CAPITULO II.

Corporación Autónoma Regional del Valle del Cauca

FASE DE PREPARACIÓN

A. Cronograma del proceso de Selección Abreviada de Menor Cuantía:

No.	ACTIVIDAD	DESDE	HASTA
1	Aviso de convocatoria pública, análisis del sector, estudio previo, proyecto de pliego de condiciones y demás documentos previos	30/11//2021	7/12/2021
2	Observaciones y comentarios al proyecto pliego de condiciones por los interesados.	1/12/2021	7/12/2021 hasta las 5:30 pm
3	Respuesta a observaciones y comentarios presentados al proyecto de pliego de condiciones.	1/12/2021	9/12/2021
4	Acto administrativo de apertura y Pliego de Condiciones Definitivo	9/12/2021	
5	Manifestación de interés en participar en el presente proceso	10/12/2021 hasta las 5:30 pm	
6	Si la entidad recibe más de diez propuestas, llevará a cabo sorteo, para seleccionar máximo diez oferentes	13/12/2021 8:30 a.m.	
7	Término para presentación de observaciones al pliego definitivo	9/12/2021	13/12/2021 5:30:pm
8	Término para respuestas a observaciones al pliego definitivo	14/12/2021	
9	Plazo máximo para expedir adendas	14/12/2021	
10	Plazo para presentar propuestas	9/12/2021	15/12/2021 5:00 pm.
11	Apertura de ofertas y elaboración acta de cierre	15/12/2021, a las 5:10 p.m	
12	Evaluación de propuestas por el Comité Evaluador	16/12/2021	
13	Publicación informe de evaluación	16/12/2021	21/12/2021
14	Presentación de observaciones al informe de evaluación	17/12/2021	21/12/2021 Hasta las 5:30 p.m.
15	Respuesta de observaciones al informe de evaluación	22/12/2021	
16	Publicación Acto Administrativo de adjudicación o de Declaratoria de Desierto	22/12/2021	

17	Fecha estimada para la firma del contrato	23/12/2021
18	Fecha estimada para la entrega de las garantías de ejecución del contrato	24/12/2021
19	Fecha estimada para la aprobación de las garantías o pólizas e inicio de ejecución del contrato	24/12/2021

B. Proyecto de pliego de condiciones y documentos soporte. En cumplimiento de lo dispuesto en el artículo 2.2.1.1.1.7.1 del Decreto 1082 de 2015, los estudios y documentos previos del presente proceso de contratación se publicarán en el SECOP II.

La publicación del proyecto de pliegos de condiciones no genera obligación para la CVC de dar apertura al proceso de selección, en virtud de ello, los posibles oferentes deberán examinar cuidadosamente tanto el proyecto como el pliego de condiciones del presente proceso y todos los documentos que hacen parte del mismo e informarse de todas las circunstancias que puedan afectar en alguna forma el objeto contractual, el valor o el plazo requerido para su cumplimiento.

De acuerdo con el principio de contradicción los interesados u oferentes pueden formular observaciones al contenido del proyecto pliego de condiciones durante el termino establecido en el cronograma del presente documento.

Todos los documentos del presente proceso pueden ser consultados a través de la plataforma del SECOP II.

C. Acto administrativo de apertura del proceso de selección y pliego de condiciones. La CVC ordenará la apertura del proceso de selección mediante acto administrativo de carácter general.

El Pliego de Condiciones comprende el objeto del contrato, su regulación jurídica, los derechos y obligaciones de las partes, la determinación y ponderación de los factores objetivos de selección y todas las demás circunstancias de tiempo, modo y lugar que se consideren necesarias para garantizar reglas justas, objetivas, claras y completas.

Todos los documentos del presente proceso pueden ser consultados a través de la plataforma del SECOP II.

D. Interpretación del pliego de condiciones y aclaraciones adicionales. Este Pliego de Condiciones debe ser interpretado como un todo y sus disposiciones no deben ser entendidas de manera separada de lo que indica su contexto general. Por lo tanto, se entiende integrada a este la información incluida en los documentos del proceso que lo acompañan y las adendas que posteriormente se expidan.

Los plazos en días establecidos en este pliego de condiciones, se entienden como días hábiles, salvo que de manera expresa, la ley o LA CVC indiquen que se trata de días calendario o meses.

Cuando el vencimiento de un plazo corresponda a un día no hábil o no laboral para LA CVC, este se trasladará al día hábil siguiente.

Las referencias a normas jurídicas incluyen las disposiciones que las modifiquen, adicionen, sustituyan o complementen.

Los proponentes u oferentes deberán examinar cuidadosamente todos los documentos de este proceso e informarse cabalmente de las condiciones técnicas, comerciales y contractuales, así como de todas las circunstancias que puedan afectar el trabajo, su costo y su tiempo de ejecución. El no hacerlo es de su exclusiva responsabilidad y entraña las consecuencias establecidas en el presente Pliego.

Si el proponente u oferente tiene dudas, encuentra discrepancias, ambigüedades, contradicciones u omisiones en cualquiera de los documentos del pliego de condiciones, incluidos los anexos, las adendas y los demás actos administrativos que se produzcan dentro de este proceso o requiere realizar una consulta, deberá pedir las correspondientes aclaraciones por escrito. LA CVC mediante adenda comunicará las aclaraciones, correcciones o adiciones a que haya lugar en los términos de ley.

El no recibir solicitudes de aclaración o consulta, por parte de los proponentes, dará a entender a LA CVC, que el proponente u oferente considera las reglas establecidas en el presente pliego como justas, claras y completas, permitiendo la confección de los ofrecimientos y asegurando la escogencia objetiva.

No se resolverán por parte de ningún funcionario de LA CVC, consultas efectuadas telefónicamente o en forma personal. Solo será tenida en cuenta en el presente proceso la información que la CVC suministre por escrito.

E. Modificación al pliego de condiciones. La CVC, puede modificar el pliego de condiciones mediante adendas, las cuales debe publicar en los días hábiles y horarios laborales de la Entidad, a más tardar el día hábil anterior al vencimiento del plazo para presentar ofertas a la hora fijada para tal presentación; salvo en la Licitación Pública, pues de conformidad con la Ley 1474 de 2011, la publicación de las adendas debe hacerse con tres (3) días de anticipación al día en que se tiene previsto el cierre del proceso de selección.

La CVC, puede expedir adendas para modificar el cronograma una vez vencido el término para la presentación de las ofertas, Art. 2.2.1.1.2.2.1 Decreto 1082 de 2015.

Las consultas y respuestas no suspenderán los términos para la presentación de las ofertas ni del proceso; sin embargo, si como resultado de las aclaraciones solicitadas fuese necesario modificar los plazos de la convocatoria pública o aclarar o modificar el pliego, esto se hará mediante adendas.

F. Procedimiento para presentar propuestas u ofertas. La oferta debe ser presentada conforme a los requisitos exigidos en el pliego electrónico y en el complemento al pliego, debidamente foliada y cargada en la plataforma del SECOP II conforme al cronograma.

Las propuestas serán abiertas el día y hora fijado en el cronograma y la plataforma del SECOP II reflejara las ofertas presentadas.

Aquellas propuestas u ofertas que estén mal dirigidas o que sean entregadas con posterioridad a la fecha y hora señaladas en el cronograma, no serán tenidas en cuenta en el proceso de selección, en los términos de la plataforma del SECOP II.

No se aceptarán ofertas enviadas vía fax, correo electrónico o a través de medios diferentes al aquí establecido.

G. Retiro y/o modificación de propuestas. Si un proponente desea retirar o modificar su propuesta, debe hacerlo en los términos establecidos por la plataforma del SECOP II.

El oferente puede retirar su oferta sin necesidad de solicitarlo a la CVC, sino realizando tramite de manera directa en la plataforma del SECOP II.

H. Ofertas Parciales. Los proponentes no pueden presentar propuestas parciales, es decir, que deben ofrecer todos los bienes y servicios requeridos en el presente pliego.

I. Ofertas condicionadas. No podrán señalarse condiciones diferentes a las establecidas en este Pliego de condiciones. En caso de que la propuesta formule condiciones diferentes a las establecidas, se rechazará la oferta respectiva.

J. Plazo de validez de las ofertas. El término de validez de la propuesta deberá tener un término igual al de la vigencia de la garantía de seriedad del ofrecimiento, esto es, treinta (30) DÍAS, contados a partir del momento de presentación de la oferta, período dentro del cual los precios permanecerán firmes y fijos.

K. Confidencialidad de la propuesta. Los oferentes deberán indicar en su oferta, cuáles de los documentos aportados son de carácter reservado e invocar las normas que ampara dicha reserva, para así dar cumplimiento a lo estipulado en el numeral 4 del artículo 24 de la Ley 80 de 1993. Si el oferente no hace pronunciamiento expreso amparado en la ley, se entenderá que toda la oferta es pública.

En caso contrario, con la presentación de la oferta se entiende y se acepta por parte del oferente que la Entidad no asume ninguna responsabilidad por entregar copias de los documentos de la oferta sobre los cuales no se acredite dicha reserva legal a quien demuestre interés legítimo y en todo caso, la Entidad se reserva el derecho a revelar dicha información a sus funcionarios y asesores externos, con el fin de verificar y evaluar la propuesta.

L. Confidencialidad de la información relacionada con datos sensibles. 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 I y 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 11- Autorización para el tratamiento de datos personales» como requisito para el otorgamiento del criterio de desempate.

M. Adjudicación con oferta única. La CVC puede adjudicar el contrato cuando solo se haya presentado una (01) oferta siempre que cumpla con los requisitos habilitantes exigidos y satisfaga los requisitos de calificación que otorga puntaje del pliego de condiciones.

N. Una propuesta por proponente. Cada proponente deberá presentar solamente una (01) propuesta, ya sea por si solo o como integrante de una forma de asociación permitida por la ley. El proponente no podrá ser parte de otra propuesta que se haya presentado en forma individual o conjunta de manera simultánea en el presente proceso, de presentarse dicha situación, prevalecerá la oferta que haya sido radicada primero en el tiempo.

O. Inhabilidades e incompatibilidades para contratar. Podrán participar en la presente Licitación Pública, las personas naturales o jurídicas que no se encuentren dentro de las causales de inhabilidad e incompatibilidad de que trata el artículo 8, Ley 80 de 1993, modificado por los artículos 1, 2 y 4 de la Ley 1474 de 2011, y habrá lugar a lo dispuesto en el artículo 9 de la precitada ley, sobre inhabilidades e incompatibilidades sobrevinientes, si fuere del caso.

De igual manera se dará aplicación a lo dispuesto en el artículo 5 de la Ley 1474 de 2011 y en la ejecución de los contratos, la CVC y el CONTRATISTA deberán observar lo dispuesto en los artículos 90 a 95 de la Ley 418 de 1997 y las normas que los modifiquen, adicionen o subroguen.

P. Acta de cierre del proceso. Se entienden recibidas las ofertas que a la fecha y hora indicada en el cronograma del proceso de contratación se encuentren radicadas virtualmente en la plataforma del SECOP II.

Vencido el termino para presentar ofertas se procede a la apertura. 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.

Las ofertas será responsabilidad del área a cargo del proceso de selección. El acta de cierre será suscrita por los funcionarios que participaron en el acto público y por los proponentes y veedores que asistan al cierre.

Sin embargo, cuando se presente una indisponibilidad del SECOP II, la cual ha sido confirmada por 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.

CAPITULO III.
REQUISITOS HABILITANTES PARA LA PARTICIPACION EN EL PROCESO DE SELECCIÓN

De conformidad con lo previsto en la Ley 1150 de 2007, los proponentes deberán presentar los documentos que a continuación se relacionan, con el propósito de que la propuesta sea hábil.

A. Requisitos de carácter jurídico.

1. Carta de presentación de la propuesta. Con la presentación de este Anexo debidamente firmado por el proponente o por el representante legal de la sociedad, consorcio o unión temporal o por el apoderado constituido para el efecto, se entiende que expresamente acepta el contexto del Pliego de Condiciones, sus anexos, formatos, formularios y matrices. (formato No. 1).

2. Poder. Cuando el proponente actúa mediante apoderado, debe presentar el poder especial debidamente autenticado para presentar la propuesta y firmar el contrato respectivo, si es el caso.

3. Fotocopia de la libreta militar. Del representante legal o del proponente, tratándose de varones menores de 50 años de nacionalidad colombiana en los términos de la Ley 48 de 1998.

4. Existencia y representación legal. La existencia y representación legal de los proponentes individuales o miembros de los proponentes plurales se acreditará de acuerdo con las siguientes reglas.

4.1. Personas naturales: Debe presentar los siguientes documentos en copia simple

- De nacionalidad Colombiana: Cédula de Ciudadanía
- Extranjera con residencia en Colombia: Cedula de Extranjería vigente expedida por autoridad competente
- Extranjera sin domicilio en Colombia: Pasaporte

4.2. Personas jurídicas: Debe presentar los siguientes documentos en copia simple

- **Nacional o extranjera con sucursal en Colombia:**

Las personas naturales o jurídicas nacionales o extranjeros con domicilio o sucursal en Colombia deberán presentar el certificado de existencia y representación legal, expedido por la Cámara de Comercio de su jurisdicción dentro de los treinta (30) días calendario anteriores a la fecha límite de recepción de propuestas del presente proceso de selección, donde conste que la existencia es de quince (15) años, que el objeto social y la actividad mercantil guardan relación con el del presente proceso de selección, además debe contar con la capacidad jurídica para celebrar y ejecutar contratos relacionados con el objeto de este proceso y acreditar que su duración abarca como mínimo un (1) año a partir de la fecha de terminación del plazo de ejecución del contrato que se suscriba. Para el caso de consorcios y uniones temporales cada miembro deberá aportar el certificado de existencia y representación legal y cumplir con las exigencias de existencia antes establecidas.

Si del Certificado de existencia expedido por la cámara de comercio o de los estatutos de la sociedad se desprende que las facultades de representante legal están limitadas por razón de la naturaleza o cuantía del negocio jurídico, el oferente deberá presentar el acta respectiva en la cual se autoriza al representante legal para firmar la propuesta y celebrar el correspondiente contrato en caso de que le sea adjudicado, y para constituir el consorcio o la unión temporal si a ello hubiere lugar, incluyendo el valor y objeto de esta selección.

1. Certificado de Existencia y Representación Legal expedido por la Cámara de Comercio o autoridad competente, en el que se verificará:

i) Fecha de expedición del certificado no mayor a treinta (30) días calendarios anteriores a la fecha se 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 fecha originalmente establecida en el Pliego de Condiciones Definitivo.
ii) Que el objeto social de la sociedad permita desarrollar las actividades descritas en el objeto del presente proceso de contratación.
iii) Que la vigencia de la persona jurídica natural o extranjera no sea inferior a la del plazo del contrato y no menor a 15 años según el requisito de experiencia y un (1) año adicional. Para efectos de la evaluación, este plazo será contado a partir de la fecha de cierre del proceso de contratación.
iv) 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 parte del órgano social competente respectivo, para cada caso.
v) El nombramiento del revisor fiscal en caso de que exista.
vi) Que las personas jurídicas extranjeras con actividades permanentes en la República de Colombia (Contratos de obra o Servicios) deberán estar legalmente establecidas en el territorio nacional, de acuerdo con lo establecido en los artículos 471 y 474 del Código de Comercio.

2. Certificación del Revisor Fiscal en caso de ser Sociedad Anónima Colombiana en la que conste si es abierta o cerrada.

3. 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 y Certificado de Existencia y Representación Legal con fecha de expedición máximo de 30 días calendario, antes de la fecha de cierre del proceso de selección.

Cuando el Representante Legal de la sucursal tenga restricciones para contraer obligaciones, deberá acreditar autorización suficiente del órgano competente 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.

- **Extranjera sin sucursal o domicilio en Colombia:**

  1. Documentos que acrediten la existencia y representación legal de la sociedad extranjera, presentados de conformidad con lo establecido en el presente pliego de condiciones, en el que debe constar como mínimo lo siguiente:

  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 presente proceso de contratación.
  iv) Facultades del representante legal o de la persona facultada 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 respectivo para cada caso.
  v) Tipo, número y fecha del documento de constitución o creación.
  vi) Fecha y clase de documento con el cual se reconoce la personería jurídica.
  vii) Vigencia de la persona jurídica no inferior al plazo del contrato y no inferior a 15 años según lo señalado en el requisito de experiencia y un (1) año adicional. Para efectos de la evaluación, este plazo será contado a partir de la fecha de cierre del proceso de contratación.
  viii) Fotocopia del documento de identificación del representante legal.

- **Entidades Estatales art. 2 Ley 80 de 1993:** Deben presentar los siguientes documentos para acreditar su existencia.

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

4.3. Proponentes Plurales: Debe presentar los siguientes documentos en copia simple

a. Acreditar la existencia del proponente plural y clasificarlo de forma clara en Unión Temporal o Consorcio. En este documento los integrantes deben expresar claramente su intención de conformar el proponente plural, en el caso de que no exista claridad sobre el tipo de asociación se solicitará la aclaración. Los proponentes deberán incluir como mínimo la información contenida en el Formato No. 2 A - Consorcio y 2 B – Unión Temporal. Los proponentes podrán incluir información adicional que no contradiga lo dispuesto en los documentos del proceso.

b. Acreditar el nombramiento de un representante y un suplente cuya intervención deberá quedar definida en los anexos anteriormente mencionados Formato No. 2 A - Consorcio y 2 B – Unión Temporal, de todas las personas naturales y/o jurídicas asociadas, con facultades suficientes para la representación sin limitaciones de todos y cada uno de los integrantes, en todos los aspectos que se requieran para la

presentación de la oferta, para la suscripción y ejecución del contrato, así como también la facultad para firmar el acta de terminación y liquidación.

c. Aportar fotocopia de la cédula de ciudadanía del representante principal y suplente de la estructura plural.

d. Acreditar que la vigencia de la estructura plural no sea inferior a la del plazo del contrato y un (1) año adicional. Para efectos de la evaluación, este plazo será contado a partir de la fecha de cierre del proceso de contratación.

e. El proponente plural debe señalar expresamente cual es el porcentaje de participación de cada uno de sus miembros. La sumatoria del porcentaje de participación 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.

Dicho documento debe estar firmado por todos y cada uno de los integrantes del proponente plural y en el caso del integrante persona jurídica, por el representante legal de dicha Entidad o por el apoderado de cualquiera de las anteriores.

5. Certificación de pago de seguridad social y aportes legales.

5.1. Personas jurídicas: El proponente persona jurídica debe presentar el formato No. 6-B 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 conste el pago de los aportes de sus empleados a los sistemas de salud, riesgos profesionales, pensiones y aportes a las cajas de compensación familiar, al instituto Colombiano de Bienestar Familiar y al Servicio Nacional de Aprendizaje.

La CVC 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 este exonerada, debe indicarlo en el anexo.

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

5.2. 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. El proponente podrá acreditar la afiliación entregando el certificado de pago de planilla, pero no será obligatoria su presentación. formato No. 6-A

Los certificados de afiliación se deben presentar con fecha de expiración no mayor a treinta (30) días calendarios, 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 de los certificados de afiliación, la fecha originalmente establecida en el pliego de condiciones definitivo.

La persona natural que reúna los requisitos para acceder a la pensión de vejez, o se pensione por invalidez o anticipadamente, presentara 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.

5.3. **Proponentes plurales:** Cada uno de los integrantes del proponente plural debe suscribir por separado la declaración de la que trata los anteriores numerales

6. Certificado del registro único tributario RUT. De conformidad con los Decretos 2788, 3426, 4243 de 2004, el proponente deberá adjuntar el Registro Único Tributario a cargo de la Dirección de Impuestos y Aduanas Nacionales - DIAN del Ministerio de Hacienda y Crédito Público.

En caso de salir favorecido con la adjudicación del contrato, el proponente plural, consorcio o unión temporal deberá presentar el RUT a nombre del consorcio o unión temporal.

7. Garantía de seriedad de la oferta. De conformidad con lo establecido en el Decreto 1082 de 2015, el proponente deberá constituir una garantía de seriedad de la oferta, expedida por compañía de seguros legalmente autorizada y establecida en Colombia, a favor de la CVC, por un valor del **DIEZ POR CIENTO (10%) DEL VALOR DE LA OFERTA** para el presente proceso, con una vigencia de **TREINTA (30) DIAS,** contados a partir de la fecha de presentación de la oferta y hasta la aprobación de la garantía de cumplimiento del contrato.

La no entrega de la Garantía de Seriedad junto con la propuesta no será subsanable y será causal de rechazo de la misma.

La garantía de seriedad de la oferta está destinada a afianzar el compromiso del proponente, de que, en caso de adjudicársele el contrato, lo formalizará en los términos y plazos prescritos en el presente pliego de condiciones.

Cuando la oferta sea presentada por un consorcio o unión temporal, la póliza de garantía debe ser tomada a nombre de todos sus integrantes tal como aparecen en el documento que acredita la existencia y representación legal, de cada uno de ellos y NO a nombre del Consorcio o Unión Temporal.

Cuando la póliza de seguros no cuente con los requerimientos del pliego de condiciones, el oferente deberá remitir las modificaciones del caso, dentro del término preclusivo y perentorio que para el efecto señala la norma, so pena del rechazo de la propuesta.

8. Verificación responsables fiscales, antecedentes disciplinarios Sistema Registro Nacional de Medidas Correctivas RNMC de la Policía Nacional de Colombia como infractor de la Ley 1801 de 2016. La CVC se reserva el derecho de verificar si aparece inhabilitado para contratar en el Sistema de Información de Registro de Sanciones y Causas de Inhabilidad "SIRI' de la Procuraduría General de la Nación y si aparece en el Sistema de Registro Nacional de Medidas Correctivas RNMC de la Policía Nacional de Colombia como infractor de la Ley 1801 de 2016.

B. Requisitos de Carácter Financiero y Organizacional.

Los proponentes deberán presentar el Certificado de Registro Único de Proponentes - **RUP** en el cual se evidencie la información financiera de la empresa (Indicadores financieros y de capacidad organizacional) de los últimos tres (3) años fiscales – 2018, 2019 y 2020 – o si no posee la antigüedad suficiente para acreditar la información financiera de este periodo, se tendrá en cuenta la que certifique el RUP desde su primer cierre fiscal; teniendo en cuenta que dicha información deberá estar VIGENTE Y EN FIRME.

En todo caso se evaluará la información que se encuentre vigente y en firme en el RUP que corresponda al mejor año fiscal o que el proponente determine que desee ser tomada en consideración para la validación del cumplimiento de su capacidad financiera y organizacional.

Vale aclarar que se evaluará la información financiera completa del año fiscal elegido (el mejor) y no fraccionada en los diferentes periodos certificados en el RUP. Así las cosas, no podrán tomarse en consideración algunos indicadores del año 2018, por ejemplo, y otros del año 2019 o del año 2020.

ANÁLISIS Y EVALUACIÓN DE LA CAPACIDAD FINANCIERA

Con base en los documentos solicitados, se procederá a efectuar la ponderación del factor habilitador de la capacidad financiera según los indicadores que a continuación se describen, teniendo en cuenta que serán habilitados solo aquellos proponentes que cumplan con el nivel requerido en todos y cada uno de ellos, los cuales se calcularán y evaluarán con dos cifras decimales:

I. Índice de Liquidez

Mide la capacidad de la empresa para cancelar las obligaciones a corto plazo y se calcula por la relación de Activo Corriente sobre Pasivo Corriente, así:

$$\text{Razon Corriente} = \frac{\text{Activo Corriente}}{\text{Pasivo Corriente}}$$

Se tendrán en cuenta las propuestas que demuestren un índice de liquidez igual o superior a dos 2 veces.

II. Índice de Endeudamiento

Determina el grado de endeudamiento en la estructura de financiación (Pasivo y Patrimonio) del proponente y se calcula por la relación del pasivo total sobre activo total, así:

$$\text{Índice de endeudamiento} = \frac{\text{Pasivo Total}}{\text{Activo Total}}$$

Se tendrán en cuenta las propuestas que presenten un Índice de Endeudamiento igual o inferior al sesenta por ciento (<=60%).

III. Razón Cobertura de Intereses

Indica la capacidad o limitación del proponente para cumplir con sus obligaciones financieras, y se calcula por la razón Utilidad Operacional sobre Gastos de Intereses:

$$\text{Cobertura de Intereses} = \frac{\text{Utilidad Operacional}}{\text{Gastos de Intereses}}$$

Se tendrán en cuenta las propuestas que demuestren un índice igual o superior a uno (>=1).

En los casos en que el proponente no tenga obligaciones financieras y por tanto no registre Gastos de Intereses será habilitado en este Indicador, siempre y cuando la Utilidad Operacional sea mayor a cero.

IV. Capital de Trabajo

Representa la liquidez operativa del proponente, es decir el remanente del proponente luego de liquidar sus activos corrientes (convertirlos en efectivo) y pagar el pasivo de corto plazo. Y se calcula mediante la diferencia entre el Activo corriente y el Pasivo Corriente.

$$\text{Capital de Trabajo} = \text{Activo corriente} - \text{Pasivo corriente}.$$

Se tendrán en cuenta las propuestas que demuestren un capital de trabajo mayor o igual al cien por ciento del presupuesto del presente proceso (>=100%).

a. Evaluación de la capacidad organizacional

Serán habilitados solo aquellos proponentes que cumplan con el nivel requerido en los siguientes indicadores:

I. Rentabilidad del Patrimonio: Mide la capacidad de generación de utilidad operacional de cada peso invertido en el Patrimonio.

$$\text{Rentabilidad sobre Patrimonio} = \frac{\text{Utilidad Operacional}}{\text{Patrimonio}}$$

Se tendrán en cuenta las propuestas que demuestren un índice superior a 10% (>=0,10).

II. Rentabilidad sobre Activos: Mide la capacidad de generación de utilidad operacional de cada peso invertido en el Activo:

$$\text{Rentabilidad sobre Activo} = \frac{\text{Utilidad Operacional}}{\text{Activo Total}}$$

Se tendrán en cuenta las propuestas que demuestren un índice igual o superior a 5% (>=0,05).

Proponentes Plurales: Para el caso de oferentes plurales, todos los integrantes de un Consorcio o Unión Temporal deben presentar la Documentación requerida (RUP) y tener en cuenta a efectos de acreditar el cumplimiento de los indicadores financieros y de capacidad organizacional el siguiente procedimiento:

Para el caso de propuestas presentadas por **Consorcios** se aplicará la fórmula de *Suma de los componentes de los indicadores* (*fórmula 2. Manual de Colombia Compra Eficiente*), y consiste en sumar las partidas que componen el numerador del indicador de todos los consorciados y dividirla por la sumatoria de las partidas que componen el denominador del mismo.

$$(iii)\ Indicador = \frac{\left(\sum_{i=1}^{n} Componente\ 1\ del\ indicador_i\right)}{\left(\sum_{i=1}^{n} Componente\ 2\ del\ indicador_i\right)}$$

Para el caso de propuestas presentadas por **Uniones Temporales**, se aplicará la fórmula de *Ponderación de los componentes de los indicadores* (*fórmula 1. Manual de Colombia Compra Eficiente*) y consiste en hallar la sumatoria del producto de cada componente del numerador del indicador por el porcentaje de participación de cada miembro de la UT y dividirla por la sumatoria del producto de cada componente del denominador del indicador por el porcentaje de participación de cada miembro de la UT.

$$(ii)\ Indicador = \frac{\left(\sum_{i=1}^{n} Componente\ 1\ del\ indicador_i \times porcentaje\ de\ participación_i\right)}{\left(\sum_{i=1}^{n} Componente\ 2\ del\ indicador_i \times porcentaje\ de\ participación_i\right)}$$

En el caso particular de la Cobertura de Intereses cuando el resultado del indicador es INDETERMINADO para alguno de los miembros de un consorcio o unión temporal, el Indicador final del proponente se determinará igualmente a partir de la aplicación de la fórmula correspondiente. En caso que este indicador sea INDETERMINADO para todos los integrantes del proponente plural, se considerará que el proponente CUMPLE con este requisito solo si TODOS demuestran poseer Resultado Operacional Positivo, en caso contrario será inhabilitado.

Para los indicadores cuyo resultado corresponde a un valor absoluto, se aplicará la sumatoria de los indicadores de los integrantes del Consorcio o Unión Temporal, para determinar el Indicador final del proponente.

Proponentes Extranjeros sin Domicilio en Colombia. Para el caso de empresas extranjeras sin domicilio o sucursal en Colombia y que por tanto no están inscritas en el RUP, estas deberán presentar los Estados Financieros Básicos – Balance General y Estado de Resultados – a la fecha de corte anual más reciente según el periodo fiscal vigente en sus respectivos países de origen o en sus estatutos sociales; suscritos por el Representante Legal y el Revisor Fiscal o Auditor del Proponente o por su Contador según sea el caso; expresados en su lengua original y en la moneda legal del país en el cual son emitidos; adicionalmente deberán presentarse traducidos al castellano y en pesos colombianos, para lo cual se deberá haber tenido en cuenta la tasa representativa del mercado TRM vigente a la fecha de

expedición de los mismos, la cual es certificada por la Superintendencia Financiera de Colombia.

En los casos en que una empresa extranjera no inscrita en el RUP por las razones antes expuestas, sea integrante de un Consorcio o Unión Temporal, se aplicará el mismo procedimiento definido para los PROPONENTES PLURALES descrito anteriormente para validar el cumplimiento de los Requisitos Habilitantes.

C. Experiencia.

De acuerdo con lo establecido con el artículo 6 de la Ley 1150 de 2007 y en el Decreto 1082 de 2015, la experiencia se verificará con el RUP, el cual debe encontrarse actualizado y en firme. El Registro Único de Proponentes debe haber sido expedido por la Cámara de Comercio de su jurisdicción dentro de los treinta (30) días calendario anteriores a la fecha límite de recepción de propuestas del presente proceso de selección.

1. <u>Del proponente</u>

- **Proponentes nacionales o extranjeros con domicilio o sucursal en Colombia.**

Se requiere que el proponente acredite su experiencia con un (1) contrato, ejecutado y terminado a entera satisfacción en los últimos cinco (5) años, celebrado con entidades públicas o privadas, identificado con todos los códigos UNSPSC solicitados en la siguiente tabla, cuyo valor sea igual o superior al 100% del presupuesto oficial de este proceso, expresado en SMMLV, lo que se certificará con el RUP, actualizado y en firme.
La clasificación de Bienes y Servicios debe ser de acuerdo con la siguiente tabla:

Clasificación UNSPSC	Segmento	Familia	Clase
43222500	Difusión de Tecnologías de Información y Telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipo de seguridad de red
43232700	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de aplicaciones de red
43233200	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de seguridad y protección
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

Adicionalmente, por especialidad del objeto a contratar y porque se necesita garantizar amplia experiencia, el proponente debe acreditar que el contrato que presenta tenga como objeto o alcance, la venta e implementación de una cantidad igual o mayor a 836 licencias antivirus.

La acreditación debe realizarse mediante certificaciones; actas de recibo final a satisfacción o actas de liquidación, en las cuales se pueda validar la información solicitada no contenida en el RUP; estos documentos deben contener como mínimo lo siguiente:

- Haber sido suscritos por el representante legal de la entidad contratante o por el director del área técnica encargada o por el funcionario delegado para tal fin.
- Nombre del Contratista
- Número telefónico
- Correo electrónico
- Número y objeto del contrato,
- Actividades ejecutadas,
- Valor ejecutado,
- Plazo de ejecución,
- Fechas de iniciación y de terminación,
- Porcentaje de participación si el contrato fue ejecutado en Consorcio o Unión Temporal,
- Indicar que fue recibido a satisfacción

La experiencia del oferente plural (unión temporal, consorcio o promesa de sociedad futura) corresponde a la suma de la experiencia que acredite cada uno de los integrantes de éste, afectada por el porcentaje de participación, cada integrante debe aportar a la experiencia solicitada.

La CVC se reserva el derecho de verificar por sus propios medios, la veracidad de la información que a través del diligenciamiento de los presentes documentos haga cada proponente o miembro de un consorcio o unión temporal.

Cuando un proponente adquiere experiencia en un contrato como integrante de un contratista plural, la experiencia derivada de ese contrato corresponde a la ponderación del valor del contrato por el porcentaje de participación.

Para el caso de consorcios y uniones temporales cada miembro deberá acreditar su inscripción en el RUP con el clasificador de bienes y servicios identificados con todos los siguientes códigos: 43222500, 43232700, 43233200, 81111800, 81112200.

- **Proponentes extranjeros sin domicilio o sucursal en Colombia.**

Se requiere que el proponente presente:

- Un (1) contrato ejecutado y terminado a entera satisfacción en los últimos cinco (5) años, celebrados con entidades públicas o privadas;
- Las actividades de dichos contratos deberán estar enmarcadas en todos los servicios de:
    - Equipo de seguridad de red
    - Software de seguridad y protección
    - Servicios de sistemas y administración de componentes de sistemas
    - Mantenimiento y soporte de software

Cuyo objeto o alcance sea a compra e implementación de una cantidad igual o mayor a 836 licencias de antivirus. El valor del contrato aportado debe ser por un valor igual o superior al cien por ciento (100%) del presupuesto oficial del presente proceso, expresado en SMMLV.

La experiencia del oferente plural, consorcio o unión temporal, corresponde a la suma de los contratos que acrediten el número y valor solicitado.
Para el caso de consorcios y uniones temporales cada miembro deberá acreditar que tiene el clasificador de bienes y servicios identificados con todos los siguientes códigos: 43222500, 43232700, 43233200, 81111800, 81112200.

La acreditación debe realizarse mediante certificaciones; actas de recibo final a satisfacción o actas de liquidación, en las cuales se pueda validar la información solicitada; estos documentos deben contener como mínimo lo siguiente:

- \- Haber sido suscritos por el representante legal de la entidad contratante o por el director del área técnica encargada o por el funcionario delegado para tal fin.
- Nombre del Contratista
- Número telefónico
- Correo electrónico
- Número y objeto del contrato,
- Actividades ejecutadas,
- Valor ejecutado,
- Plazo de ejecución,
- Fechas de iniciación y de terminación,
- Porcentaje de participación si el contrato fue ejecutado en Consorcio o Unión Temporal,

Indicar que fue recibido a satisfacción

La experiencia del oferente plural (unión temporal, consorcio o promesa de sociedad futura) corresponde a la suma de la experiencia que acredite cada uno de los integrantes de éste, afectada por el porcentaje de participación, cada integrante debe aportar a la experiencia solicitada.

La experiencia del oferente plural (unión temporal, consorcio o promesa de sociedad futura) corresponde a la suma de la experiencia que acredite cada uno de los integrantes de éste, afectada por el porcentaje de participación.

La CVC se reserva el derecho de verificar por sus propios medios, la veracidad de la información que a través del diligenciamiento de los presentes documentos haga cada proponente o miembro de un consorcio o unión temporal.

Cuando un proponente adquiere experiencia en un contrato como integrante de un contratista plural, la experiencia derivada de ese contrato corresponde a la ponderación del valor del contrato por el porcentaje de participación.

Tabla de Salarios Mínimos Mensuales Legales Vigentes (SMMLV): Para la sumatoria de los valores de los contratos a presentar como experiencia, se debe tener en cuenta que los contratos se sumarán en salarios mínimos legales mensuales vigentes del año en el cual se dio término a la ejecución del contrato, para lo cual se muestran valores de referencia en la siguiente tabla:

Ene-14	$ 616.000
Ene-15	$ 644.350
Ene-16	$ 689.454
Ene-17	$ 737.717
Ene-18	$781.242
Ene-19	$828.116
Ene-20	$877.803
Ene-21	$908.526

2. <u>Certificación de Fabricante</u>. El oferente deberá presentar un documento emitido directamente por el fabricante de la solución ofertada, donde certifique estar registrado en su programa de canales/partners y donde certifique mínimo 5 años de estar dentro de los tres más altos niveles de canal/partner, y que cuenta con capacidad para: comercializar e implementar las soluciones de dicho fabricante en el territorio colombiano.

No se aceptarán certificaciones emitidas por mayoristas, distribuidores u otro tercero diferente al fabricante. Dichas certificaciones deberán contar con fecha de expedición no mayor a 60 días anteriores a la fecha de presentación de la oferta.

3. <u>Personal mínimo requerido</u>

Se requiere que el proponente certifique en la carta presentación de la Propuesta, la experiencia del equipo de trabajo según los perfiles profesionales de cada integrante, sus respectivos soportes y demás documentos legales que así lo acrediten dando cumplimiento a la siguiente información requerida por la Corporación:

Experiencia del Equipo de Trabajo:

El proponente deberá disponer del siguiente equipo de Trabajo y acreditar su experiencia, así:

Un (1) Gerente de Proyectos: Ingeniero Industrial, Electrónico, Sistemas o Telemático, para desarrollar la planeación y ejecución de las fases del proyecto:

- Experiencia general mínima de cinco (5) años contados a partir de la finalización de las materias
- Experiencia específica mínima de cinco (5) años ejerciendo cargos relacionados con funciones de gerencia o dirección en el sector de las TIC.

Un (1) Tecnólogo/Ingeniero Líder diseñador de políticas de seguridad informática: Tecnólogo/Ingeniero Industrial, Electrónico, Sistemas, Telemático o administración de redes con:

- Experiencia general mínima de cinco (5) años trabajando en empresas del sector TIC, contados a partir de la terminación de materias.
- Experiencia específica mínima de ocho (8) meses ejerciendo funciones como configurador, operador y/o administrador de tecnologías de infraestructura o software.
- Especialización en Seguridad Informática o en su defecto contar con todas las siguientes certificaciones: CISSP y CISM y CEH-Ethical Hacking, e ISO27001:2013, vigentes a la fecha de la presentación de la oferta.
- Certificado de fábrica en nivel fundamentos y/o profesional en plataformas de protección de Endpoint, protección de servidores y XDR, con una fecha de

expedición no mayor a 2 años, de la misma marca ofertada para el presente proceso.

Un (1) TECNÓLOGO/INGENIERO DE SEGURIDAD DE ENDPOINT Y PROTECCIÓN DE INFORMACIÓN: Tecnólogo/Ingeniero Electrónico, Sistemas, Telemático o administración de redes, para la validación técnica, implementación y ajustes sobre las plataformas de seguridad de endpoint y protección de información DLP, con:

- Experiencia general mínima de tres (3) años trabajando en empresas del sector TIC, contados a partir de la terminación de materias.
- Experiencia específica mínima de dos (2) años como implementador, analista o administrador de soluciones de seguridad de endpoint y DLP.
- Certificado de fábrica en nivel fundamentos, esencial o profesional en plataformas de protección de Endpoint, protección de servidores o XDR, con una fecha de expedición no mayor a 2 años de la misma marca ofertada para el presente proceso.

Se debe adjuntar con la documentación requerida, los comprobantes de pago de aportes a seguridad social de los últimos 3 meses, con el fin de comprobar que el profesional es empleado directo de la empresa oferente, o de una de las empresas que compongan un proponente plural.

D. Comité Verificador y Evaluador de las propuestas. Una vez vencido el término para la presentación de propuestas dentro del presente proceso de selección, la CVC designará un Comité Evaluador conformado por servidores públicos o por particulares contratados para evaluar las ofertas del presente proceso.

En el evento en el cual la CVC no acoja la recomendación efectuada por el Comité Evaluador, debe justificar su decisión.

E. Presentación de aclaraciones, documentos solicitados y recepción de observaciones, al Informe de Evaluación. La CVC, dentro del plazo de traslado del Informe de Evaluación señalado en el presente pliego de condiciones, recibirá las aclaraciones, precisiones y/o documentos de los requisitos que no afecten la asignación de puntaje y que el Comité Evaluador requiera a los proponentes interesados a través del Informe de Evaluación.

Estas aclaraciones, precisiones y/o documentos deben ser entregados por los proponentes hasta el término de traslado del Informe de Evaluación y serán rechazadas las propuestas de aquellos oferentes que no suministren la información y documentación solicitada por la entidad estatal hasta el plazo anteriormente señalado, conforme a cronograma del proceso.

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

La CVC dentro del plazo de traslado del Informe de Evaluación señalado en el presente pliego de condiciones recibirá también las observaciones que los proponentes consideren pertinentes al Informe de Evaluación.

F. Reglas de subsanabilidad. El proponente tiene la responsabilidad y carga de presentar su oferta en forma concreta e íntegra, esto es, respondiendo todos los puntos del pliego de

condiciones y adjuntando todos los documentos de soporte o prueba de las condiciones que pretenda hacer valer en el proceso.

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, que han sido solicitados por la CVC, a través del Informe de Evaluación, deberán ser entregados por los proponentes hasta el vencimiento del término de traslado, conforme a cronograma del proceso.

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

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

Los proponentes deben contestar cualquier requerimiento de la CVC mediante comunicación escrita, en los términos y condiciones que para el efecto se señale en el pliego de condiciones.

Serán RECHAZADAS las propuestas de los proponentes que no subsanen los documentos solicitados.

Corporación Autónoma Regional del Valle del Cauca

CAPITULO IV.
PONDERACIÓN DE PROPUESTAS

La CVC, previo análisis comparativo de las ofertas que cumplan con los requisitos establecidos en el pliego de condiciones seleccionará el ofrecimiento más favorable a la entidad y a los fines que ella busca, aplicando los mismos criterios para todas ellas, lo que permite asegurar una selección objetiva.

Discriminación de costos de la propuesta económica: El proponente deberá suministrar todos los precios y total, de acuerdo con el cuadro del formulario No. 1 B. "PRPUESTA ECONÓMICA DEL PROPONENTE"

En caso de error en la suma, se tendrá en cuenta el resultado total corregido. Las enmendaduras u otros cambios deberán refrendarse con la firma del proponente en el mismo Anexo de la propuesta.

El anexo que contenga la propuesta económica debe ser firmado con el nombre o nombres completos del proponente, cuando se trate de una o más personas naturales. Si se trata de una sociedad, debe ser firmado por el representante legal u otra persona autorizada para obrar en nombre de la misma. En ambos casos, se deberá colocar la antefirma correspondiente.

No se podrán hacer cambios en los ítems del Formulario No. 1 B, ni agregarle comentarios. El original de la oferta prevalecerá en caso de discrepancias con las copias.

Descuentos que practica la CVC en pagos: Retención de IVA, retención de industria y comercio, retención en la fuente a título de impuesto sobre la renta (el concepto que aplique) , estampillas, entre otros, así:

Descuento Tributario	Tarifa
Retención en la fuente renta honorarios persona jurídica	11%
Retención de IVA	15%
Estampillo Pro unipacífico antes de IVA	0.5%
Estampilla pro Uceva antes de IVA	0.5%
Retención de impuesto de industria y comercio (susceptible de variación dependiendo el domicilio del sujeto de retención)	11x1000

Para determinar la oferta más favorable la CVC tendrá en cuenta la ponderación de los elementos de calidad y precio, soportados en puntajes y/o formulas.

FACTOR	CRITERIOS DE PONDERACION	PUNTAJE
Económico	Precio (fórmula)	40 %
Técnico	Calidad (puntaje)	60 %
Total		**100 %**

* Incentivos a la industria nacional

A. Factor Económico - Precio: Se asignará un puntaje máximo de 40, aplicando como método de cálculo del puntaje para el factor precio la Media Geométrica con Presupuesto Oficial, consiste en establecer la media geométrica de las Ofertas válidas y el presupuesto

oficial un número determinado de veces y la asignación de puntos en función de la proximidad de las Ofertas a dicha media geométrica, como resultado de aplicar las fórmulas que se indican en seguida. Para el cálculo de la media geométrica con presupuesto oficial se tendrá en cuenta el número de Ofertas válidas y se incluirá el presupuesto oficial del Proceso de Contratación en el cálculo tantas veces como se indica en el siguiente cuadro:

Número de propuestas (n)	**Número de veces en las que se incluye el presupuesto oficial (nv)**
1 a 3	1
4 a 6	2
7 a 9	3
10 a 12	4
13 a 15	5
…..	…..

Y así sucesivamente por cada tres propuestas válidas se incluirá una vez el presupuesto oficial del proceso de contratación.

Seguidamente se determinará la media geométrica con la inclusión del presupuesto oficial de acuerdo a lo establecido en el cuadro anterior mediante la siguiente fórmula:

$$MGPO = \frac{\sqrt[(nv+n)]{PO * PO * \cdots POnv * P1 * P2 * \cdots Pn}}{\sqrt[(nv+n)]{PO * PO * \cdots POnv * P1 * P2 * \cdots Pn}}$$

Dónde:

MGPO = Media geométrica con presupuesto oficial.
N = Número de propuestas válidas.
nv = Número de veces que se incluye el presupuesto oficial (PO).
PO = Presupuesto oficial.
Pn = Valor de la propuesta económica corregida del proponente i.

Obtenida la media geométrica con presupuesto oficial se procederá a ponderar las propuestas de acuerdo con la siguiente formula.

$$\text{Puntaje i para valores menores o iguales a MGPO= 600} \times \left(1 - \left(\frac{\text{MGPO-Vi}}{\text{MGPO}}\right)\right)$$

$$\text{Puntaje i para valores mayores a MGPO= 600} \times \left(1 - 2\left(\frac{|\text{MGPO-Vi}|}{\text{MGPO}}\right)\right)$$

Donde
MGPO = Media geométrica con presupuesto oficial
Vi = Valor total corregido de cada una de las propuestas i
i = Número de propuesta

En el caso de propuestas económicas con valores mayores a la media geométrica con presupuesto oficial se tomará el valor absoluto de la diferencia entre la media geométrica con presupuesto oficial y el valor de la propuesta, como se observa en la fórmula de ponderación.

En todo caso, cuando el valor de la propuesta supere el presupuesto oficial establecido, aplicará causal de rechazo contenida en el pliego de condiciones.

B. Factor Calidad: Se asignará un puntaje máximo de 60 puntos al proponente que oferte: Una (1) Capacitación virtual para la mesa de ayuda de la corporación de ocho (8) horas, orientada a la implementación y soporte técnico de los clientes antivirus.

Lo cual se acreditará mediante una carta firmada por el representante legal del oferente, donde se compromete a dictar estrictamente la capacitación señalada.

C. Incentivo.

➢ **Apoyo a la industria nacional.** Los proponentes pueden obtener puntaje de apoyo a la industria nacional por: i) Servicios Nacionales o Bienes Colombianos o por Trato Nacional. ii) Por la Incorporación de Servicios Nacionales o Bienes Colombianos.

La CVC en ningún caso otorgará simultáneamente el puntaje por: i) Servicio Nacional o Bienes Colombianos o por Trato Nacional. ii) Incorporación de Servicios Nacionales o Bienes Colombianos.

Los puntajes para estimular la industria nacional se relacionan en la siguiente tabla:

Concepto	Puntos
Promoción de servicios nacionales o con trato nacional	10%
Incorporación de componente nacional en servicios extranjeros	5%

Para que el proponente obtenga puntos por servicios nacionales debe presentar: i) Persona natural colombiana, la cédula de ciudadanía del proponente. ii) Persona natural extranjera residente en Colombia, la visa de residencia que le permita la ejecución del objeto contractual

de conformidad con la ley. iii) La persona jurídica constituida en Colombia, el certificado de existencia y representación legal emitido por las Cámara de Comercio.

Para que el proponente extranjero obtenga puntaje por trato nacional debe acreditar que los servicios son originados de los estados mencionados en la sesión de **acuerdos comerciales aplicables al presente proceso de contratació**n, información que se acreditará con los documentos que aporte el proponente extranjero para acreditar su domicilio.

Incorporación del componente nacional en servicios extranjeros: La entidad asignara el puntaje descrito en la siguiente tabla a los proponentes extranjeros sin derecho a trato nacional que incorporen el porcentaje de personal calificado colombiano como se describe a continuación.

Porcentaje de Personal	Puntos

D. Informe de evaluación. Al finalizar el plazo para subsanar y presentar observaciones, la CVC se pronunciará sobre las aclaraciones y documentos presentados de carácter habilitante, responderá las observaciones presentadas y publicará las respuestas a las observaciones y como consecuencia de ello puede dar lugar a que se modifique el informe de evaluación.

E. Acto administrativo de adjudicación. La adjudicación se realizará mediante acto administrativo, resolución motivada que será publicada en el SECOP II.

El acto administrativo de adjudicación, es irrevocable y obliga a la entidad y al adjudicatario; por lo tanto, contra la resolución de adjudicación no procede ningún recurso.

El adjudicatario del proceso de selección debe firmar el contrato en el término señalado en el cronograma, en caso de no hacerlo, la CVC hará efectivo el valor de la garantía de seriedad de la oferta. En este evento, la CVC, mediante resolución motivada podrá adjudicar el contrato, dentro de los quince (15) días siguientes, al proponente calificado en segundo lugar siempre y cuando su propuesta sea legalmente favorable para la corporación conforme al pliego de condiciones.

F. Factores de desempate. En caso de empate en el puntaje total de dos o más ofertas, LA CVC de conformidad con el artículo 35 de la Ley 2069 de 2020 con el fin de deberá aplicar las siguientes reglas de forma sucesiva y excluyente para seleccionar al proponente favorecido, respetando en todo caso los compromisos internacionales vigentes:

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

Se entiende por servicio de origen nacional aquellos prestados por empresas constituidas de acuerdo con la legislación nacional, por personas naturales de Colombia o por residentes en Colombia, lo que se verificara de la siguiente manera:

a) Con el certificado de existencia y representación legal para personas jurídicas.

b) Para personas naturales con la copia de la cédula de ciudadanía, de extranjería o visa de residente, si es el caso.

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

Este factor debe ser acreditado de la siguiente manera:

a) La condición de Mujer cabeza de familia: Declaración por parte de la mujer ante notario, expresando las circunstancias básicas del respectivo caso, junto con la copia de los documentos de identidad. (Parágrafo del artículo 2 de la Ley 82 de 1993)

b) La condición de Mujer víctima de la violencia intrafamiliar: deberá aportarse la respectiva medida de protección proferida por el comisario de familia del lugar donde ocurrieron los hechos y a falta de este, el juez civil municipal o promiscuo municipal, o la autoridad indígena –en los casos de violencia intrafamiliar en las comunidades indígenas, junto con copia de los documentos de identidad. (Artículos 16 y 17 de la Ley 1257 de 2008)

c) La participación mayoritaria se acreditará así: Si se trata de personas jurídicas: con el certificado de existencia y representación legal. Para el caso de proponente plural: con el documento de constitución del proponente plural, en la que conste que más del 50% de la participación accionaria o cuota parte son de titularidad de género femenino. Igualmente acreditando la condición indicada de cada una de las mujeres que participen en la sociedad de conformidad con los literales a y b del presente factor de desempate y aportar copia de los documentos de identidad de cada una de ellas.

3. Preferir la propuesta presentada por el oferente que acredite en las condiciones establecidas en la ley que por lo menos el diez por ciento (10%) de su nómina está en condición de discapacidad a la que se refiere la Ley 361 de 1997. Si la oferta es presentada por un proponente plural, el integrante del oferente que acredite que el diez por ciento (10%) de su nómina está en condición de discapacidad en los términos del presente numeral, debe tener una participación de por lo menos el veinticinco por ciento (25%) en el consorcio, unión temporal o promesa de sociedad futura y aportar mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta.

Este factor debe acreditarse aportando los siguientes documentos:

a) El proponente deberá allegar certificación vigente expedida por el Ministerio del Trabajo.

b) El proponente deberá aportar una certificación emitida por el representante legal o revisor fiscal (según corresponda) en la que relacione el número total de trabajadores con discapacidad, vinculados a la planta de personal del proponente a la fecha de cierre del proceso, el cual debe corresponder al diez (10%) de su nómina, en donde se evidencie que el personal referido ha sido contratado por lo menos con un (1) año de anterioridad a la fecha de cierre y se manifesté el compromiso de mantener vinculado a dicho personal por un lapso igual al de la contratación.

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

Para acreditar este factor, la persona natural, el representante legal de la persona jurídica o el revisor fiscal (según corresponda), adjuntará certificación bajo gravedad de juramento, en la que conste el número total de trabajadores vinculados a la planta de personal del proponente, con una anterioridad igual o mayor a un año, que no son beneficiarios pensión de vejez, familiar o de sobrevivencia y que han cumplido el requisito de edad de pensión establecido en la ley junto con los documentos de identificación de los trabajadores vinculados.

Para los casos de constitución inferior a un año se tendrá en cuenta a aquellos trabajadores que hayan estado vinculados desde el momento de constitución de la misma. (Artículo 3 Ley 2040 de 2020)

Cuando se trate de proponentes plurales, cualquiera de sus integrantes podrá acreditar las condiciones antes establecidas

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

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

Para acreditar este criterio se deberá adjuntar el certificado expedido por la persona natural, el representante legal y/o el revisor fiscal de la persona jurídica según corresponda, que acredite que al menos el 10% de su nómina pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitanas, junto con la copia de los contratos respectivos y la certificación expedida por el Ministerio del Interior o la autoridad que corresponda en los términos del Decreto 2893 de 2011, o la norma que lo modifique, sustituya o complemente.

Cuando se trate de proponentes plurales, el representante legal y/o revisor fiscal de cada uno de sus integrantes certificará que por lo menos diez por ciento (10%) del total de la nómina, pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitanas y documento idóneo que acredite la vinculación de la persona mayor con el proponente, tales como contrato, pagos al sistema de seguridad social entre otros. El porcentaje de participación del proponente plural, se definirá de acuerdo con la sumatoria de la nómina de cada uno de los integrantes del Proveedor plural.

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

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

Para acreditar este requisito el proponente deberá demostrar la participación mayoritaria de personas en proceso de reintegración o reincorporación, con alguno de los siguientes documentos:

a. Certificación en las desmovilizaciones colectivas que expide la Oficina de Alto Comisionado para la Paz.

b. Certificado que expida el Comité Operativo para la Dejación de las Armas respecto de las personas desmovilizadas en forma individual.

c. Otro documento que para el efecto determine las autoridades competentes.

En el caso de las personas jurídicas, el representante legal y/o revisor fiscal certificará bajo la gravedad de juramento que más del 50% de la composición accionaria o cuotas partes de la persona jurídica está constituida por personas en proceso de reintegración o reincorporación. Además, deberá aportar alguno de los certificados antes citados, junto con los documentos de identificación de cada una de las personas que están en proceso de reincorporación o reintegración.

Cuando se trate de proponentes plurales, cualquiera de sus integrantes podrá acreditar las condiciones antes establecidas. En todo caso, cuando varios proponentes plurales acrediten este factor de desempate, se preferirá aquel en el que el integrante del proponente plural certifique que la participación mayoritaria de personas en proceso de reintegración o reincorporación tiene una mayor participación porcentual en el consorcio o unión temporal.

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

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

Este factor debe ser acreditado de la siguiente manera:

La condición de Mujer cabeza de familia: Declaración por parte de la mujer ante notario, expresando las circunstancias básicas del respectivo caso, junto con la copia de los documentos de identidad. (Parágrafo del artículo 2 de la Ley 82 de 1993)

La condición en de persona proceso de reincorporación o reintegración: a.) Certificación en las desmovilizaciones colectivas que expide la Oficina de Alto Comisionado para la Paz, o

b.) Certificado que expida el Comité Operativo para la Dejación de las Armas respecto de las personas desmovilizadas en forma individual, o c) Otro documento que para el efecto determine las autoridades competentes.

Para el caso del literal c, el representante del proponente plural certificará, bajo la gravedad de juramento, que ni la madre cabeza de familia o persona en proceso de reincorporación o reintegración, ni la persona jurídica, ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural a la fecha de cierre del proceso de selección.

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

Se acreditará mediante el Certificado de Existencia y Representación legal expedido por la Cámara de Comercio.

La calidad de cooperativa o asociación mutual se acreditará con el certificado de existencia y representación legal y los estatutos de constitución, en caso de ser necesarios.

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

Se acreditará mediante el Certificado de Existencia y Representación legal expedido por la Cámara de Comercio de cada uno de los integrantes del proponente plural.

La calidad de cooperativa o asociación mutual se acreditará con el certificado de existencia y representación legal y los estatutos de constitución, en caso de ser necesarios.

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

Para acreditar la condición descrita en el presente numeral, el proponente deberá aportar certificación expedida por el revisor fiscal o, en su defecto, por la representante legal avalada por un contador público en el cual se acredite por lo menos el 25% del total de pagos

realizados a MIPYMES, cooperativas o asociaciones mutuales por concepto de proveeduría del proponente, realizados durante el año anterior. Para el efecto, el oferente deberá allegar sus estados financieros o información contable con fundamento en la cual se evidencia la información requerida.

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

La calidad de Sociedad de Beneficio e Interés Colectivo o Sociedad BIC, del segmento MIPYMES, se acreditará con el certificado de existencia y representación legal o el RUP de la sociedad en el que conste que reúne los requisitos del artículo 2 de la Ley 1901 de 2018 o la norma que la modifique o sustituya y además que se verifique la calidad de Mipyme.

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

12. Utilizar un método aleatorio para seleccionar el oferente, método que deberá haber sido previsto previamente en los Documentos del Proceso. Si subsiste aún el empate, se procederá a elegir el ganador mediante el sorteo por balotas así:

i) La Entidad ordenará a los proponentes empatados en orden alfabético, según el nombre de la persona natural, la persona jurídica o el proponente plural.
ii) Una vez ordenados, la Entidad compradora le asigna un número entero a cada uno de ellos de forma ascendente, de tal manera que al primero de la lista le corresponde el número 1 y así sucesivamente.
iii) La Entidad procederá a incorporar en una bolsa oscura un numero de balotas identificadas con un número igual al número de proponentes que se encuentren en condición de empatados.
iv) Se moverán las balotas en la bolsa por espacio de un minuto y la primera que se extraiga será la ganadora.

Este procedimiento quedará consignado en acta la cual se publicará en el SECOP

Nota: La acreditación de los criterios de desempate, deberán ser presentados y acreditados junto con la propuesta el día del cierre del proceso señalado en el cronograma del proceso. Por lo anterior y dado que estos documentos no son subsanables toda vez que sirven para la comparación de las ofertas en caso de empate, en el evento que se alleguen con posterioridad a esta fecha, no se tendrán en cuenta.

G. Declaratoria de desierto el proceso de selección. La declaratoria de desierto del proceso de selección únicamente procederá por motivos o causas que impidan la escogencia objetiva y se declarará en acto administrativo, en el que se señalarán en forma expresa y detallada las razones que han conducido a esa decisión.

H. Causas de rechazo de las propuestas. En el presente título se relacionan las causales para desestimar una propuesta, haciendo claridad que cuando se hace referencia a proponente u oferente, se entenderá que dicha denominación incluye a los miembros de un consorcio o unión temporal.

1. Cuando el proponente incurra en una de las inhabilidades o incompatibilidades establecidas por la Constitución Política y/o las leyes.

2. Cuando la oferta se presente extemporáneamente o no se presente en el lugar establecido en estos pliegos de condiciones.
3. Cuando el valor de la propuesta supere el presupuesto oficial establecido.
4. Cuando el proponente no consigne el valor de la propuesta, establecido en el formulario No. 1 B “Propuesta Económica”.
5. Cuando no se incluya la oferta económica.
6. Cuando formule oferta con valor artificialmente bajo, una vez surtido el debido proceso conforme al artículo 2.2.1.1.2.2.4 del Decreto 1082 de 2015.
7. Cuando el proponente no presente los documentos, no subsane sus omisiones o no entregue las aclaraciones que le solicite expresamente el verificador dentro del plazo perentorio para ello, o cuando las respuestas y/o soluciones a los anteriores requerimientos no satisfagan las condiciones exigidas en el presente pliego.
8. Cuando se presente la propuesta en forma condicionada al cumplimiento de cualquier circunstancia o modalidad no prevista en el pliego de condiciones.
9. Cuando se tenga evidencia concreta de que el oferente está o ha ejecutado cualquier acción tendiente a influir o presionar a las personas encargadas de verificar las propuestas.
10. Cuando el oferente esté incurso en los literales g) y h) del numeral 1 del artículo 8 de la Ley 80 de 1993, en aplicación de lo dispuesto en el artículo 2.2.1.1.2.2.5 del Decreto 1082 de 2015, se dará prioridad a quién haya presentado su propuesta primero en tiempo, por lo cual deberán desestimarse los demás oferentes incursos en las causales relacionadas que se hayan presentado con posterioridad.
11. Que el proponente o alguno de los integrantes del proponente plural o sus representantes legales, o el representante común del proponente plural, registren antecedentes como responsables fiscales, disciplinarios o penales, que impliquen inhabilidad para contratar con el Estado¸ o en general que el Proponente o alguno de los integrantes del proponente plural o sus representantes legales, o el representante común del proponente plural, estén incursos en cualquiera de las causales de incapacidad, inhabilidad o incompatibilidad, que le impida contratar con La Entidad de conformidad con la Constitución y la ley.
12. Cuando la oferta presente deficiencias e inexactitudes que no puedan ser aclaradas y que impidan compararla o se presente la oferta en forma parcial.
13. Cuando de acuerdo con el dictamen del Revisor Fiscal el Proponente o alguno de sus miembros, se encuentre en causal de disolución o liquidación en los términos del Código de Comercio.
14. Cuando el Contador y/o el Revisor Fiscal haya(n) sido sancionado(s) por la Junta Central de Contadores en el período en el que prepararon y/o auditaron los estados financieros presentados dentro de la oferta.
15. Cuando los proponentes o sus equipos de trabajo hayan participado en la elaboración de estudios o asesoren a la Entidad en asuntos que tengan directa relación con el objeto de la contratación respectiva.
16. Presentar la garantía de seriedad de la oferta con posterioridad a la fecha de cierre del proceso de selección, o con una fecha de expedición posterior a ésta.

CAPITULO V.
DE LOS REQUISITOS DE PERFECCIONAMIENTO Y EJECUCIÓN DEL CONTRATO.

A. Perfeccionamiento del contrato. Se presenta cuando se logra acuerdo sobre el objeto y la contraprestación, se eleve a escrito y se suscriba por las partes.

Las condiciones de ejecución del contrato están previstas en el Anexo No. 5 Clausulas Complemento al Contrato Electrónico, que contiene la forma de pago, anticipo pago anticipado según el caso, obligaciones y derechos generales del Contratista, obligación de la CVC, garantías (las que apliquen), multas, clausula penal, plazo, lugar de ejecución, clausulas excepcionales cuando apliquen y otras condiciones particulares aplicables al negocio jurídico a celebrar.

B. Gastos del contratista. Serán de cuenta del Contratista todos los gastos, derechos e impuestos tasas y similares que se deriven de la ejecución del contrato, de conformidad con la ley Colombiana, que se causen con ocasión del perfeccionamiento y ejecución del contrato.

C. Sucursal o agencia en Colombia. La persona jurídica extranjera sin domicilio o sucursal adjudicataria del contrato deberá establecer sucursal o agencia en Colombia.

D. Caducidad, tterminación, modificación e interpretación unilaterales. El presente contrato se rige por las cláusulas de terminación, modificación, e interpretación unilaterales, como también por la caducidad, siempre y cuando apliquen.

E. Documentos del contrato. Forman parte del contrato los siguientes documentos:

.- El análisis del sector económico, el estudio previo, el pliego de condiciones con las especificaciones técnicas y el análisis del riesgo y sus diferentes anexos,
.-adendas,
.-la propuesta del contratista y
.-las actas de modificación del contrato que se suscriban entre la CVC y el Contratista.

F. Sujeción a la ley. El contrato que celebre la CVC con personas naturales o jurídicas nacionales o extranjeras, estará sometido a la ley Colombiana y a la jurisdicción de los Jueces de la República. Todas las disposiciones legales vigentes en materia contractual se entienden incorporadas al presente Pliego de Condiciones y a la ejecución del contrato, así no se encuentren mencionadas en el presente documento.

G. Información para el control de la ejecución del contrato. La interventoría o la supervisión, según lo que aplique, implica según el caso:

.- El conocimiento de las condiciones técnicas exigidas en el proceso contractual.
.- La revisión del cumplimiento del contratista de los ofrecimientos hechos para acceder a puntaje en la ponderación.
.- La verificación del cumplimiento del equipo de trabajo ofrecido, en caso de que aplique.
.- La verificación del cumplimiento de los requisitos de ejecución del contrato.
.- La elaboración conjunta del cronograma de trabajo.
.- La suscripción del acta de inicio.
.- El seguimiento y control durante la ejecución del contrato.

En el ejercicio del cumplimiento obligacional están facultados para solicitar informes, aclaraciones y explicaciones sobre el desarrollo de la ejecución contractual y serán responsables por mantener informada a la Entidad contratante.

Las condiciones acreditadas durante el proceso de selección que den lugar a la obtención del puntaje del 1%, deben mantenerse durante la ejecución del contrato como una obligación contractual, es decir, los contratistas durante la ejecución del contrato deben mantener en su planta de personal como mínimo el número de trabajadores con discapacidad que certificó del Ministerio de Trabajo para obtener el puntaje durante el Proceso de Contratación.

El supervisor o el interventor del contrato, según corresponda, es el encargado de realizar el seguimiento al cumplimiento de dicha obligación. La reducción del número de trabajadores con discapacidad acreditado para obtener el puntaje adicional constituye un incumplimiento del contrato por parte del contratista, y dará lugar a las consecuencias del incumplimiento establecidas en el contrato y en la normatividad aplicable.

El interventor o supervisor que no haya informado oportunamente a la Entidad de un posible incumplimiento de un contrato bajo su responsabilidad, será solidariamente responsable de los perjuicios ocasionados a la Entidad.

H. Lliquidación del contrato. A la terminación del contrato o al producirse una causa de terminación anticipada del mismo, se procederá a su liquidación, actuación que se llevará a cabo dentro de los cuatro (4) meses siguientes, contados a partir de la fecha de terminación.

I. Obligaciones posteriores a la liquidación del contrato. Vencidos los términos de las garantías de calidad, la Entidad Estatal debe dejar constancia del cierre del expediente del proceso de contratación.

J. Registro de Libros Contables. El contratista extranjero sin domicilio en Colombia debe llevar un Registro de Libros Contables en los términos del Artículo 488 Código del Comercio.

Corporación Autónoma Regional del Valle del Cauca

ANEXOS

FORMATOS

FORMULARIO DE PRESUPUESTO OFICIAL

MATRICES

Corporación Autónoma Regional del Valle del Cauca

ANEXO No. 1 - ANEXO TECNICO

A. REQUERIMIENTOS TÉCNICOS

La Corporación busca adquirir e implementar la renovación de licencias de 836 licencias de solución de protección para endpoint con integración incluida a plataforma XDR y 166 licencias para asociar a la plataforma XDR los equipos de cómputo que actualmente cuentan con solución de protección de endpoint en la institución en la sede principal, en las sedes DAR y subsedes.

Para dar cumplimiento a los requerimientos técnicos de los equipos activos suministrados los proponentes deberán adjuntar las hojas de datos o datasheet de los respectivos fabricantes. Los manuales, vínculos a páginas web y fichas técnicas provistas por los fabricantes podrán ser entregadas en idioma inglés.

ITEM	LICENCIAMIENTO	ESPECIFICACIÓN	DESCRIPCIÓN	CUMPLE SI/NO	OBSERVACIÓN
1	solución de protección para endpoint con integración incluida a plataforma XDR	MARCA	DILIGENCIAR		
1.1.1		VERSIÓN	DILIGENCIAR		
1.1.2		CANTIDAD	836		
1.1.3		SOLUCIÓN DE PROTECCIÓN PARA ENDPOINT	Debe ser una solución que fusione una serie de técnicas avanzadas de protección contra amenazas entregadas a través de una arquitectura de agente único		
1.1.4			La solución debe tener la capacidad de brindar proteccion con los siguientes elementos: machine learning de alta fidelidad (en pre-ejecución y en ejecución), análisis de comportamiento (contra ataques de scripts, inyección, ransomware, memoria y navegadores), análisis en memoria para identificación de malware fileless, protección contra variantes, reputación web, prevenció de explotación de vulnerabilidades, bloque de comando y control, protección contra fuga de información DLP, control de dispositivos y aplicaciones, recuperación ante ransomware (ransomware rollback), detección y respuesta extendida XDR		
1.1.5			Debe contar con los siguientes módulos de protección incluídos dentro del licenciamiento sin la necesidad de activar a adquirir licenciamientos adicionales: Antimalware, Reputación Web, Firewall, Machine Learning, IDS/IPS, Control de aplicaciones, Data Loss Prevention DLP, Control de dispositivos.		

1.1.6			La solución debe brindar alta disponibilidad del servicio		
1.2.1		CONSOLA DE ADMINISTRACION	La consola de administración debe permitir administrar los agentes instalados en la red de equipos. Permitiendo conocer el estado de los agentes.		
1.2.2			La consola de administración debe estar despleagada en la Nube para garantizar la administración en todo el tiempo sin importar el lugar donde estén las maquinas administradas		
1.2.3			La consola de administración debe permitir agrupar los agentes en grupos para facilitar la configuración y administración de los mismos.		
1.2.4			La consola de administración debe permitir configurar notificaciones sobre riesgos de seguridad y ver los Logs enviados por los agentes sobre los eventos de los mismos.		
1.2.5			La consola de administración debe proporcionar un Dashboard que brinde información global sobre los agentes, eventos de reputación web, usuarios afectados, eventos de comando y control, incidentes de filtración de datos, entre otros e igualmente debe permitir que secciones o widgets sean agregados o eliminados según se requiera.		
1.2.6			La consola de administración debe permitir consultar los Logs de instalación tanto del agente como el del servidor de administración.		

1.2.7			La consola de administración debe permitir visualizar estadísticas de históricos de actualizaciones de patrones de análisis de antivirus, antispyware, análisis de comportamiento, conexiones sospechosas, y exploits de los navegadores de internet.		
1.2.8			La consola de administración debe permitir visualizar los logs de los eventos sobre los equipos donde se encuentra instalado el agente, dichos eventos deben estar relacionados a temas de malware, spyware, reputación web, conexiones sospechosas, archivos sospechosos, Command & Control Callbacks, Behavior Monitoring, Machine Learning, control de dispositivos, DLP, y escaneos. Adicionalmente la solución debe permitir filtrar dichos logs por periodos de tiempo preestablecidos, por rangos de fechas y por tipo de escaneo.		
1.2.9			La consola de administración debe permitir la visualización de los logs de registro de los eventos de la actualización del servidor de actualizaciones.		
1.2.10			La consola de administración debe permitir la visualización de los logs de registro de los eventos del servidor de administraciones.		
1.2.11			La consola de administración debe tener la capacidad de generar reporte en formato PDF, DOCX y XLSX		
1.2.12			La consola debe poder operarse en la nube sin requerir recursos de infraestructura y entregarse como software como servicio		
1.2.13			La solución debe tener la capacidad de finalizar sesiones en la consola de administración por tiempo de inactividad		

1.2.14			La solución debe tener la capacidad de eliminar de los logs de los eventos del sistema, servidor y agentes, para que estos sean eliminados con una frecuencia especifica		
1.2.15			La solucion debe permitir la configuracion de proxy tanto para los agentes como para el servidor de administracion.		
1.2.16			La solución debe permitir la realización de backups de los datos de configuraciones de la solución, los certificados SSL, datos de los agentes, y logs almacenados en el servidor de administración.		
1.2.17			La solución debe permitir la realización de backups de los logs almacenados en los agentes.		
1.2.18			La consola de administración de la solución debe proporcionar gráficos y estadísticas de distribución de la solución, distribución de políticas y agentes administrados.		
1.2.19			La solución debe tener la capacidad de identificar o agrupar los logs por políticas, inventario de equipos, aplicaciones conocidas, acciones del administrador, mensajes de los agentes y mensajes del servidor.		

1.2.20			La solución debe permitir realizar una sincronización de la lista de objetos sospechosos obtenidos de otras soluciones del mismo fabricante.		
1.2.21			La solución debe contar con roles definidos con diferentes niveles de acceso para editar y/o visualizar los datos y configuraciones de la solución.		
1.2.22			La solución debe permitir realizar búsquedas en los registros o logs, haciendo uso de filtros y permitir exportarlos en archivos con formato (CVS o XLSX).		
1.2.23			Se podrán crear usuario y roles para el acceso a la plataforma de administración		
1.2.24			La solución propuesta debe contar con un Dashboard el cual permita visualizar en tiempo real C&C, Ancho de banda usado, amenazas detectas, estado del servidor, estado de los agentes		
1.2.25			Es requisito contar con la habilidad de configurar permisos granulares en la consola de administración para delegar operaciones y trabajos específicos a diversos usuarios o grupos de usuarios, así como perfiles de auditoría que solo permitan visualizar datos, pero sin la capacidad de modificar ninguna configuración		

1.3.1			Los agentes deben ser instalados mediante instalación web, link de instalación por correo, instalación por script, instalación remota, y/o paquete de instalación.		
1.3.2			Los agentes deben requerir contraseña de administración para ser desinstalados de los equipos.		
1.3.3			Las políticas de seguridad deben aplicarse en los agentes de forma individual y/o por grupos.		
1.3.4		AGENTES	El agente debe tener la capacidad de eliminar los archivos sospechosos de forma automática.		
1.3.5			El agente debe estar integrada en un solo agente para dar protección de amenazas, protección de vulnerabilidades, control de aplicaciones y DLP		
1.3.6			Los agentes deben tener la capacidad de conectarse a múltiples fuentes de actualización (patrones, firmas, url sospechosas, etc), si alguna de estas es inaccesible para el agente.		
1.3.7			Los agentes de proteccion de los equipos deben tener la capacidad de protegerse contra intentos de desinstalacion o cancelacion de los procesos por los usuarios o por una aplicación de terceros.		
1.3.8			La solución debe permitir el uso de protocolos SSL para la comunicación entre los agentes y el servidor de administración.		

1.4.1		Regulatorios y cumplimiento	La solución debe estar ubicada en el cuadrante de líderes de Gartner conocido como “Magic Quadrant for Endpoint Protection Platforms” mínimo en los últimos 5 años anteriores.		
1.4.2			La solución debe estar listada como líder en el último cuadrante de Forrester de Endpoint Security Suites y Endpoint Detections and Responses		
1.5.1		Sistemas Operativos soportados	Windows 7 (32-bit / 64-bit) Service Pack 1		
1.5.2			Windows 8.1 (32-bit / 64-bit)		
1.5.3			Windows 10 (32-bit / 64-bit)		
1.5.4			Windows Server 2008 R2 (64-bit)		
1.5.5			Windows MultiPoint Server 2010 (64-bit)		
1.5.6			Windows MultiPoint Server 2011 (64-bit)		
1.5.7			Windows Server 2012 (64-bit)		
1.5.8			Windows Server 2016 (64-bit)		
1.5.9			Windows Server 2019 (64-bit)		
1.6.1		ANTIMALWARE	La solucion debe tener la capacidad de brindar proteccion contra malware, virus de red, conecciones sospechosas, amenazas web, spyware, trojanos, monitoreo de comportamiento, ataques conbinados y ataques de dia cero para equipos de punto final (Endpoint).		

1.6.2			La solución debe contar con firewall (reglas de conexiones de aplicación, IP, puerto y protocolo), reputación de archivos y/o reputación web.		
1.6.3			La solución debe permitir realizar escaneos de los endpoint de forma manual, programada y en tiempo real.		
1.6.4			La solución debe tener la capacidad de aislar los equipos o ponerlos en cuarentena cuando se detecta algún ataque para evitar la propagación de este dentro de la red.		
1.6.5			La solución debe permitir la integración con Active Directory		
1.6.6			La solución debe permitir realizar una migración a versiones superiores de la misma conservando las configuraciones, incluida la base de datos.		
1.6.7			La solución debe permitir recuperar los archivos que sean enviados a cuarentena.		
1.6.8			La solución debe proporcionar protección a los agentes contra Ramsomware		
1.6.9			La solución debe proporcionar una consola de administración que pueda ser utilizada desde un entorno web.		
1.6.10			La solución debe tener la capacidad de analizar la reputación de archivos		

1.6.11			La solución debe permitir la creación, modificación y eliminación de roles y usuarios para la administración de la misma.		
1.6.12			La solución debe tener la capacidad de proteger los equipos que se encuentren dentro de la red y fuera de ella		
1.6.13			La solución debe tener la capacidad de programar las sincronizaciones de los equipos para horas y fechas específicas		
1.6.14			La solución debe permitir la configuración de un servidor SMTP para el envío de notificaciones vía Email		
1.6.15			La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas al administrador, cuando una amenaza sea detectada		
1.6.16			La solución debe permitir la configuración de la plantilla del correo para el envío de notificaciones		
1.6.17			La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas al administrador, cuando uno de los equipos sea enviado a cuarentena.		
1.6.18			La solución debe permitir la configuración de la plantilla del correo para el envío de notificaciones cuando los equipos sean enviados a cuarentena.		

1.6.19			La solución debe permitir la configuración de los tipos de eventos que serán notificados y visualizados en el agente, y adicionalmente configurar el mensaje de las alertas dependiendo de la criticidad del evento (High, Medium, Low)		
1.6.20			Protección de Exploración de la memoria: identificando procesos en ejecución a medida que se ejecuta en la memoria para determinar si es malicioso. Permite terminar el proceso en ejecución dependiendo de la configuración de la acción.		
1.6.21			Protección contra ataques de exploits: controla los programas que demuestran un comportamiento anormal asociado con ataques de exploits.		
1.6.22			Protección de exploits de documentos: escanee documentos en busca de códigos de exploits integrados y vulnerabilidades conocidas		
1.6.23			Aprendizaje automático: analiza archivos desconocidos de baja prevalencia al extraer características de los archivos para examinarlos utilizando algoritmos de aprendizaje automático para determinar si el archivo es malicioso (es decir, malware / ransomware / amenazas de dia 0).		
1.6.24			Protección contra ransomware: busca la ofuscación / cifrado rápido de archivos mediante un proceso desconocido, elimina ese proceso y restaura los archivos cifrados.		
1.6.25			La solucion debe permitir la detección de amenazas tipo Fileless a través de la exploración de memoria mejorada para detectar comportamientos de procesos sospechosos. El agente debe tenre la capacidad de terminar los procesos sospechosos antes de que se pueda hacer cualquier daño.		
1.6.26			La solucion debe permitir proteger los equipos frente a vulnerabilidades no conocidas presentes en los equipos		

1.7.1		DLP- DATA LOSS PREVENTION	La solucion debe tener la capacidad de prevenir y/o informar sobre la fuga o perdida de informacion sensible de la organización ya sea de forma accidental o deliberada.		
1.7.2			La solucion debe permitir identificar o configurar los activos digitales que se desean proteger.		
1.7.3			La solucion debe permitir la creacion de politicas que limiten la trasmision o transferencias de activos digitales por los canales de comunicación convencionales (email y/o dispositivos externos).		
1.7.4			La solucion debe tener la capacidad de igualmente brindar proteccion y aplicar politicas para transferencia de activos digitales mediante cliente de correo ya sera software o web.		
1.7.5			La solucion debe permitir que la organización haga cumplir con las normas de privacidad establecidas.		
1.7.6			La solucion debe tener la capacidad de brindar proteccion contra filtrado de datos sensibles y proporcionar un control de dispositivos, permitiendo confugurar reglas o politicas para ser aplicadas a grupos o agentes individuales.		
1.7.7			La solucion debe proporcionar identificadores de datos y/o plantillas para la creacion de politicas.		
1.7.8			La solucion debe tener la capacidad de identificar o reconocer archivos ejecutables, documentos, graficos vectoriales, archivos multimedia, archivos comprimidos, bases de datos, hojas de calculo, presentacion, archivos vinculados e incrustados, y/o archivos encriptados.		
1.7.9			La solucion debe tener la capacidad de localizar activos digitales almacenados en portatiles, equipos de escriotorio, y servidores.		
1.7.10			La solucion debe tener la capacidad de proporcionar filtros de proteccion para canales de red como FTP o HTTP, canales de aplicaciones o perifericos.		
1.7.11			La solucion debe tener la capacidad de detectar datos estructurados y no estructurados.		
1.7.12			La solucion debe mantener un monitoreo constante.		

1.7.13			La solución debe proveer plantillas que permitan el cumplimiento de estándares como GLBA, HIPAA, PCI-DSS o SB-1386		
1.7.14			La solucion debe permitir generar un control de dispocitivos externos al equipo, generando bloqueos y alertas pero permitir dispocitivos por su ID,		
1.7.15			La solución debe permitir la integración con Directorio Activo y permitir la delegación de administración		
1.7.16			La solución debe contar con una consola de administración WEB que permita la configuración de políticas e implementaciones, reportes de los equipos, extracción de huellas digitales, y actualizaciones.		
1.7.17			La solucion debe tener la capacidad de identificar los activos digitales almacenados en los dispositivos o el trafico en la red utilizando expresiones regulares (predefinidas y/o personalizadas), atributos de archivos (tipo y/o tamaño), huellas digitales, palabras clave, y/o plantillas (predefinidas y/ personalizadas)		
1.7.18			Las plantillas de identificación de activos digitales deben permitir combinar identificadores de datos (expresiones, atributos de archivos, huellas digitales, lista de palabras).		
1.7.19			La solución debe permitir usar plantillas predefinidas por el fabricante, personalizarlas, crear plantillas, importar plantillas, exportar plantillas, y eliminar las plantillas.		
1.7.20			La solución debe permitir implementar políticas independientes tanto para agentes en los dispositivos como para agentes en la red.		
1.7.21			La solución debe permitir generar reportes ya sea por demanda o de forma programada (Diario, semanal o mensual), estos reportes deben contener información de los logs de los agentes. Dichos reportes deben mostrar información relevante como top de incidentes, información resumida, reporte de auditoria, entre otros.		
1.7.22			La solución debe permitir almacenar reportes y estos deben estar disponibles en formatos PDF, HTML, o Microsoft Excel		

1.7.23			La solución debe tener la capacidad de administrar los logs de manera que pueda eliminar los Logs que tengan un tiempo de más de 90 días, igualmente debe permitir la realización de un backup y limpieza de los mismos de forma manual.		
1.7.24			La solución debe soportar la detección de fuga de información en los siguientes tipos de archivo: .pdf .odt, .ott, .stw, .sxw .wpd, .wps .xml .xbd, .xdw .htm .jtd .sam .doc, .docm, .docx, .dot, .dotm, .dotx .wri .rtf .sgml .wsd, .bmp .dib .dcm .eps .img .gif .jpg .mac .png .tif, .tiff .ico .pcx, .dxf .dwg, .dws .cel, .dgn .cdb .CATDrawing, .CATPart, .CATProduct .cdr .dvi .gds .attr, .sgfx, .ssht .drw .ps .prt .svf .prtdot, .sldasm, .slddrw, .sldprt, .swf .aiff .mod .mov .avi .mid .mpeg .mpg .au .wav .wma .wmv, .7z .arc .arj .bz2 .Z .cpio .gz .lzh .chm .msg .pst .dbx .eml .pgp .rar .shar .tar .rpm .uue .zip, .sas .db .dif .dbf .fp7 .tbl .accdb, .mdb, ods, .ots, .stc, .sxc .csv .123 .wk1 .wk3 .wk4 .wke .wks .xlam .xlc .xls .xlsb .xlsm .xlsx .xltm .xltx .xlw .qpw .wb3 .wb2 .wb1 .wq1, .odp, .otp, .sti, .sxi .shw .pre .pot, .potm, .potx, .pps, .ppsm, .ppsx .ppt .pptm .pptx .vdw, .vdx, .vsd, .vss, .vst, .vsx, .vtx, .7z, .rar, .zip .accdb, .doc, .docx, .pdf, .ppt, .pptx, .w b1, .wb2, .wq1, .wpd, .xls, .xlsx, .mml .pub .qxp .one .mpp .hlp .iam, .idw, .ipt, .msoffice, .pqw y .pif		
1.7.25			La solución debe permitir configurar las fuentes de actualización para los parches o hot fixes y adicionalmente permitir configurar la periodicidad de las mismas.		
1.7.26			La herramienta de análisis local debe tener la capacidad de adquirir huellas digitales para los archivos almacenados en el equipo.		
1.7.27			La solución provee expresiones predefinidas para los números de tarjetas de crédito. A estos números se les realiza una verificación adicional por el número de prefijo y verificación con LUHN.		
1.7.28			La solución provee expresiones predefinidas para las direcciones de correo electrónico		
1.7.29			La solución provee expresiones predefinidas para los números de cuentas de bancos internacionales (IBAN).		

1.7.30			La solución provee expresiones predefinidas para códigos de identificación de negocio SWIFT BIC.		
1.7.31			La solución provee una lista de palabras predefinidas para la validación de formularios como fecha de nacimiento, fecha de expiración, Nombres y apellidos, lugar de nacimiento, departamentos o ciudades y direcciones de domicilios.		
1.7.32			La solución provee una lista de palabras que pueden ser usadas en contextos ofensivos, racistas o que incluyan elementos para causar daño (armas)		
1.7.33			La solución provee una lista de palabras que puedan identificar comandos o instrucciones en lenguajes de programación como C#, C/C++, COBOL, Java, Perl y VB.		
1.7.34			La solución debe permitir exportar e importar datos como políticas de seguridad y roles de usuarios		
1.7.35			La solución debe permitir configurar y programar el reinicio de los dispositivos de forma que no afecte negativamente las operaciones de la organización.		
1.7.36			la solución debe permitir la implementación de políticas para evitar que los usuarios publiquen contenido en clientes de mensajería instantánea o sitios de webmail		
1.8.1		CONTROL DE APLICACIONES	La solución debe tener la capacidad de prevenir la ejecución de aplicaciones no deseadas o desconocidas en los endpoint		

1.8.2			La solución debe tener la capacidad de configurar acciones sobre los archivos que estén en la lista de Suspicious Objects proporcionada por el fabricante para sus soluciones de seguridad.		
1.8.3			La solución debe permitir bloquear o permitir aplicaciones de acuerdo a puntaje de seguridad propio del fabricante.		
1.8.4			La solución debe tener la capacidad de bloquear o permitir aplicaciones basada en patrones y puntaje de prevalencia de la aplicación.		
1.8.5			La solución debe permitir establecer reglas para el cumplimiento de control de aplicaciones, dichas reglas deben permitir o bloquear aplicaciones de acuerdo con las políticas de la organización.		
1.9.1		PROTECCION WEB	La solución debe contar con reputación web adicional reputación de archivos		
1.9.2			La solución debe permitir el filtrado URL		
1.9.3			La solución debe permitir realizar un control de Ancho de Banda		
1.9.4			La solución debe permitir la inspección de trafico HTTP Y HTTPS		

1.9.5			La solución debe proteger la navegación en los equipos portátiles, endpoint y equipos que salen de la red corporativa		
1.9.6			El filtrado de URL de la solución debe estar definido por niveles de riesgo establecidos por el fabricante		
1.9.7			Si una URL no está en la base de datos para verificar su confiabilidad esta debe ser testada en tiempo real utilizando tecnología de categorización dinámica		
1.10.1		PLATAFORMA XDR	Debe permitir a la entidad tener la capacidad de detección y respuesta en email, endpoints, servidores, workloads en la nube y la red a través de una sola plataforma, es decir, poder hacer estas tareas de detección y respuesta en múltiples capas.		
1.10.2			Debe proveer un mejor contexto y un análisis más profundo, para que la entidad pueda responder de forma más rápida y eficiente a amenazas, minimizando el impacto y alcance de un incidente en la organización		
1.10.3			debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques.		
1.10.4			Los modelos de correlación deben combinar multiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.		
1.10.5			La Plataforma de XDR debe proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad		
1.10.6			Debe proveer una vista de alertas (llamadas workbenches) con la capacidad de investigar más a fondo.		
1.10.7			Las alertas deben permitir ver un análisis de causa raíz (también llamado Execution Profile) identificar el alcance del impacto y permitir tomar acciones de respuesta.		

1.10.8			Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado).		
1.10.9			Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.		
1.10.10			debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.		
1.10.11			Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las accionas que una amenaza llevó a cabo en un servidor, endpoint, o carga de trabajo en la nube.		
1.10.12			Debe permitir investigar adicionalmente desde la perspectiva de red (Network Analysis) para reproducri las comunicaciones y ver el detalle de acciones de un atacante como comunicaciones de comando y control o movimientos laterales.		
1.10.13			Debe permitir la búsqueda proactiva a traves de endpoint, red, email, y servidores (como telemetría, NetFlow, metadata, etc.) usando un simple constructor de consultas.		
1.10.14			Debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros, y filtrar los resultados añadiendo criterios adicionales de búsqueda.		
1.10.15			Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz.		
1.10.16			Se debe poder construir, guardar y reutilizar búsquedas para Threat Hunting básico		
1.10.17			Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el vendor		

1.10.18			La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campana asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a entradas de blog relacionados si están disponibles.		
1.10.19			Enlaces desde el workbench a la documentación del framework de MITRE ATT&CK		
1.10.20			En una sola ubicación debe poder iniciar y ver estado de respuesta en endpoint, email, servidores y red.		
1.10.21			Debe ofrecer opciones de respuesta “context aware” para acciones rápida desde la plataforma.		
1.10.22			Debe permitir ejecutar acciones de respuesta rápidamente haciendo click derecho en el workbench o desde los resultados de búsqueda de Threat Intelligence		
1.10.23			Una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR.		
1.10.24			Debe proveer un conector para Splunk nativo		
1.10.25			Debe ser una solución hospedada y administrada en Nube (SaaS) para tomar ventaja de tecnologías Cloud		
1.10.26			debe analizar la data recolectada por los sensoress para proveer alertas inteligentes, y detecciones de alta fidelidad.		
1.10.27			Los sensores deben soportar integración nativa del vendor para obtener toda la data de actividad (telemetria, metadata, netflow) no solo data de alertas.		

1.10.28			Los sensores deben soportar trabajar al menos en los siguientes sistemas operativos de Estaciones de trabajo de usuarios: Windows 7 y superior Mac OS X El Capitan 10.11 y superior		
1.10.29			Los sensores deben soportar trabajar al menos en las siguientes sistemas operativos de servidores Windows (Windows 2008 y superior) Linux (Including visibility over docker containers attacks) Red Hat Enterprise Linux 6 y superior Ubuntu 16 y superior CentOS 6 y superior Debian 8 y superior Amazon Linux/Amazon Linux 2 Oracle Linux 6 y superior SUSE Linux Enterprise Server 12 y superior CloudLinux 7 y superior		
1.10.30			Los sensores deben soportar trabajar por integración directa vía API con los proveedores de correo Microsoft 365 & G Suite		
1.10.31			Los sensores deben soportar trabajar Network por integración nativa con sistema BDS		
1.10.32			En el caso de estaciones de trabajo de usuarios y servidores, la funcionalidad XDR debe ser una capacidad que puede tener embebida en el mismo agente de protección de endpoint. XDR no debe ser un agente adicional		
1.10.33			Los modelos de detección deben consistir en uno o mes conjunto de filtros que integran recursos internos y externos como las técnicas y tácticas de MITRE ATT&CK		
1.10.34			El vendor debe constantemente refinar y añadir modelos de detección y filtros para mejorar las capacidades de detección y reducir falsos positivos to improve.		

1.10.35			Los modelos deben priorizar la respuesta del administrador en base a puntajes (score).		
1.10.36			El aplicativo de Detection Model Management debe permitir controlar el tipo de alertas que se disparan y se envían a Workbench.		
1.10.37			Los modelos deben tener una severidad asociada dependiendo del tipo de evento y la información de MITRE. Critical: Hay fuerte evidencia de compromiso por un ataque dirigido, APT u operaciones de cibercrimen. High: Hay indicadores altamente sospechosos de compromiso por un ataque dirigido, APT u operaciones de cibercrimen Medium: Hay indicadores sospechosos posiblemente relacionados con infección de malware, violación de políticas u operaciones de cibercrimen. Low: Hay indicadores levemente sospechosos. Usado para monitoreo y Threat Hunting		
1.10.38			Los modelos deben especificar para que productor en específico (Workstation/Server/Email/Network) aplica una alerta		
1.10.39			Los modelos deben especificar y permitir modificar “status”: encendido/apagado		
1.10.40			Los modelos deben especificar la ultima vez que se actualizó		
1.10.41			Debe hacer una sección de excepciones dentro de la App de Model Management que despliegue todas las excepciones que se añadieron.		

1.10.42			La excepcion debe ser granular y debe mostrar lo siguiente: Object: El objeto que se ha añadido como excepción en una investigación Filter: El filtro que identificó el objeto como un indicador de amenaza Type: El atributo del objeto añadido Data field: Log definido por el objeto Match type: Exacto o Parcial (soporta wildcards) Description: Información definida por el usuario para la excepción Created: Fecha y hora en que se añadió la excepción Created by: Usuario que creó la excepción		
1.10.43			Debe permitir añadir excepciones durante la investigación de una alerta.		
1.10.44			En el proceso de añadir una excepción se debe poder definir una descripción para documentar la excepción		
1.10.45			Debe integrar inteligencia al minuto con reportes del vendor y terceras partes confiables para ayudar a identificar amenazas		
1.10.46			Debe poder analizar los logs, comparar la data contra los reportes de Threat Intelligence automáticamente, y generar alertas basadas en indicadores sospechosos o maliciosos detectados		

1.10.47			La App de Workbench debe mostrar alertas por los modelos de detección y permitir investigar a más detalle. La data del Workbench debe incluir: Status: New/In Progress/Closed/Closed – False Positive Score: basado en la severidad del modelo de detección y el impacto de la alerta. Workbench ID: identificador único para la alerta Model: Modelo que disparó la alerta Model severity: Severidad asignada al modelo que disparó la alerta Impact scope: Número de entidades afectadas por Servers/Workstations/Users/Cuentas de correo Created: Fecha y Hora que XDR generó la alerta		
1.10.48			Endpoint Profile: Debe incluir Hostname/IPv4/GUID/MAC Address/OS version/Producto/Último usuario que inció sesión		
1.10.49			Email Profile: debe incluir: Asunto del correo/Message ID/Risk level/Fecha y hora del correo/Dirección de remitente/dirección de destinatarios/Información de cada adjunto al correo/URLs embebidas/Cabecera del correo		
1.10.50			Despliega el análisis de causa raíz y provee información adicional que puede ser útil para la investigación.		
1.10.51			Debe desplegar un análisis visual de los objetos envueltos en un evento		
1.10.52			Debe resaltar los objetos en la cadena que son posiblemente maliciosos		
1.10.53			Debe desplegar el objeto o la lista de objetos que coinciden con los criterios de investigación definidos		

1.10.54			Debe resaltar el objeto “mas probable” que creó el objeto que coincidió con el criterio de investigación.		
1.10.55			Debe desplegar detalles del endpoint que fue investigado		
1.10.56			La cadena de análisis debe usar íconos para los distintos tipos de objetos (servidor/endpoint/url/archivos, etc…). La descripción debe estar directamente en la ventana de investigación para entender rápidamente la relación entre los distintos objetos.		
1.10.57			Debe poder obtenerse una representación visual de correlación de eventos de la perspectiva de la red y no del endpoint.		
1.10.58			Network Analytics debe usar como sensor al BDS (Breach Detection System) y debe proveer integración nativa para compartir no solo eventos sino el contexto entero (toda la telemetría posible).		
1.10.59			Debe tener una barra de reproducción (play/pause) con un “time slider” para ver eventos correlacionados vs tiempo		
1.10.60			Cada gráfica de correlación debe tener 1 o más líneas de correlación que muestran actividad maliciosa o sospechosa entre un origen y destino.		
1.10.61			Cada línea de correlación representa 1 o más transacciones entre 2 hosts.		
1.10.62			El grosor de la línea es proporcional al número de transacciones entre los hosts. Al colocar el mouse sobre la línea debe mostrar el número de transacciones para esa línea de correlación		
1.10.63			La línea de correlación debe poder ser entre host interno y externo. También debe poder ser entre 2 hosts internos (para identificar movimientos laterales).		

1.10.64			Cada línea de correlación debe indicar los protocolos usados. Y debe existir una flecha para indicar direccionalidad de la comunicación.		
1.10.65			Debe identificar actividades claves para hosts internos y externos en la gráfica.		
1.10.66			Debe incluir actividades similares a: Machine Learning, Lateral Activity, Detected Event, C&C Activity, and Malicious Download.		
1.10.67			Correlation Information Pop-up Window: Debe incluir los sigueintes campos: Source IP/Destination IP/Severity/URLs/Hashes/Protocols/Number of transactions/Reason/Earliest date/Latest date		
1.10.68			Response Management app: Debe permitir tomar acciones y llevar registro de las acciones tomadas.		
1.10.69			Debe responder a amenazas sin dejar la consola de XDR.		
1.10.70			Debe haber distintas acciones que se puedan tomar en los objetos maliciosos/sospechosos. Añadir a lista de bloqueo Eliminar de lista de bloqueo Terminar procesos en endpoints Recolectar archivos en endpoints Bloquear remitente de correo Poner en cuarentana un correo Borrar un correo Aislar un equipo Restaurar la conexión en equipos aislados		
1.10.71			Después de activar la respuesta a un evento u objeto, debe poderse ver el estado de la tarea de respuesta y los detalles de comando en una tabla de Gestión de Respuesta		

1.10.72			Debe permitir realizar barridos IoC, personalizar búsquedas por especificación de parámetros, filtros y otros criterios y búsqueda de múltiples eventos que ocurraen en un mismo Endpoint		
1.10.73			Debe tener un constructor de peticiones que debe permitir combinar atributos de búsqueda, operadores y especificar valores en una misma petición de búsqueda		
1.10.74			Debe listar busquedas previas		
1.10.75			Debe permitir guardar búsquedas para encontrar nueva data relacionada a los mismos criterios.		
1.10.76			El administrador debe poder ver los queries guardados		
1.10.77			Debe ser fácil limpiar los criterios de búsqueda		
1.10.78			Los resultados deben ser exportables a CSV o JSON		
1.10.79			Los resultados deben mostrar origen de los datos (workstation/servidor/email/network)		
1.10.80			El administrador debe ser capaz de ver los logs en RAW		
1.10.81			debe permitir diferentes tipos de búsquedas, filtros, y un lenguaje de consultas basado en Kibana para identificar, categorizar y obtener los resultados de búsqueda.		

1.10.82			La configuración administrativa de XDR debe brindar a los usuarios la capacidad de configurar cuentas de usuario, roles y configuraciones, conectar productos adicionales y configurar opciones de monitoreo adicionales. Las siguientes opciones deben estar disponibles: SAML Single Sign-On Account Management Role Management Product Connector Alert Notifications Audit Logs Remote Support		
1.11.1		GARANTIA	soporte directo de fabricante con una disponibilidad 7x24 para atención de incidentes y contar con actualizaciones de software por la vigencia del contrato		
1.11.2			Soporte directo de fabricante para la atención de incidentes de forma remota por medio de correo electrónico y telefónico.		
1.11.3			El fabricante deberá contar con un servicio de laboratorio de investigación en español para proporcionar de forma rápida actualizaciones de bases de firmas de virus sobre amenazas enfocadas en regiones hispanohablantes		
ITEM	**LICENCIAMIENTO**	**ESPECIFICACIÓN**	**DESCRIPCIÓN**		
2	licencias para asociar a plataforma XDR	MARCA	DILIGENCIAR		
2.1.1		VERSIÓN	DILIGENCIAR		
2.1.2		CANTIDAD	166		
2.2.1		Sistemas Operativos soportados	Windows 7 (32-bit / 64-bit) Service Pack 1		
2.2.2			Windows 8.1 (32-bit / 64-bit)		

2.2.3			Windows 10 (32-bit / 64-bit)		
2.2.4			Windows Server 2008 R2 (64-bit)		
2.2.5			Windows MultiPoint Server 2010 (64-bit)		
2.2.6			Windows MultiPoint Server 2011 (64-bit)		
2.2.7			Windows Server 2012 (64-bit)		
2.2.8			Windows Server 2016 (64-bit)		
2.2.9			Windows Server 2019 (64-bit)		
2.3.1		PLATAFORMA XDR	Debe permitir a la entidad tener la capacidad de detección y respuesta en email, endpoints, servidores, workloads en la nube y la red a través de una sola plataforma, es decir, poder hacer estas tareas de detección y respuesta en múltiples capas.		
2.3.2			Debe proveer un mejor contexto y un análisis más profundo, para que la entidad pueda responder de forma más rápida y eficiente a amenazas, minimizando el impacto y alcance de un incidente en la organización		
2.3.3			debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques.		
2.3.4			Los modelos de correlación deben combinar multiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.		
2.3.5			La Plataforma de XDR debe proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad		
2.3.6			Debe proveer una vista de alertas (llamadas workbenches) con la capacidad de investigar más a fondo.		

2.3.7			Las alertas deben permitir ver un análisis de causa raíz (también llamado Execution Profile) identificar el alcance del impacto y permitir tomar acciones de respuesta.		
2.3.8			Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado).		
2.3.9			Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.		
2.3.10			debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.		
2.3.11			Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las accionas que una amenaza llevó a cabo en un servidor, endpoint, o carga de trabajo en la nube.		
2.3.12			Debe permitir investigar adicionalmente desde la perspectiva de red (Network Analysis) para reproducri las comunicaciones y ver el detalle de acciones de un atacante como comunicaciones de comando y control o movimientos laterales.		
2.3.13			Debe permitir la búsqueda proactiva a traves de endpoint, red, email, y servidores (como telemetría, NetFlow, metadata, etc.) usando un simple constructor de consultas.		
2.3.14			Debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros, y filtrar los resultados añadiendo criterios adicionales de búsqueda.		
2.3.15			Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz.		
2.3.16			Se debe poder construir, guardar y reutilizar búsquedas para Threat Hunting básico		

2.3.17			Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el vendor		
2.3.18			La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campana asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a entradas de blog relacionados si están disponibles.		
2.3.19			Enlaces desde el workbench a la documentación del framework de MITRE ATT&CK		
2.3.20			En una sola ubicación debe poder iniciar y ver estado de respuesta en endpoint, email, servidores y red.		
2.3.21			Debe ofrecer opciones de respuesta “context aware” para acciones rápida desde la plataforma.		
2.3.22			Debe permitir ejecutar acciones de respuesta rápidamente haciendo click derecho en el workbench o desde los resultados de búsqueda de Threat Intelligence		
2.3.23			Una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR.		
2.3.24			Debe proveer un conector para Splunk nativo		
2.3.25			Debe ser una solución hospedada y administrada en Nube (SaaS) para tomar ventaja de tecnologías Cloud		
2.3.26			debe analizar la data recolectada por los sensoress para proveer alertas inteligentes, y detecciones de alta fidelidad.		

2.3.27			Los sensores deben soportar integración nativa del vendor para obtener toda la data de actividad (telemetria, metadata, netflow) no solo data de alertas.		
2.3.28			Los sensores deben soportar trabajar al menos en los siguientes sistemas operativos de Estaciones de trabajo de usuarios: Windows 7 y superior Mac OS X El Capitan 10.11 y superior		
2.3.29			Los sensores deben soportar trabajar al menos en las siguientes sistemas operativos de servidores Windows (Windows 2008 y superior) Linux (Including visibility over docker containers attacks) Red Hat Enterprise Linux 6 y superior Ubuntu 16 y superior CentOS 6 y superior Debian 8 y superior Amazon Linux/Amazon Linux 2 Oracle Linux 6 y superior SUSE Linux Enterprise Server 12 y superior CloudLinux 7 y superior		
2.3.30			Los sensores deben soportar trabajar por integración directa vía API con los proveedores de correo Microsoft 365 & G Suite		
2.3.31			Los sensores deben soportar trabajar Network por integración nativa con sistema BDS		
2.3.32			En el caso de estaciones de trabajo de usuarios y servidores, la funcionalidad XDR debe ser una capacidad que puede tener embebida en el mismo agente de protección de endpoint. XDR no debe ser un agente adicional		
2.3.33			Los modelos de detección deben consistir en uno o mes conjunto de filtros que integran recursos internos y externos como las técnicas y tácticas de MITRE ATT&CK		

2.3.34			El vendor debe constantemente refinar y añadir modelos de detección y filtros para mejorar las capacidades de detección y reducir falsos positivos to improve.		
2.3.35			Los modelos deben priorizar la respuesta del administrador en base a puntajes (score).		
2.3.36			El aplicativo de Detection Model Management debe permitir controlar el tipo de alertas que se disparan y se envían a Workbench.		
2.3.37			Los modelos deben tener una severidad asociada dependiendo del tipo de evento y la información de MITRE. Critical: Hay fuerte evidencia de compromiso por un ataque dirigido, APT u operaciones de cibercrimen. High: Hay indicadores altamente sospechosos de compromiso por un ataque dirigido, APT u operaciones de cibercrimen Medium: Hay indicadores sospechosos posiblemente relacionados con infección de malware, violación de políticas u operaciones de cibercrimen. Low: Hay indicadores levemente sospechosos. Usado para monitoreo y Threat Hunting		
2.3.38			Los modelos deben especificar para que productor en específico (Workstation/Server/Email/Network) aplica una alerta		
2.3.39			Los modelos deben especificar y permitir modificar “status”: encendido/apagado		
2.3.40			Los modelos deben especificar la ultima vez que se actualizó		
2.3.41			Debe hacer una sección de excepciones dentro de la App de Model Management que despliegue todas las excepciones que se añadieron.		

2.3.42			La excepcion debe ser granular y debe mostrar lo siguiente: Object: El objeto que se ha añadido como excepción en una investigación Filter: El filtro que identificó el objeto como un indicador de amenaza Type: El atributo del objeto añadido Data field: Log definido por el objeto Match type: Exacto o Parcial (soporta wildcards) Description: Información definida por el usuario para la excepción Created: Fecha y hora en que se añadió la excepción Created by: Usuario que creó la excepción		
2.3.43			Debe permitir añadir excepciones durante la investigación de una alerta.		
2.3.44			En el proceso de añadir una excepción se debe poder definir una descripción para documentar la excepción		
2.3.45			Debe integrar inteligencia al minuto con reportes del vendor y terceras partes confiables para ayudar a identificar amenazas		
2.3.46			Debe poder analizar los logs, comparar la data contra los reportes de Threat Intelligence automáticamente, y generar alertas basadas en indicadores sospechosos o maliciosos detectados		

2.3.47			La App de Workbench debe mostrar alertas por los modelos de detección y permitir investigar a más detalle. La data del Workbench debe incluir: Status: New/In Progress/Closed/Closed – False Positive Score: basado en la severidad del modelo de detección y el impacto de la alerta. Workbench ID: identificador único para la alerta Model: Modelo que disparó la alerta Model severity: Severidad asignada al modelo que disparó la alerta Impact scope: Número de entidades afectadas por Servers/Workstations/Users/Cuentas de correo Created: Fecha y Hora que XDR generó la alerta		
2.3.48			Endpoint Profile: Debe incluir Hostname/IPv4/GUID/MAC Address/OS version/Producto/Último usuario que inció sesión		
2.3.49			Email Profile: debe incluir: Asunto del correo/Message ID/Risk level/Fecha y hora del correo/Dirección de remitente/dirección de destinatarios/Información de cada adjunto al correo/URLs embebidas/Cabecera del correo		
2.3.50			Despliega el análisis de causa raíz y provee información adicional que puede ser útil para la investigación.		
2.3.51			Debe desplegar un análisis visual de los objetos envueltos en un evento		
2.3.52			Debe resaltar los objetos en la cadena que son posiblemente maliciosos		
2.3.53			Debe desplegar el objeto o la lista de objetos que coinciden con los criterios de investigación definidos		

2.3.54			Debe resaltar el objeto “mas probable” que creó el objeto que coincidió con el criterio de investigación.		
2.3.55			Debe desplegar detalles del endpoint que fue investigado		
2.3.56			La cadena de análisis debe usar íconos para los distintos tipos de objetos (servidor/endpoint/url/archivos, etc…). La descripción debe estar directamente en la ventana de investigación para entender rápidamente la relación entre los distintos objetos.		
2.3.57			Debe poder obtenerse una representación visual de correlación de eventos de la perspectiva de la red y no del endpoint.		
2.3.58			Network Analytics debe usar como sensor al BDS (Breach Detection System) y debe proveer integración nativa para compartir no solo eventos sino el contexto entero (toda la telemetría posible).		
2.3.59			Debe tener una barra de reproducción (play/pause) con un “time slider” para ver eventos correlacionados vs tiempo		
2.3.60			Cada gráfica de correlación debe tener 1 o más líneas de correlación que muestran actividad maliciosa o sospechosa entre un origen y destino.		
2.3.61			Cada línea de correlación representa 1 o más transacciones entre 2 hosts.		
2.3.62			El grosor de la línea es proporcional al número de transacciones entre los hosts. Al colocar el mouse sobre la línea debe mostrar el número de transacciones para esa línea de correlación		
2.3.63			La línea de correlación debe poder ser entre host interno y externo. También debe poder ser entre 2 hosts internos (para identificar movimientos laterales).		

2.3.64			Cada línea de correlación debe indicar los protocolos usados. Y debe existir una flecha para indicar direccionalidad de la comunicación.		
2.3.65			Debe identificar actividades claves para hosts internos y externos en la gráfica.		
2.3.66			Debe incluir actividades similares a: Machine Learning, Lateral Activity, Detected Event, C&C Activity, and Malicious Download.		
2.3.67			Correlation Information Pop-up Window: Debe incluir los sigueintes campos: Source IP/Destination IP/Severity/URLs/Hashes/Protocols/Number of transactions/Reason/Earliest date/Latest date		
2.3.68			Response Management app: Debe permitir tomar acciones y llevar registro de las acciones tomadas.		
2.3.69			Debe responder a amenazas sin dejar la consola de XDR.		
2.3.70			Debe haber distintas acciones que se puedan tomar en los objetos maliciosos/sospechosos. Añadir a lista de bloqueo Eliminar de lista de bloqueo Terminar procesos en endpoints Recolectar archivos en endpoints Bloquear remitente de correo Poner en cuarentana un correo Borrar un correo Aislar un equipo Restaurar la conexión en equipos aislados		
2.3.71			Después de activar la respuesta a un evento u objeto, debe poderse ver el estado de la tarea de respuesta y los detalles de comando en una tabla de Gestión de Respuesta		

2.3.72			Debe permitir realizar barridos IoC, personalizar búsquedas por especificación de parámetros, filtros y otros criterios y búsqueda de múltiples eventos que ocurraen en un mismo Endpoint		
2.3.73			Debe tener un constructor de peticiones que debe permitir combinar atributos de búsqueda, operadores y especificar valores en una misma petición de búsqueda		
2.3.74			Debe listar busquedas previas		
2.3.75			Debe permitir guardar búsquedas para encontrar nueva data relacionada a los mismos criterios.		
2.3.76			El administrador debe poder ver los queries guardados		
2.3.77			Debe ser fácil limpiar los criterios de búsqueda		
2.3.78			Los resultados deben ser exportables a CSV o JSON		
2.3.79			Los resultados deben mostrar origen de los datos (workstation/servidor/email/network)		
2.3.80			El administrador debe ser capaz de ver los logs en RAW		
2.3.81			debe permitir diferentes tipos de búsquedas, filtros, y un lenguaje de consultas basado en Kibana para identificar, categorizar y obtener los resultados de búsqueda.		

2.3.82			La configuración administrativa de XDR debe brindar a los usuarios la capacidad de configurar cuentas de usuario, roles y configuraciones, conectar productos adicionales y configurar opciones de monitoreo adicionales. Las siguientes opciones deben estar disponibles: SAML Single Sign-On Account Management Role Management Product Connector Alert Notifications Audit Logs Remote Support		
2.4.1		GARANTIA	soporte directo de fabricante con una disponibilidad 7x24 para atención de incidentes y contar con actualizaciones de software por la vigencia del contrato		
2.4.2			Soporte directo de fabricante para la atención de incidentes de forma remota por medio de correo electrónico y telefónico.		
2.4.3			El fabricante deberá contar con un servicio de laboratorio de investigación en español para proporcionar de forma rápida actualizaciones de bases de firmas de virus sobre amenazas enfocadas en regiones hispanohablantes		

Obligaciones del Contratista: Los licenciamientos entregados deberán contar con una vigencia y garantía de mínimo un (1) año, prestada directamente por el fabricante.

- **Con respecto a la entrega e instalación de licenciamientos en los equipos de cómputo de la entidad**

- Aplicar las políticas de seguridad establecidas por la entidad
- La actualización de patrones y de la plataforma será por parte del proveedor de la solución
- Adjuntar a su oferta una carta emitida por el fabricante o mayorista, en donde se certifica que tiene la experiencia suficiente para la instalación y soporte de las soluciones ofertadas y que se encuentra autorizado para comercializarlas en el territorio colombiano
- El proveedor de la solución debe disponer de mínimo 1 ingeniero certificado por el fabricante en las soluciones ofertadas
- Hacer la validación de activación y acceso a la consola de administración de la solución y garantizar el correcto registro de licenciamiento contratado
- Realizar la configuración de las reglas, perfiles y políticas de seguridad de equipo de usuario final en la consola de administración de la solución y asegurar que cumplan

las funciones (protección antimalware, DLP, control de aplicaciones, protección web) que actualmente cumple la solución existente.

- Realizar y validar la integración y sincronización de la consola de administración de la solución con el directorio activo de la CVC, para aplicar políticas de seguridad de equipo final basadas en roles de usuarios corporativos.
- Realizar la configuración de 5 reportes de seguridad usando las herramientas disponibles en la consola de administración de la solución
- Activar y realizar la integración del producto de protección de antivirus con la plataforma de XDR en nube
- Entregar la transferencia de conocimientos para los ingenieros de la entidad
- Realizar el proceso de desinstalación de agentes de antivirus a 836 equipos de la Corporación
- Realizar el proceso de instalación de agentes en 836 endpoint de manera remota y sincronización remota a la plataforma XDR de 166 equipos de cómputo que actualmente cuentan con solución de protección de endpoint en la institución.
- Acordar con el Supervisor los tiempos de desinstalación e instalación de los agentes de software y el método de contacto de los usuarios.

Corporación Autónoma Regional del Valle del Cauca

ANEXO No. 2 - CRONOGRAMA

No.	ACTIVIDAD	DESDE	HASTA
1	Aviso de convocatoria pública, análisis del sector, estudio previo, proyecto de pliego de condiciones y demás documentos previos	30/11//2021	7/12/2021
2	Observaciones y comentarios al proyecto pliego de condiciones por los interesados.	1/12/2021	7/12/2021 hasta las 5:30 pm
3	Respuesta a observaciones y comentarios presentados al proyecto de pliego de condiciones.	1/12/2021	9/12/2021
4	Acto administrativo de apertura y Pliego de Condiciones Definitivo	9/12/2021	
5	Manifestación de interés en participar en el presente proceso	10/12/2021 hasta las 5:30 pm	
6	Si la entidad recibe más de diez propuestas, llevará a cabo sorteo, para seleccionar máximo diez oferentes	13/12/2021 8:30 a.m.	
7	Término para presentación de observaciones al pliego definitivo	9/12/2021	13/12/2021 5:30:pm
8	Término para respuestas a observaciones al pliego definitivo	14/12/2021	
9	Plazo máximo para expedir adendas	14/12/2021	
10	Plazo para presentar propuestas	9/12/2021	15/12/2021 5:00 pm.
11	Apertura de ofertas y elaboración acta de cierre	15/12/2021, a las 5:10 p.m	
12	Evaluación de propuestas por el Comité Evaluador	16/12/2021	
13	Publicación informe de evaluación	16/12/2021	21/12/2021
14	Presentación de observaciones al informe de evaluación	17/12/2021	21/12/2021 Hasta las 5:30 p.m.
15	Respuesta de observaciones al informe de evaluación	22/12/2021	
16	Publicación Acto Administrativo de adjudicación o de Declaratoria de Desierto	22/12/2021	

17	Fecha estimada para la firma del contrato	23/12/2021
18	Fecha estimada para la entrega de las garantías de ejecución del contrato	24/12/2021
19	Fecha estimada para la aprobación de las garantías o pólizas e inicio de ejecución del contrato	24/12/2021

ANEXO No. 3
GLOSARIO

Antimalware: Es un tipo de programa diseñado para prevenir, detectar y remediar software malicioso en los dispositivos informáticos.

DLP: Es un sistema que realiza el escaneo de datos en tiempo real en reposo y en movimiento, evalúa los datos contra definiciones de políticas existentes, identifica violaciones de políticas y automáticamente aplica algún tipo de acciones de corrección predefinidas, como alertas a usuarios y administradores, poner en cuarentena archivos sospechosos, encriptar datos o bloquear el tráfico directamente.

Malware: cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Sistema Operativo: Es el conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software.

URL: Es la dirección específica que se asigna a cada uno de los recursos disponibles en la red con la finalidad de que estos puedan ser localizados o identificados.

ANEXO No. 4
PACTO DE TRANSPARENCIA

El Suscrito a saber _____, domiciliado en _____ identificado con la cédula de ciudadanía No. _____de _____, quien obra en calidad de _____ que en adelante se denominará el proponente, manifiesta su voluntad de asumir el presente PACTO DE INTEGRIDAD, teniendo en cuenta las siguientes consideraciones:

1. Que la CVC adelanta el proceso de Selección Abreviada de Menor Cuantía CVC No.38 de 2021, cuyo objeto consiste en: *ADQUISICION, IMPLEMENTACIÓN Y SOPORTE TECNICO DE NIVEL 3 DE LICENCIAS ANTIVIRUS PARA LA CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA"*
2. Que es interés del proponente y de la CVC, apoyar la acción del Estado Colombiano para promover la cultura de la probidad y fortalecer la transparencia en los procesos de contratación.
3. Que el Proponente pacta y asume los siguientes compromisos:

- NO ofrecerá ni dará sobornos, ni ninguna otra forma de halago a ningún funcionario público en relación con su propuesta, en el proceso de contratación.
- NO permitirá que nadie, bien sea empleado suyo o un agente comisionista independiente, o un asesor o Proveedor o Contratista lo haga en su nombre.
- Impartirá instrucciones a todos sus empleados, agentes y asesores y a cualquier otro representante suyo exigiéndole el cumplimiento en todo momento de las leyes de la República de Colombia en el presente proceso de contratación y la relación contractual que podría derivarse de ella, y les impondrá las obligaciones de: No ofrecer o pagar sobornos y cualquier halago a los funcionarios de la CVC ni a cualquier otro servidor público o privado que pueda influir en la adjudicación de la propuesta, bien sea directa o indirectamente, ni a terceras personas que por su influencia sobre funcionarios públicos, puedan influir sobre la adjudicación de la propuesta, ni a ofrecer pagos ni halagos a los funcionarios de la CVC, durante el desarrollo del contrato que se suscriba si llegase a ser elegida su propuesta.
- NO efectuará acuerdos o realizará actos o conductas que tengan por objeto o como objeto la colusión en el presente proceso contractual.
- Se compromete a verificar toda la información, que a través de terceros deba presentar a esta Entidad para efectos del proceso contractual.
- Asumirá la responsabilidad por el suministro de información inconsistente, imprecisa o que no corresponda a la realidad para efectos de esta contratación.
- Actuará bajo los principios de la ética, la moral, las buenas costumbres, la probidad y en general bajo los principios del artículo 23 de la Ley 80 de 1993, que rigen la contratación estatal.
- Asume a través de la suscripción del presente compromiso, las consecuencias previstas en el pliego de condiciones, si se verificare el incumplimiento de los compromisos de integridad en el proceso contractual.

En todo caso, con la firma de este documento, se entiende que el proponente conoce y acepta, todas y cada una de las obligaciones incluidas en el mismo y por lo tanto, no será necesario para habilitarlo, la entrega de este documento al momento de presentar la oferta; toda vez que este documento se entiende incorporado en la carta de presentación de la propuesta.

FIRMA DEL PROPONENTE
C.C. o NIT.

ANEXO No. 5
CLAUSULAS COMPLEMENTARIAS AL CONTRATO ELECTRÓNICO

Entre los suscritos a saber: …….., mayor de edad, vecino de Cali (V), identificado con la cédula de ciudadanía No.……, expedida en ……, quien obra en nombre y representación de LA CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA -CVC, en su condición de DIRECTOR GENERAL de la misma, de conformidad con el nombramiento contenido en la Resolución ……, haciendo constar que LA CVC es un ente Corporativo autónomo de carácter público, creado mediante el Decreto 3110 de 1954, transformado por la Ley 99 de 1993 y reestructurado mediante el Decreto Legislativo 1275 de 1994, dotado de autonomía administrativa y financiera, patrimonio propio y personería jurídica, coordinado por el Ministerio de Ambiente, Vivienda y Desarrollo Territorial, quien en adelante para efectos del presente contrato se denominará **LA CVC**, de una parte, y de la otra ……. mayor de edad, vecino de Cali, identificado con la cedula de ciudadanía No. ……. expedida en la ciudad de ……., quien obra en nombre y representación de la firma ……, en su calidad de Gerente y representante legal, haciendo constar que la misma es una Sociedad …….., con domicilio en……; y quien para los efectos de este documento se denominará **EL CONTRATISTA**, hemos convenido celebrar el presente contrato de xxx determinado por las siguientes cláusulas, **PRIMERA.- OBJETO.** Consiste en "*ADQUISICION, IMPLEMENTACIÓN Y SOPORTE TECNICO DE NIVEL 3 DE LICENCIAS ANTIVIRUS PARA LA CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA "* **xxxxxxxxxxxxxxxxxxxxxxxxx***".* **SEGUNDA.- ESPECIFICACIONES TECNICAS. XXXXX TERCERA.- OBLIGACIONES DEL CONTRATISTA.** XXXXXXXXXX **Parágrafo:** El CONTRATISTA ya sea en sus instalaciones o en las instalaciones de la CVC o cuando envíe personal a cualquiera de los lugares donde se ejecutará el contrato, deberá dar aplicación a todos los Protocolos de Bioseguridad que establezcan las autoridades nacionales, con ocasión de la Pandemia del Covid-19. **CUARTA.- OBLIGACIONES DE LA CVC.** 1) Cancelar el valor del contrato en la forma y términos establecidos en la Cláusula Quinta del presente acuerdo. 2) Suministrar oportunamente la información que requiera el CONTRATISTA, para el cumplimiento de las obligaciones contractuales **QUINTA.- VALOR Y FORMA DE PAGO. El Valor** es de XXXXX. **La Forma de Pago**: XXXXXXXXX**. Parágrafo 1**: El Contratista deberá antes de cada pago presentar un informe de actividades realizadas. **Parágrafo 2**: El Contratista deberá presentar certificación emitida por el Revisor Fiscal o Representante legal según el caso, en donde conste que la firma se encuentra al día en el pago de salarios, pago de aportes a sus empleados a los Sistemas Generales de Seguridad Social, (Salud, Pensión y Riesgos Profesionales) y aportes parafiscales (Cajas de Compensación Familiar, SENA, ICBF, subsidio familiar y subsidio de transporte), acompañado de un listado detallado de la totalidad de los empleados que laboran en la ejecución del presente objeto contractual. De igual forma debe presentarse fotocopia de la Planilla de Pago en la que conste que se encuentra al día en el pago de aportes de la totalidad de los operarios que laboran en la ejecución del presente objeto contractual, al Sistema General de Seguridad Social y

Parafiscales. **Parágrafo 3:** Las facturas que presente el CONTRATISTA para llevar a cabo cualquier cobro inherente al contrato, deben cumplir con todos los requisitos establecidos por la Dirección de Impuestos Nacionales de Colombia-DIAN. En el evento que la CVC reporte cualquier novedad en dicho documento el CONTRATISTA tendrá la obligación de realizar las correcciones pertinentes a fin de dar continuidad al proceso de pago. No se realizarán pagos que no cumplan con el lleno de los requisitos legales. **Parágrafo 4:** La CVC efectuará Los reconocimientos o descuentos a que haya lugar proporcional al monto de cada factura. Si la factura no ha sido bien elaborada o si le faltan los documentos de soporte, el término para el pago sólo empezará a contarse desde la fecha en que quede corregida la factura o desde aquella en que se haya aportado el último de los documentos. Todas las demoras que se presenten por. estos conceptos serán responsabilidad del CONTRATISTA, quien no tendrá por ello derecho al pago de intereses o compensación de ninguna naturaleza. **SEXTA.- SUJECIÓN A LAS APROPIACIONES PRESUPUESTALES.** El presente contrato posee el certificado de disponibilidad presupuestal, así: xxxxxxx, expedido por el Coordinador del Grupo de Presupuesto. **SEPTIMA.- PLAZO.** Es de xxxxxxxx. **OCTAVA.- INEXISTENCIA DE RELACIÓN LABORAL.** EL CONTRATISTA ejecutará el presente contrato por sus propios medios y con plena autonomía técnica y directiva, en consecuencia y de conformidad con lo dispuesto por el numeral 3, artículo 32, Ley 80 de1993, este contrato no genera relación laboral alguna entre EL CONTRATISTA y el personal que este emplee para la prestación del servicio y LA CVC, por lo cual no tiene derecho al reconocimiento ni al pago de Prestaciones Sociales y/o a ningún tipo de acreencias laborales por parte de LA CVC. En consecuencia, la CVC únicamente se obliga a reconocer la suma expresamente pactada. **NOVENA.- CLAUSULA PENAL PECUNIARIA.** En caso de incumplimiento por parte del CONTRATISTA de cualquiera de sus obligaciones legales o contractuales, LA CVC podrá declarar tal incumplimiento mediante resolución motivada, de conformidad con el artículo 86 de la Ley 1474 de 2011, y exigir el pago a título de pena en los términos del artículo 1592 del Código Civil para imputar el valor de los perjuicios que pueda sufrir La CVC en caso de incumplimiento, se establece una suma equivalente al VEINTE POR CIENTO (20%) del valor total del contrato; para lo cual, el presente contrato firmado por las partes prestará mérito ejecutivo, renunciando el CONTRATISTA a requerimientos de constitución en mora. **Parágrafo 1:** La CVC podrá, previo informe escrito presentado por el SUPERVISOR del Contrato, y una vez surtido el debido proceso conforme al artículo 86 de la Ley 1474 de 2011, declarar el incumplimiento del contrato y la cláusula penal pecuniaria se hará efectiva directamente por LA CVC, pudiendo para el efecto descontarla de las sumas que adeude al CONTRATISTA o hacer efectiva la garantía única que respalda el cumplimiento del contrato, cuando a ello haya lugar. **Parágrafo 2:** Si existiere discrepancia sobre el monto de los intereses, se aplicarán los regulados en el artículo 1617 del Código Civil. **DECIMA.- TERMINACIÓN, MODIFICACIÓN E INTERPRETACIÓN UNILATERALES.** El presente contrato se rige por las cláusulas de terminación, modificación, e interpretación unilateral contenidas en los artículos 15, 16 y 17 de la Ley 80 de 1993. **DECIMA PRIMERA.- SUSPENSIÓN.** Por circunstancias de fuerza mayor o caso fortuito, por ser conveniente a los intereses de LA CVC o por mutuo acuerdo, se podrá suspender temporalmente la ejecución total o parcial del contrato, sin que cesen los efectos legales del mismo. En este caso, LAS PARTES SUSCRIBIRÁN UN ACTA DE SUSPENSIÓN TEMPORAL en la cual se haga constar dicha circunstancia y la fecha estimada de reiniciación del mismo. **Parágrafo 1:** La parte contratante que resulte afectada por tales hechos y que no puedan por ello cumplir con las obligaciones contractuales, deberá notificar por escrito a la otra parte, inmediatamente el surgimiento y a la terminación de dichas condiciones. Tal aviso deberá enviarse a la otra parte por comunicación escrita, dentro de los cinco (5) días siguientes a partir de la fecha del comienzo de las mismas. Dentro de un plazo no mayor a diez (10) días desde la fecha del

aviso, la parte afectada por la fuerza mayor o caso fortuito deberá enviar una carta anexando el documento de la autoridad competente en el cual se certifiquen las condiciones arriba mencionadas y las medidas tomadas para evitarlas, debe ser ello procedente excepto en el evento de que se trate de hechos notorios de público conocimiento. Durante el periodo en que persistan las circunstancias arriba mencionadas, las partes están obligadas a tomar las medidas necesarias para reducir los perjuicios provocados por las mismas. La parte afectada por tales circunstancias, que no la haya sido posible cumplir con las obligaciones contractuales, deberá informar periódicamente a la otra sobre el estado en que están transcurriendo la fuerza mayor y el caso fortuito, si estas circunstancias duran más de seis (6) meses, las partes deberán ponerse de acuerdo con el fin de adecuar las condiciones del contrato a las nuevas situaciones que se presenten. **Parágrafo 2:** Una vez suscrita el acta de suspensión se deberá remitir copia de la misma a la compañía de Seguros que emitió la garantía para que tome las medidas del caso. Superadas las causas que dieron origen a la suspensión del contrato, mediante acta suscrita por las partes SE REINICIARÁ su ejecución y EL CONTRATISTA deberá modificar la Garantía teniendo en cuenta el tiempo de suspensión del contrato. **DECIMA SEGUNDA.- CADUCIDAD ADMINISTRATIVA**. LA CVC podrá declarar la caducidad del presente contrato, si se presenta alguno o algunos de los hechos constitutivos de incumplimiento de las obligaciones a cargo del CONTRATISTA que afecte en manera grave y directa la ejecución del contrato y se evidencie que pueda generar su paralización; igualmente podrá darse la declaratoria de caducidad por las casusas de orden legal establecida en las diferentes normas que regulen dicha sanción para Contratistas estatales. La CVC por medio de acto administrativo lo dará por terminado y ordenará la liquidación en el estado en que se encuentre. Decretada la caducidad no habrá lugar a indemnización alguna para el CONTRATISTA, quien se hará acreedor a las sanciones e inhabilidades previstas en el artículo 18 de la Ley 80 de 1993 y demás disposiciones aplicables. La declaratoria de caducidad será constitutiva del siniestro de incumplimiento. **DECIMA TERCERA.- MULTAS.** Las partes contratantes de común acuerdo establecen que El CONTRATISTA se hará acreedor al pago de multas conminatorias para el cumplimiento de las obligaciones a su cargo, por cada día de mora o retraso injustificado en la ejecución de las actividades pactadas, hasta por una cuantía equivalente al 0,5% del valor total del contrato, previo informe escrito presentado por el interventor o supervisor del Contrato y una vez surtido el debido proceso conforme al artículo 86 de la Ley 1474 de 2011. **Parágrafo 1**: Una vez en firme el acto administrativo que decreta la imposición de la multa, el valor de esta última se deducirá de las cuentas que sé le adeuden al contratista, sin perjuicio de hacer efectivas las garantías. **Parágrafo 2**: La constitución del CONTRATISTA en mora del cumplimiento de cualquiera de sus obligaciones y en general el incumplimiento del contrato, será comunicada oficialmente al CONTRATISTA y su Garante, por la CVC, fijándoles un término para presentar los descargos que tuvieren a su favor, vencido el cual la CVC procederá a hacer efectivas las estipulaciones de la cláusula penal, o las multas y el resultado se les comunicará oportunamente al CONTRATISTA por parte de la CVC. **DECIMA CUARTA.- CESION.** Dado que el presente contrato se celebra teniendo en cuenta las calidades y características del contratista, le está prohibido a éste ceder total o parcialmente el mismo sin la autorización previa y escrita de LA CVC. **DECIMA QUINTA.- MODIFICACIONES.** El presente contrato podrá modificarse por mutuo acuerdo para suprimir o adicionar trabajos, suministros o servicios, en los términos del art. 16 de la Ley 80 de 1993, previo concepto técnico favorable de Interventor o Supervisor del contrato. **DECIMA SEXTA.- SUPERVISIÓN**. La supervisión, vigilancia y control en la ejecución del CONTRATO, se realizará con los lineamientos de la Ley 1474 de 2011 y el Manual de Supervisión e interventoría de LA CVC y demás normas concordantes. **Parágrafo 1**: El interventor o supervisor no tendrán autorización para exonerar al CONTRATISTA de ninguna de sus obligaciones, o deberes que emanen del presente Contrato, ni para imponerle

obligaciones distintas a las estipuladas en este Contrato, ni para exonerarlo de ninguno de los deberes y responsabilidades que conforme al mismo son de su cargo. Por lo tanto, dicho interventor o supervisor tampoco podrá impartir instrucciones al CONTRATISTA que impliquen modificaciones a los términos de este Contrato. Toda orden, recomendación o sugerencia del interventor o supervisor se entregará al CONTRATISTA por escrito y debe ajustarse a lo pactado en el presente contrato. **Parágrafo 2**: Será responsabilidad del interventor o supervisor, verificar, antes de autorizar el pago, el cumplimiento por parte del CONTRATISTA de las obligaciones con los sistemas de salud, riesgos profesionales o riesgos laborales, pensiones y aportes parafiscales y efectuar las correspondientes retenciones cuando sea del caso, dejando constancia de tal actuación en la respetiva acta de liquidación. **Parágrafo 3:** El interventor o supervisor ejercerá todas las actividades que le son propias, de conformidad con lo señalado en el contrato respectivo y en la reglamentación expedida para tal efecto por la Dirección General de la CVC. **DECIMA SEPTIMA.- DOCUMENTOS DEL CONTRATO.** Constituyen documentos del contrato los siguientes: **1)** La Propuesta presentada por el CONTRATISTA, **2)** Estudios y documentos previos, **3)** Pliego de Condiciones Definitivo, **4)** Adendas, los demás documentos mencionados en las consideraciones preliminares y todos aquellos requeridos para la presente contratación, conforme a la Ley 80 de 1993 y demás normas complementarias. **DECIMA OCTAVA.- INHABILIDADES E INCOMPATIBILIDADES.** EL CONTRATISTA declara bajo la gravedad del juramento que no se encuentra incurso en ninguna de las causales de inhabilidad e incompatibilidad o prohibición que consagra la Constitución Política y la Ley. **DECIMA NOVENA.- GARANTÍA ÚNICA.** El CONTRATISTA deberá constituir a favor de LA CVC, una Garantía que avale el cumplimiento de todas y cada una de las obligaciones surgidas del contrato y la ejecución idónea y oportuna del objeto contratado. Consistente en una póliza expedida por una Compañía de Seguros legalmente autorizada para funcionar en Colombia o en una Garantía bancaria la cual se mantendrá vigente durante la vida del contrato hasta su liquidación y la prolongación de sus efectos, se ajustará a los límites, existencia y extensión del riesgo amparado. Los riesgos a amparar son: **Amparo de Cumplimiento del Contrato:** por un monto equivalente al veinte por ciento (20%) del valor del contrato y con una vigencia que cubra el plazo de ejecución del contrato y seis (6) meses más, contados a partir de la fecha de la expedición de la póliza. **Amparo de Calidad del servicio:** por un valor equivalente al veinte por ciento (20%) del valor del contrato y con una vigencia de un (1) año, contado a partir de la fecha de suscripción del acta de entrega y recibo final, a entera satisfacción del supervisor designado por la CVC. **Amparo Pago de los Salarios, Prestaciones Sociales e Indemnizaciones:** del personal que hubiese empleado en la realización de las labores, por una cuantía equivalente al diez por ciento (10%) del valor total del contrato, con vigencia igual a la duración del contrato y tres (3) años más, contados a partir de la fecha de expedición de la póliza. **Parágrafo 1:** En el evento de concederse prórrogas en el plazo para la ejecución del contrato o celebrarse modificación al contrato, se procederá así: a) Si es prórroga del plazo se prorrogará la vigencia de la póliza en los correspondientes riesgos amparados, en el mismo término de la prórroga autorizada. b) Si es aumento del valor del contrato, aumentará el valor de los riesgos amparados en la garantía única y otorgada en igual proporción. Para adicionar o prorrogar la garantía única de cumplimiento, se le concede al CONTRATISTA un término perentorio de cinco (5) días hábiles a partir del perfeccionamiento de la adición al presente contrato o a la entrega de la copia de la minuta que adiciona el contrato. **Parágrafo 2:** En el evento en que por cualquier motivo LA CVC, haga efectiva la garantía constituida, EL CONTRATISTA se compromete a constituir una nueva garantía en la proporción y por el término respectivo amparando el riesgo correspondiente. **VIGESIMA.- OBLIGACIONES CON EL SISTEMA GENERAL DE SEGURIDAD SOCIAL**. De conformidad con lo señalado en el artículo 50 de la Ley 789 de 2002, concordado con el artículo 41 de la Ley 80

de 1993, modificado por el artículo 23 de la Ley 1150 de 2007, para la celebración del presente contrato, el CONTRATISTA deberá acreditar el cumplimiento de sus obligaciones frente al Sistema de Seguridad Social Integral y parafiscales, cuando a estas últimas hubiera lugar. **Parágrafo**: Al momento de liquidar el presente contrato, el Supervisor deberá verificar y dejar constancia en el Acta, del cumplimiento de las obligaciones del CONTRATISTA frente a los aportes mencionados, durante toda la vigencia del contrato, estableciendo una correcta relación entre el monto cancelado y la sumas que debió haber cotizado. En el evento en que no se hubiera realizado totalmente los aportes correspondientes, LA CVC deberá poner en conocimiento de dichos hechos a la Superintendencia Nacional de Salud y al Ministerio de Protección Social, a fin de que dichas entidades en cumplimiento de lo dispuesto en el artículo 5° de la Ley 828 del 2003, efectúen las investigaciones e impongan las sanciones a que hubiere lugar sobre el contratista que ha evadido o eludido el deber de cotizar a los Sistemas Generales de Pensión y Salud. **VIGÉSIMA PRIMERA.- RÉGIMEN LEGAL APLICABLE Y JURISDICCIÓN.** Este contrato se rige por las normas Civiles y Comerciales en concordancia con la Ley 80 de 1993, Ley 1150 de 2007, Decreto 1082 de 2015 y demás normas concordantes, en todo aquello que sea procedente. Las eventuales controversias que surjan de la celebración, ejecución, terminación o liquidación del contrato, serán competencia de la Jurisdicción Contencioso Administrativa, sin perjuicio de lo previsto en la cláusula siguiente. **VIGÉSIMA SEGUNDA.- LIQUIDACIÓN DEL CONTRATO.** A la terminación del contrato o al producirse una causa de terminación anticipada del mismo, se procederá a su liquidación, actuación que se llevará a cabo dentro de los cuatro (4) meses siguientes, de no adelantarse en este tiempo se procederá conforme con lo establecido en el Art. 11 Ley 1150 de 2007. **VIGESIMA TERCERA.- COMPROMISO ANTICORRUPCIÓN.** EL CONTRATISTA apoyará la acción del Estado Colombiano y particularmente la CVC podrá fortalecer la transparencia y responsabilidad de rendir cuentas, y en este contexto deberá asumir explícitamente los siguientes compromisos, sin perjuicio de su obligación de cumplir la Constitución y la Ley Colombiana tales como: 1).- EL CONTRATISTA se compromete a no ofrecer ni dar dadivas ni ninguna otra forma de halago a ningún funcionario público, ni pariente en cuarto grado de consanguinidad y segundo de afinidad y primero civil, ni a ningún asesor de LA CVC. 2).- El contratista se compromete formalmente a no efectuar acuerdos o realizar actos o conductas que tengan por objeto la colusión en la ejecución del presente contrato. **VIGÉSIMA CUARTA.- IMPUESTOS.** Todos los impuestos que se causen por razón de la suscripción, desarrollo, ejecución y liquidación del presente contrato, con excepción de los que estrictamente correspondan a LA CVC, son de cargo exclusivo del CONTRATISTA. En materia de impuestos, LA CVC efectuará a las cuentas o facturas del CONTRATISTA las retenciones que establezca la ley. **VIGÉSIMA QUINTA.- DIRECCIONES Y NOTIFICACIONES.** Las notificaciones o comunicaciones entre las partes contratantes deberán dirigirse a las siguientes direcciones: A la Corporación Autónoma Regional del Valle del Cauca - CVC en la Carrera 56 No. 11 – 36, Dirección Técnica Ambiental, piso 3° de la ciudad de Santiago de Cali y al CONTRATISTA en XXXXXXX. El cambio de dirección será notificado por escrito a la otra parte con la debida anticipación. Cualquier notificación, orden, instrucción o comunicación de la CVC, se dirigirá al CONTRATISTA, y será entregada personalmente a éste en sus oficinas o a través de correo certificado, caso en el cual la respectiva comunicación se considerará recibida dentro de los tres (3) días hábiles siguientes a la fecha de su despacho, salvo el caso en que dicha notificación, orden, instrucción o comunicación sea enviada a través de fax, confirmado telefónicamente, evento en el cual se considerará recibido el mismo día de su envío. **VIGESIMA SEXTA.- LUGAR DE EJECUCIÓN.** XXXXXXX. **Parágrafo**: EL CONTRATISTA, al momento de estar ejecutando el presente contrato en cualquiera de las instalaciones de la CVC, deberá dar aplicación a los Protocolos de Bioseguridad que establezcan las autoridades nacionales, con ocasión de la Pandemia del Covid-19, asumiendo

los costos que ello implique para todo su personal. **VIGÉSIMA SEPTIMA.- DOMICILIO CONTRACTUAL.** Sin perjuicio de las disposiciones procesales, para todos los efectos relacionados con el presente contrato, el domicilio será la ciudad de Santiago de Cali. **CLAUSULA VIGÉSIMA OCTAVA.- PERFECCIONAMIENTO Y EJECUCIÓN.** El contrato se entiende perfeccionado con la firma de las partes, para su ejecución se requiere de la expedición del Registro Presupuestal, la aprobación de la Garantía constituida por el CONTRATISTA y la certificación del Contratista de estar a paz y salvo en el sistema integral de seguridad social. Para constancia se firma en Santiago de Cali a los_días del mes de __de 2021,

LA CVC,

EL CONTRATISTA,

FORMATO No. 1
CARTA DE PRESENTACIÓN DE LA PROPUESTA

Ciudad y Fecha

Señores:
Corporación Autónoma Regional del Valle del Cauca-CVC
Oficina de Tecnologías de la Información

El suscrito, _____ (persona natural o jurídica, cédula de ciudadanía o NIT.), en representación de_____(razón social o nombre persona jurídica, consorcio o unión temporal), por medio de la presente someto a su consideración, la propuesta para XXXXXXX, de acuerdo con los requisitos establecidos en el Pliego de Condiciones de la Selección Abreviada de Menor Cuantía No. 38 de 2021.

En caso de que me sea adjudicado el contrato, me comprometo a cumplir estrictamente de acuerdo con el plazo y lugar de ejecución, así como el valor ofertado, las obligaciones o especificaciones técnicas establecidas en el Pliego de Condiciones, en las Adendas, en sus Anexos y en los Estudios y Documentos Previos.

El suscrito declara expresamente:

a) Que ninguna persona o entidad distinta a las aquí nombradas tiene interés en esta propuesta ni en el contrato, que, como consecuencia de ello, en caso de que llegue a celebrarse el contrato, este solo compromete a los firmantes.

b) Que he estudiado los documentos de la Selección Abreviada de Menor Cuantía, sus adendas, la información sobre preguntas y respuestas (de ser del caso) y por ello acepto todos los requisitos, condiciones técnicas y obligaciones para el cumplimiento del objeto contractual, en ellos estipulados.

c) Que he analizado todas las circunstancias que inciden en la determinación de precios de la propuesta y que mi precio ofertado no variará durante la ejecución del contrato, salvo, en aquello expresamente autorizado en los pliegos de condiciones.

d) Que en caso de que se me adjudique el contrato, me comprometo a formalizarlo con base en los documentos de la Selección Abreviada de Menor Cuantía y otorgar las garantías que se establecen en el pliego de condiciones y en la minuta del contrato.

e) Que he recibido a través del SECOP II, la siguiente información de la Selección Abreviada de Menor Cuantía.

INFORMACIÓN SOBRE PREGUNTAS Y RESPUESTAS	FECHA DE RECIBO

ADENDAS Nº	FECHA DE RECIBO

f) El suscrito declara bajo la gravedad de juramento que no se encuentra incurso en ninguna de las inhabilidades e incompatibilidades de que trata la Ley 80 de 1993, adicionado la Ley 1150 de 2007 y por la Ley 1474 de 2011.

g) El suscrito representante legal de la sociedad proponente declara bajo juramento que ni él ni los demás representantes legales de la misma, ni sus socios se encuentran incursos dentro de las causales de inhabilidad e incompatibilidad a que se refiere el artículo 8º de la Ley 80 de 1993.

h) Informo que la dirección a la cual se me puede dirigir correspondencia, es la siguiente:

Dirección:
Ciudad:
Teléfonos:
Correo electrónico:

i) Información de la persona o personas que suscribirá(n) el contrato en caso de adjudicación del mismo:

Nombre(s) completo(s), identificación (número y lugar de expedición del documento) y cargo(s)

j) La presente oferta tiene vigencia por espacio de xxxx (xx) días calendario contados a partir del cierre de la Selección Abreviada de Menor Cuantía CVC 38 de 2021

k) Con la firma del presente documento se entiende que el proponente conoce y acepta las obligaciones del Anexo No. 2 “Pacto de Transparencia”.

l) Con la firma del presente documento se expresan los cumplimientos en el Anexo

Corporación Autónoma Regional del Valle del Cauca

No. 1 ANEXO TECNICO, Literal B, Características Técnicas.

ITEM	LICENCIAMIENTO	ESPECIFICACIÓN	DESCRIPCIÓN	CUMPLE SI/NO	OBSERVACIÓN
1	solución de protección para endpoint con integración incluida a plataforma XDR	MARCA	DILIGENCIAR		
1.1.1		VERSIÓN	DILIGENCIAR		
1.1.2		CANTIDAD	836		
1.1.3		SOLUCIÓN DE PROTECCIÓN PARA ENDPOINT	Debe ser una solución que fusione una serie de técnicas avanzadas de protección contra amenazas entregadas a través de una arquitectura de agente único		
1.1.4			La solución debe tener la capacidad de brindar proteccion con los siguientes elementos: machine learning de alta fidelidad (en pre-ejecución y en ejecución), análisis de comportamiento (contra ataques de scripts, inyección, ransomware, memoria y navegadores), análisis en memoria para identificación de malware fileless, protección contra variantes, reputación web, prevenció de explotación de vulnerabilidades, bloque de comando y control, protección contra fuga de información DLP, control de dispositivos y aplicaciones, recuperación ante ransomware (ransomware rollback), detección y respuesta extendida XDR		
1.1.5			Debe contar con los siguientes módulos de protección incluídos dentro del licenciamiento sin la necesidad de activar a adquirir licenciamientos adicionales: Antimalware, Reputación Web, Firewall, Machine Learning, IDS/IPS, Control de aplicaciones, Data Loss Prevention DLP, Control de dispositivos.		
1.1.6			La solución debe brindar alta disponibilidad del servicio		

1.2.1		CONSOLA DE ADMINISTRACION	La consola de administración debe permitir administrar los agentes instalados en la red de equipos. Permitiendo conocer el estado de los agentes.		
1.2.2			La consola de administración debe estar despleagada en la Nube para garantizar la administración en todo el tiempo sin importar el lugar donde estén las maquinas administradas		
1.2.3			La consola de administración debe permitir agrupar los agentes en grupos para facilitar la configuración y administración de los mismos.		
1.2.4			La consola de administración debe permitir configurar notificaciones sobre riesgos de seguridad y ver los Logs enviados por los agentes sobre los eventos de los mismos.		
1.2.5			La consola de administración debe proporcionar un Dashboard que brinde información global sobre los agentes, eventos de reputación web, usuarios afectados, eventos de comando y control, incidentes de filtración de datos, entre otros e igualmente debe permitir que secciones o widgets sean agregados o eliminados según se requiera.		
1.2.6			La consola de administración debe permitir consultar los Logs de instalación tanto del agente como el del servidor de administración.		
1.2.7			La consola de administración debe permitir visualizar estadísticas de históricos de actualizaciones de patrones de análisis de antivirus, antispyware, análisis de comportamiento, conexiones		

			sospechosas, y exploits de los navegadores de internet.		
1.2.8			La consola de administración debe permitir visualizar los logs de los eventos sobre los equipos donde se encuentra instalado el agente, dichos eventos deben estar relacionados a temas de malware, spyware, reputación web, conexiones sospechosas, archivos sospechosos, Command & Control Callbacks, Behavior Monitoring, Machine Learning, control de dispositivos, DLP, y escaneos. Adicionalmente la solución debe permitir filtrar dichos logs por periodos de tiempo preestablecidos, por rangos de fechas y por tipo de escaneo.		
1.2.9			La consola de administración debe permitir la visualización de los logs de registro de los eventos de la actualización del servidor de actualizaciones.		
1.2.10			La consola de administración debe permitir la visualización de los logs de registro de los eventos del servidor de administraciones.		
1.2.11			La consola de administración debe tener la capacidad de generar reporte en formato PDF, DOCX y XLSX		
1.2.12			La consola debe poder operarse en la nube sin requerir recursos de infraestructura y entregarse como software como servicio		
1.2.13			La solución debe tener la capacidad de finalizar sesiones en la consola de administración por tiempo de inactividad		

1.2.14			La solución debe tener la capacidad de eliminar de los logs de los eventos del sistema, servidor y agentes, para que estos sean eliminados con una frecuencia especifica		
1.2.15			La solucion debe permitir la configuracion de proxy tanto para los agentes como para el servidor de administracion.		
1.2.16			La solución debe permitir la realización de backups de los datos de configuraciones de la solución, los certificados SSL, datos de los agentes, y logs almacenados en el servidor de administración.		
1.2.17			La solución debe permitir la realización de backups de los logs almacenados en los agentes.		
1.2.18			La consola de administración de la solución debe proporcionar gráficos y estadísticas de distribución de la solución, distribución de políticas y agentes administrados.		
1.2.19			La solución debe tener la capacidad de identificar o agrupar los logs por políticas, inventario de equipos, aplicaciones conocidas, acciones del administrador,		

			mensajes de los agentes y mensajes del servidor.		
1.2.20			La solución debe permitir realizar una sincronización de la lista de objetos sospechosos obtenidos de otras soluciones del mismo fabricante.		
1.2.21			La solución debe contar con roles definidos con diferentes niveles de acceso para editar y/o visualizar los datos y configuraciones de la solución.		
1.2.22			La solución debe permitir realizar búsquedas en los registros o logs, haciendo uso de filtros y permitir exportarlos en archivos con formato (CVS o XLSX).		
1.2.23			Se podrán crear usuario y roles para el acceso a la plataforma de administración		
1.2.24			La solución propuesta debe contar con un Dashboard el cual permita visualizar en tiempo real C&C, Ancho de banda usado, amenazas detectas, estado del servidor, estado de los agentes		

1.2.25			Es requisito contar con la habilidad de configurar permisos granulares en la consola de administración para delegar operaciones y trabajos específicos a diversos usuarios o grupos de usuarios, así como perfiles de auditoría que solo permitan visualizar datos, pero sin la capacidad de modificar ninguna configuración		
1.3.1		AGENTES	Los agentes deben ser instalados mediante instalación web, link de instalación por correo, instalación por script, instalación remota, y/o paquete de instalación.		
1.3.2			Los agentes deben requerir contraseña de administración para ser desinstalados de los equipos.		
1.3.3			Las políticas de seguridad deben aplicarse en los agentes de forma individual y/o por grupos.		
1.3.4			El agente debe tener la capacidad de eliminar los archivos sospechosos de forma automática.		
1.3.5			El agente debe estar integrada en un solo agente para dar protección de amenazas, protección de vulnerabilidades, control de aplicaciones y DLP		
1.3.6			Los agentes deben tener la capacidad de conectarse a múltiples fuentes de actualización (patrones, firmas, url sospechosas, etc), si alguna de estas es inaccesible para el agente.		

1.3.7			Los agentes de proteccion de los equipos deben tener la capacidad de protegerse contra intentos de desinstalacion o cancelacion de los procesos por los usuarios o por una aplicación de terceros.		
1.3.8			La solución debe permitir el uso de protocolos SSL para la comunicación entre los agentes y el servidor de administración.		
1.4.1		Regulatorios y cumplimiento	La solución debe estar ubicada en el cuadrante de líderes de Gartner conocido como “Magic Quadrant for Endpoint Protection Platforms” mínimo en los últimos 5 años anteriores.		
1.4.2			La solución debe estar listada como líder en el último cuadrante de Forrester de Endpoint Security Suites y Endpoint Detections and Responses		
1.5.1		Sistemas Operativos soportados	Windows 7 (32-bit / 64-bit) Service Pack 1		
1.5.2			Windows 8.1 (32-bit / 64-bit)		
1.5.3			Windows 10 (32-bit / 64-bit)		
1.5.4			Windows Server 2008 R2 (64-bit)		
1.5.5			Windows MultiPoint Server 2010 (64-bit)		
1.5.6			Windows MultiPoint Server 2011 (64-bit)		

1.5.7			Windows Server 2012 (64-bit)		
1.5.8			Windows Server 2016 (64-bit)		
1.5.9			Windows Server 2019 (64-bit)		
1.6.1		ANTIMALWARE	La solucion debe tener la capacidad de brindar proteccion contra malware, virus de red, conecciones sospechosas, amenazas web, spyware, trojanos, monitoreo de comportamiento, ataques conbinados y ataques de dia cero para equipos de punto final (Endpoint).		
1.6.2			La solución debe contar con firewall (reglas de conexiones de aplicación, IP, puerto y protocolo), reputación de archivos y/o reputación web.		
1.6.3			La solución debe permitir realizar escaneos de los endpoint de forma manual, programada y en tiempo real.		
1.6.4			La solución debe tener la capacidad de aislar los equipos o ponerlos en cuarentena cuando se detecta algún ataque para evitar la propagación de este dentro de la red.		
1.6.5			La solución debe permitir la integración con Active Directory		
1.6.6			La solución debe permitir realizar una migración a versiones superiores de la misma conservando las configuraciones, incluida la base de datos.		
1.6.7			La solución debe permitir recuperar los archivos que sean enviados a cuarentena.		
1.6.8			La solución debe proporcionar protección a los agentes contra Ramsomware		

1.6.9			La solución debe proporcionar una consola de administración que pueda ser utilizada desde un entorno web.		
1.6.10			La solución debe tener la capacidad de analizar la reputación de archivos		
1.6.11			La solución debe permitir la creación, modificación y eliminación de roles y usuarios para la administración de la misma.		
1.6.12			La solución debe tener la capacidad de proteger los equipos que se encuentren dentro de la red y fuera de ella		
1.6.13			La solución debe tener la capacidad de programar las sincronizaciones de los equipos para horas y fechas específicas		
1.6.14			La solución debe permitir la configuración de un servidor SMTP para el envío de notificaciones vía Email		
1.6.15			La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas al administrador, cuando una amenaza sea detectada		
1.6.16			La solución debe permitir la configuración de la plantilla del correo para el envío de notificaciones		

1.6.17			La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas al administrador, cuando uno de los equipos sea enviado a cuarentena.		
1.6.18			La solución debe permitir la configuración de la plantilla del correo para el envío de notificaciones cuando los equipos sean enviados a cuarentena.		
1.6.19			La solución debe permitir la configuración de los tipos de eventos que serán notificados y visualizados en el agente, y adicionalmente configurar el mensaje de las alertas dependiendo de la criticidad del evento (High, Medium, Low)		
1.6.20			Proteccion de Exploración de la memoria: identificando procesos en ejecución a medida que se ejecuta en la memoria para determinar si es malicioso. Permite terminar el proceso en ejecución dependiendo de la configuración de la acción.		
1.6.21			Protección contra ataques de exploits: controla los programas que demuestran un comportamiento anormal asociado con ataques de exploits.		
1.6.22			Protección de exploits de documentos: escanee documentos en busca de códigos de exploits integrados y vulnerabilidades conocidas		
1.6.23			Aprendizaje automático: analiza archivos desconocidos de baja prevalencia al extraer características de los archivos para examinarlos utilizando algoritmos de aprendizaje automático para determinar si el archivo es malicioso (es decir, malware / ransomware / amenazas de dia 0).		

1.6.24			Protección contra ransomware: busca la ofuscación / cifrado rápido de archivos mediante un proceso desconocido, elimina ese proceso y restaura los archivos cifrados.		
1.6.25			La solucion debe permitir la detección de amenazas tipo Fileless a través de la exploración de memoria mejorada para detectar comportamientos de procesos sospechosos. El agente debe tenre la capacidad de terminar los procesos sospechosos antes de que se pueda hacer cualquier daño.		
1.6.26			La solucion debe permitir proteger los equipos frente a vulnerabilidades no conocidas presentes en los equipos		
1.7.1		DLP- DATA LOSS PREVENTION	La solucion debe tener la capacidad de prevenir y/o informar sobre la fuga o perdida de informacion sensible de la organización ya sea de forma accidental o deliberada.		
1.7.2			La solucion debe permitir identificar o configurar los activos digitales que se desean proteger.		
1.7.3			La solucion debe permitir la creacion de politicas que limiten la trasmision o transferencias de activos digitales por los canales de comunicación convencionales (email y/o dispositivos externos).		
1.7.4			La solucion debe tener la capacidad de igualmente brindar proteccion y aplicar politicas para transferencia de activos digitales mediante cliente de correo ya sera software o web.		
1.7.5			La solucion debe permitir que la organización haga cumplir con las normas de privacidad establecidas.		

1.7.6			La solucion debe tener la capacidad de brindar proteccion contra filtrado de datos sensibles y proporcionar un control de dispositivos, permitiendo confugurar reglas o politicas para ser aplicadas a grupos o agentes individuales.		
1.7.7			La solucion debe proporcionar identificadores de datos y/o plantillas para la creacion de politicas.		-
1.7.8			La solucion debe tener la capacidad de identificar o reconocer archivos ejecutables, documentos, graficos vectoriales, archivos multimedia, archivos comprimidos, bases de datos, hojas de calculo, presentacion, archivos vinculados e incrustados, y/o archivos encriptados.		-
1.7.9			La solucion debe tener la capacidad de localizar activos digitales almacenados en portatiles, equipos de escriotorio, y servidores.		-
1.7.10			La solucion debe tener la capacidad de proporcionar filtros de proteccion para canales de red como FTP o HTTP, canales de aplicaciones o perifericos.		-
1.7.11			La solucion debe tener la capacidad de detectar datos estructurados y no estructurados.		-
1.7.12			La solucion debe mantener un monitoreo constante.		-
1.7.13			La solución debe proveer plantillas que permitan el cumplimiento de estándares como GLBA, HIPAA, PCI-DSS o SB-1386		-
1.7.14			La solucion debe permitir generar un control de dispocitivos externos al equipo, generando bloqueos y alertas pero permitir dispocitivos por su ID,		-
1.7.15			La solución debe permitir la integración con Directorio Activo y permitir la delegación de administración		-

1.7.16			La solución debe contar con una consola de administración WEB que permita la configuración de políticas e implementaciones, reportes de los equipos, extracción de huellas digitales, y actualizaciones.		-
1.7.17			La solucion debe tener la capacidad de identificar los activos digitales almacenados en los dispositivos o el trafico en la red utilizando expresiones regulares (predefinidas y/o personalizadas), atributos de archivos (tipo y/o tamaño), huellas digitales, palabras clave, y/o plantillas (predefinidas y/ personalizadas)		-
1.7.18			Las plantillas de identificación de activos digitales deben permitir combinar identificadores de datos (expresiones, atributos de archivos, huellas digitales, lista de palabras).		-
1.7.19			La solución debe permitir usar plantillas predefinidas por el fabricante, personalizarlas, crear plantillas, importar plantillas, exportar plantillas, y eliminar las plantillas.		-
1.7.20			La solución debe permitir implementar políticas independientes tanto para agentes en los dispositivos como para agentes en la red.		-
1.7.21			La solución debe permitir generar reportes ya sea por demanda o de forma programada (Diario, semanal o mensual), estos reportes deben contener información de los logs de los agentes. Dichos reportes deben mostrar información relevante como top de incidentes, información resumida, reporte de auditoria, entre otros.		-
1.7.22			La solución debe permitir almacenar reportes y estos deben estar disponibles en formatos PDF, HTML, o Microsoft Excel		-

1.7.23			La solución debe tener la capacidad de administrar los logs de manera que pueda eliminar los Logs que tengan un tiempo de más de 90 días, igualmente debe permitir la realización de un backup y limpieza de los mismos de forma manual.		-
1.7.24			La solución debe soportar la detección de fuga de información en los siguientes tipos de archivo: .pdf .odt, .ott, .stw, .sxw .wpd, .wps .xml .xbd, .xdw .htm .jtd .sam .doc, .docm, .docx, .dot, .dotm, .dotx .wri .rtf .sgml .wsd, .bmp .dib .dcm .eps .img .gif .jpg .mac .png .tif, .tiff .ico .pcx, .dxf .dwg, .dws .cel, .dgn .cdb .CATDrawing, .CATPart, .CATProduct .cdr .dvi .gds .attr, .sgfx, .ssht .drw .ps .prt .svf .prtdot, .sldasm, .slddrw, .sldprt, .swf .aiff .mod .mov .avi .mid .mpeg .mpg .au .wav .wma .wmv, .7z .arc .arj .bz2 .Z .cpio .gz .lzh .chm .msg .pst .dbx .eml .pgp .rar .shar .tar .rpm .uue .zip, .sas .db .dif .dbf .fp7 .tbl .accdb, .mdb, ods, .ots, .stc, .sxc .csv .123 .wk1 .wk3 .wk4 .wke .wks .xlam .xlc .xls .xlsb .xlsm .xlsx .xltm .xltx .xlw .qpw .wb3 .wb2 .wb1 .wq1, .odp, .otp, .sti, .sxi .shw .pre .pot, .potm, .potx, .pps, .ppsm, .ppsx .ppt .pptm .pptx .vdw, .vdx, .vsd, .vss, .vst, .vsx, .vtx, .7z, .rar, .zip .accdb, .doc, .docx, .pdf, .ppt, .pptx, .w b1, .wb2, .wq1, .wpd, .xls, .xlsx, .mml .pub .qxp .one .mpp .hlp .iam, .idw, .ipt, .msoffice, .pqw y .pif		-
1.7.25			La solución debe permitir configurar las fuentes de actualización para los parches o hot fixes y adicionalmente permitir configurar la periodicidad de las mismas.		-
1.7.26			La herramienta de análisis local debe tener la capacidad de adquirir huellas digitales para los archivos almacenados en el equipo.		-

1.7.27			La solución provee expresiones predefinidas para los números de tarjetas de crédito. A estos números se les realiza una verificación adicional por el número de prefijo y verificación con LUHN.		-
1.7.28			La solución provee expresiones predefinidas para las direcciones de correo electrónico		-
1.7.29			La solución provee expresiones predefinidas para los números de cuentas de bancos internacionales (IBAN).		-
1.7.30			La solución provee expresiones predefinidas para códigos de identificación de negocio SWIFT BIC.		-
1.7.31			La solución provee una lista de palabras predefinidas para la validación de formularios como fecha de nacimiento, fecha de expiración, Nombres y apellidos, lugar de nacimiento, departamentos o ciudades y direcciones de domicilios.		-
1.7.32			La solución provee una lista de palabras que pueden ser usadas en contextos ofensivos, racistas o que incluyan elementos para causar daño (armas)		-
1.7.33			La solución provee una lista de palabras que puedan identificar comandos o instrucciones en lenguajes de programación como C#, C/C++, COBOL, Java, Perl y VB.		-
1.7.34			La solución debe permitir exportar e importar datos como políticas de seguridad y roles de usuarios		-

1.7.35			La solución debe permitir configurar y programar el reinicio de los dispositivos de forma que no afecte negativamente las operaciones de la organización.		-
1.7.36			la solución debe permitir la implementación de políticas para evitar que los usuarios publiquen contenido en clientes de mensajería instantánea o sitios de webmail		-
1.8.1		CONTROL DE APLICACIONES	La solución debe tener la capacidad de prevenir la ejecución de aplicaciones no deseadas o desconocidas en los endpoint		-
1.8.2			La solución debe tener la capacidad de configurar acciones sobre los archivos que estén en la lista de Suspicious Objects proporcionada por el fabricante para sus soluciones de seguridad.		-
1.8.3			La solución debe permitir bloquear o permitir aplicaciones de acuerdo a puntaje de seguridad propio del fabricante.		-
1.8.4			La solución debe tener la capacidad de bloquear o permitir aplicaciones basada en patrones y puntaje de prevalencia de la aplicación.		-
1.8.5			La solución debe permitir establecer reglas para el cumplimiento de control de aplicaciones, dichas reglas deben permitir o bloquear aplicaciones de acuerdo con las políticas de la organización.		-

1.9.1		PROTECCION WEB	La solución debe contar con reputación web adicional reputación de archivos		-
1.9.2			La solución debe permitir el filtrado URL		-
1.9.3			La solución debe permitir realizar un control de Ancho de Banda		-
1.9.4			La solución debe permitir la inspección de trafico HTTP Y HTTPS		-
1.9.5			La solución debe proteger la navegación en los equipos portátiles, endpoint y equipos que salen de la red corporativa		-
1.9.6			El filtrado de URL de la solución debe estar definido por niveles de riesgo establecidos por el fabricante		-
1.9.7			Si una URL no está en la base de datos para verificar su confiabilidad esta debe ser testada en tiempo real utilizando tecnología de categorización dinámica		-
1.10.1		PLATAFORMA XDR	Debe permitir a la entidad tener la capacidad de detección y respuesta en email, endpoints, servidores, workloads en la nube y la red a través de una sola plataforma, es decir, poder hacer estas tareas de detección y respuesta en múltiples capas.		-

1.10.2			Debe proveer un mejor contexto y un análisis más profundo, para que la entidad pueda responder de forma más rápida y eficiente a amenazas, minimizando el impacto y alcance de un incidente en la organización		-
1.10.3			debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques.		-
1.10.4			Los modelos de correlación deben combinar multiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.		-
1.10.5			La Plataforma de XDR debe proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad		-
1.10.6			Debe proveer una vista de alertas (llamadas workbenches) con la capacidad de investigar más a fondo.		-
1.10.7			Las alertas deben permitir ver un análisis de causa raíz (también llamado Execution Profile) identificar el alcance del impacto y permitir tomar acciones de respuesta.		-
1.10.8			Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado).		-
1.10.9			Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.		-
1.10.10			debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.		-

1.10.11			Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las accionas que una amenaza llevó a cabo en un servidor, endpoint, o carga de trabajo en la nube.		-
1.10.12			Debe permitir investigar adicionalmente desde la perspectiva de red (Network Analysis) para reproducri las comunicaciones y ver el detalle de acciones de un atacante como comunicaciones de comando y control o movimientos laterales.		-
1.10.13			Debe permitir la búsqueda proactiva a traves de endpoint, red, email, y servidores (como telemetría, NetFlow, metadata, etc.) usando un simple constructor de consultas.		-
1.10.14			Debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros, y filtrar los resultados añadiendo criterios adicionales de búsqueda.		-
1.10.15			Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz.		-
1.10.16			Se debe poder construir, guardar y reutilizar búsquedas para Threat Hunting básico		-
1.10.17			Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el vendor		-
1.10.18			La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campana asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a		-

			entradas de blog relacionados si están disponibles.		
1.10.19			Enlaces desde el workbench a la documentación del framework de MITRE ATT&CK		-
1.10.20			En una sola ubicación debe poder iniciar y ver estado de respuesta en endpoint, email, servidores y red.		-
1.10.21			Debe ofrecer opciones de respuesta “context aware” para acciones rápida desde la plataforma.		-
1.10.22			Debe permitir ejecutar acciones de respuesta rápidamente haciendo click derecho en el workbench o desde los resultados de búsqueda de Threat Intelligence		-
1.10.23			Una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR.		-
1.10.24			Debe proveer un conector para Splunk nativo		-
1.10.25			Debe ser una solución hospedada y administrada en Nube (SaaS) para tomar ventaja de tecnologías Cloud		-
1.10.26			debe analizar la data recolectada por los sensoress para proveer alertas inteligentes, y detecciones de alta fidelidad.		-

1.10.27			Los sensores deben soportar integración nativa del vendor para obtener toda la data de actividad (telemetria, metadata, netflow) no solo data de alertas.		-
1.10.28			Los sensores deben soportar trabajar al menos en los siguientes sistemas operativos de Estaciones de trabajo de usuarios: Windows 7 y superior Mac OS X El Capitan 10.11 y superior		-
1.10.29			Los sensores deben soportar trabajar al menos en las siguientes sistemas operativos de servidores Windows (Windows 2008 y superior) Linux (Including visibility over docker containers attacks) Red Hat Enterprise Linux 6 y superior Ubuntu 16 y superior CentOS 6 y superior Debian 8 y superior Amazon Linux/Amazon Linux 2 Oracle Linux 6 y superior SUSE Linux Enterprise Server 12 y superior CloudLinux 7 y superior		-
1.10.30			Los sensores deben soportar trabajar por integración directa vía API con los proveedores de correo Microsoft 365 & G Suite		-
1.10.31			Los sensores deben soportar trabajar Network por integración nativa con sistema BDS		-
1.10.32			En el caso de estaciones de trabajo de usuarios y servidores, la funcionalidad XDR debe ser una capacidad que puede tener embebida en el mismo agente de protección de endpoint. XDR no debe ser un agente adicional		-
1.10.33			Los modelos de detección deben consistir en uno o mes conjunto de filtros que integran recursos internos y externos como las técnicas y tácticas de MITRE ATT&CK		-

1.10.34			El vendor debe constantemente refinar y añadir modelos de detección y filtros para mejorar las capacidades de detección y reducir falsos positivos to improve.		-
1.10.35			Los modelos deben priorizar la respuesta del administrador en base a puntajes (score).		-
1.10.36			El aplicativo de Detection Model Management debe permitir controlar el tipo de alertas que se disparan y se envían a Workbench.		-
1.10.37			Los modelos deben tener una severidad asociada dependiendo del tipo de evento y la información de MITRE. Critical: Hay fuerte evidencia de compromiso por un ataque dirigido, APT u operaciones de cibercrimen. High: Hay indicadores altamente sospechosos de compromiso por un ataque dirigido, APT u operaciones de cibercrimen Medium: Hay indicadores sospechosos posiblemente relacionados con infección de malware, violación de políticas u operaciones de cibercrimen. Low: Hay indicadores levemente sospechosos. Usado para monitoreo y Threat Hunting		-
1.10.38			Los modelos deben especificar para que productor en específico (Workstation/Server/Email/Network) aplica una alerta		-
1.10.39			Los modelos deben especificar y permitir modificar “status”: encendido/apagado		-
1.10.40			Los modelos deben especificar la ultima vez que se actualizó		-

1.10.41			Debe hacer una sección de excepciones dentro de la App de Model Management que despliegue todas las excepciones que se añadieron.		-
1.10.42			La excepcion debe ser granular y debe mostrar lo siguiente: Object: El objeto que se ha añadido como excepción en una investigación Filter: El filtro que identificó el objeto como un indicador de amenaza Type: El atributo del objeto añadido Data field: Log definido por el objeto Match type: Exacto o Parcial (soporta wildcards) Description: Información definida por el usuario para la excepción Created: Fecha y hora en que se añadió la excepción Created by: Usuario que creó la excepción		-
1.10.43			Debe permitir añadir excepciones durante la investigación de una alerta.		-
1.10.44			En el proceso de añadir una excepción se debe poder definir una descripción para documentar la excepción		-
1.10.45			Debe integrar inteligencia al minuto con reportes del vendor y terceras partes confiables para ayudar a identificar amenazas		-
1.10.46			Debe poder analizar los logs, comparar la data contra los reportes de Threat Intelligence automáticamente, y generar alertas basadas en indicadores sospechosos o maliciosos detectados		-

1.10.47			La App de Workbench debe mostrar alertas por los modelos de detección y permitir investigar a más detalle. La data del Workbench debe incluir: Status: New/In Progress/Closed/Closed – False Positive Score: basado en la severidad del modelo de detección y el impacto de la alerta. Workbench ID: identificador único para la alerta Model: Modelo que disparó la alerta Model severity: Severidad asignada al modelo que disparó la alerta Impact scope: Número de entidades afectadas por Servers/Workstations/Users/Cuentas de correo Created: Fecha y Hora que XDR generó la alerta		-
1.10.48			Endpoint Profile: Debe incluir Hostname/IPv4/GUID/MAC Address/OS version/Producto/Último usuario que inció sesión		-
1.10.49			Email Profile: debe incluir: Asunto del correo/Message ID/Risk level/Fecha y hora del correo/Dirección de remitente/dirección de destinatarios/Información de cada adjunto al correo/URLs embebidas/Cabecera del correo		-
1.10.50			Despliega el análisis de causa raíz y provee información adicional que puede ser útil para la investigación.		-
1.10.51			Debe desplegar un análisis visual de los objetos envueltos en un evento		-
1.10.52			Debe resaltar los objetos en la cadena que son posiblemente maliciosos		-

1.10.53			Debe desplegar el objeto o la lista de objetos que coinciden con los criterios de investigación definidos		-
1.10.54			Debe resaltar el objeto “mas probable” que creó el objeto que coincidió con el criterio de investigación.		-
1.10.55			Debe desplegar detalles del endpoint que fue investigado		-
1.10.56			La cadena de análisis debe usar íconos para los distintos tipos de objetos (servidor/endpoint/url/archivos, etc…). La descripción debe estar directamente en la ventana de investigación para entender rápidamente la relación entre los distintos objetos.		-
1.10.57			Debe poder obtenerse una representación visual de correlación de eventos de la perspectiva de la red y no del endpoint.		-
1.10.58			Network Analytics debe usar como sensor al BDS (Breach Detection System) y debe proveer integración nativa para compartir no solo eventos sino el contexto entero (toda la telemetría posible).		-
1.10.59			Debe tener una barra de reproducción (play/pause) con un “time slider” para ver eventos correlacionados vs tiempo		-
1.10.60			Cada gráfica de correlación debe tener 1 o más líneas de correlación que muestran actividad maliciosa o sospechosa entre un origen y destino.		-
1.10.61			Cada línea de correlación representa 1 o más transacciones entre 2 hosts.		-

1.10.62			El grosor de la línea es proporcional al número de transacciones entre los hosts. Al colocar el mouse sobre la línea debe mostrar el número de transacciones para esa línea de correlación		-
1.10.63			La línea de correlación debe poder ser entre host interno y externo. También debe poder ser entre 2 hosts internos (para identificar movimientos laterales).		-
1.10.64			Cada línea de correlación debe indicar los protocolos usados. Y debe existir una flecha para indicar direccionalidad de la comunicación.		-
1.10.65			Debe identificar actividades claves para hosts internos y externos en la gráfica.		-
1.10.66			Debe incluir actividades similares a: Machine Learning, Lateral Activity, Detected Event, C&C Activity, and Malicious Download.		-
1.10.67			Correlation Information Pop-up Window: Debe incluir los sigueintes campos: Source IP/Destination IP/Severity/URLs/Hashes/Protocols/Number of transactions/Reason/Earliest date/Latest date		-
1.10.68			Response Management app: Debe permitir tomar acciones y llevar registro de las acciones tomadas.		-
1.10.69			Debe responder a amenazas sin dejar la consola de XDR.		-

1.10.70			Debe haber distintas acciones que se puedan tomar en los objetos maliciosos/sospechosos. Añadir a lista de bloqueo Eliminar de lista de bloqueo Terminar procesos en endpoints Recolectar archivos en endpoints Bloquear remitente de correo Poner en cuarentana un correo Borrar un correo Aislar un equipo Restaurar la conexión en equipos aislados		-
1.10.71			Después de activar la respuesta a un evento u objeto, debe poderse ver el estado de la tarea de respuesta y los detalles de comando en una tabla de Gestión de Respuesta		-
1.10.72			Debe permitir realizar barridos IoC, personalizar búsquedas por especificación de parámetros, filtros y otros criterios y búsqueda de múltiples eventos que ocurraen en un mismo Endpoint		-
1.10.73			Debe tener un constructor de peticiones que debe permitir combinar atributos de búsqueda, operadores y especificar valores en una misma petición de búsqueda		-
1.10.74			Debe listar busquedas previas		-
1.10.75			Debe permitir guardar búsquedas para encontrar nueva data relacionada a los mismos criterios.		-
1.10.76			El administrador debe poder ver los queries guardados		-
1.10.77			Debe ser fácil limpiar los criterios de búsqueda		-

1.10.78			Los resultados deben ser exportables a CSV o JSON		-
1.10.79			Los resultados deben mostrar origen de los datos (workstation/servidor/email/network)		-
1.10.80			El administrador debe ser capaz de ver los logs en RAW		-
1.10.81			debe permitir diferentes tipos de búsquedas, filtros, y un lenguaje de consultas basado en Kibana para identificar, categorizar y obtener los resultados de búsqueda.		-
1.10.82			La configuración administrativa de XDR debe brindar a los usuarios la capacidad de configurar cuentas de usuario, roles y configuraciones, conectar productos adicionales y configurar opciones de monitoreo adicionales. Las siguientes opciones deben estar disponibles: SAML Single Sign-On Account Management Role Management Product Connector Alert Notifications Audit Logs Remote Support		-
1.11.1		GARANTIA	soporte directo de fabricante con una disponibilidad 7x24 para atención de incidentes y contar con actualizaciones de software por la vigencia del contrato		-
1.11.2			Soporte directo de fabricante para la atención de incidentes de forma remota por medio de correo electrónico y telefónico.		-

1.11.3			El fabricante deberá contar con un servicio de laboratorio de investigación en español para proporcionar de forma rápida actualizaciones de bases de firmas de virus sobre amenazas enfocadas en regiones hispanohablantes		
ITEM	**LICENCIAMIENTO**	**ESPECIFICACIÓN**	**DESCRIPCIÓN**	**CE**	**FOLIO**
2	licencias para asociar a plataforma XDR	MARCA	DILIGENCIAR		
2.1.1		VERSIÓN	DILIGENCIAR		
2.1.2		CANTIDAD	166		
2.2.1		Sistemas Operativos soportados	Windows 7 (32-bit / 64-bit) Service Pack 1		
2.2.2			Windows 8.1 (32-bit / 64-bit)		
2.2.3			Windows 10 (32-bit / 64-bit)		
2.2.4			Windows Server 2008 R2 (64-bit)		
2.2.5			Windows MultiPoint Server 2010 (64-bit)		
2.2.6			Windows MultiPoint Server 2011 (64-bit)		
2.2.7			Windows Server 2012 (64-bit)		
2.2.8			Windows Server 2016 (64-bit)		
2.2.9			Windows Server 2019 (64-bit)		

2.3.1		PLATAFORMA XDR	Debe permitir a la entidad tener la capacidad de detección y respuesta en email, endpoints, servidores, workloads en la nube y la red a través de una sola plataforma, es decir, poder hacer estas tareas de detección y respuesta en múltiples capas.		-
2.3.2			Debe proveer un mejor contexto y un análisis más profundo, para que la entidad pueda responder de forma más rápida y eficiente a amenazas, minimizando el impacto y alcance de un incidente en la organización		-
2.3.3			debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques.		-
2.3.4			Los modelos de correlación deben combinar multiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.		-
2.3.5			La Plataforma de XDR debe proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad		-
2.3.6			Debe proveer una vista de alertas (llamadas workbenches) con la capacidad de investigar más a fondo.		-
2.3.7			Las alertas deben permitir ver un análisis de causa raíz (también llamado Execution Profile) identificar el alcance del impacto y permitir tomar acciones de respuesta.		-
2.3.8			Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado).		-
2.3.9			Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.		-

2.3.10			debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.		-
2.3.11			Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las accionas que una amenaza llevó a cabo en un servidor, endpoint, o carga de trabajo en la nube.		-
2.3.12			Debe permitir investigar adicionalmente desde la perspectiva de red (Network Analysis) para reproducri las comunicaciones y ver el detalle de acciones de un atacante como comunicaciones de comando y control o movimientos laterales.		-
2.3.13			Debe permitir la búsqueda proactiva a traves de endpoint, red, email, y servidores (como telemetría, NetFlow, metadata, etc.) usando un simple constructor de consultas.		-
2.3.14			Debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros, y filtrar los resultados añadiendo criterios adicionales de búsqueda.		-
2.3.15			Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz.		-
2.3.16			Se debe poder construir, guardar y reutilizar búsquedas para Threat Hunting básico		-
2.3.17			Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el vendor		-

2.3.18			La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campana asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a entradas de blog relacionados si están disponibles.		-
2.3.19			Enlaces desde el workbench a la documentación del framework de MITRE ATT&CK		-
2.3.20			En una sola ubicación debe poder iniciar y ver estado de respuesta en endpoint, email, servidores y red.		-
2.3.21			Debe ofrecer opciones de respuesta “context aware” para acciones rápida desde la plataforma.		-
2.3.22			Debe permitir ejecutar acciones de respuesta rápidamente haciendo click derecho en el workbench o desde los resultados de búsqueda de Threat Intelligence		-
2.3.23			Una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR.		-
2.3.24			Debe proveer un conector para Splunk nativo		-
2.3.25			Debe ser una solución hospedada y administrada en Nube (SaaS) para tomar ventaja de tecnologías Cloud		-
2.3.26			debe analizar la data recolectada por los sensoress para proveer alertas inteligentes, y detecciones de alta fidelidad.		-

2.3.27			Los sensores deben soportar integración nativa del vendor para obtener toda la data de actividad (telemetria, metadata, netflow) no solo data de alertas.		-
2.3.28			Los sensores deben soportar trabajar al menos en los siguientes sistemas operativos de Estaciones de trabajo de usuarios: Windows 7 y superior Mac OS X El Capitan 10.11 y superior		-
2.3.29			Los sensores deben soportar trabajar al menos en las siguientes sistemas operativos de servidores Windows (Windows 2008 y superior) Linux (Including visibility over docker containers attacks) Red Hat Enterprise Linux 6 y superior Ubuntu 16 y superior CentOS 6 y superior Debian 8 y superior Amazon Linux/Amazon Linux 2 Oracle Linux 6 y superior SUSE Linux Enterprise Server 12 y superior CloudLinux 7 y superior		-
2.3.30			Los sensores deben soportar trabajar por integración directa vía API con los proveedores de correo Microsoft 365 & G Suite		-
2.3.31			Los sensores deben soportar trabajar Network por integración nativa con sistema BDS		-
2.3.32			En el caso de estaciones de trabajo de usuarios y servidores, la funcionalidad XDR debe ser una capacidad que puede tener embebida en el mismo agente de protección de endpoint. XDR no debe ser un agente adicional		-
2.3.33			Los modelos de detección deben consistir en uno o mes conjunto de filtros que integran recursos internos y externos como las técnicas y tácticas de MITRE ATT&CK		-

2.3.34			El vendor debe constantemente refinar y añadir modelos de detección y filtros para mejorar las capacidades de detección y reducir falsos positivos to improve.		-
2.3.35			Los modelos deben priorizar la respuesta del administrador en base a puntajes (score).		-
2.3.36			El aplicativo de Detection Model Management debe permitir controlar el tipo de alertas que se disparan y se envían a Workbench.		-
2.3.37			Los modelos deben tener una severidad asociada dependiendo del tipo de evento y la información de MITRE. Critical: Hay fuerte evidencia de compromiso por un ataque dirigido, APT u operaciones de cibercrimen. High: Hay indicadores altamente sospechosos de compromiso por un ataque dirigido, APT u operaciones de cibercrimen Medium: Hay indicadores sospechosos posiblemente relacionados con infección de malware, violación de políticas u operaciones de cibercrimen. Low: Hay indicadores levemente sospechosos. Usado para monitoreo y Threat Hunting		-
2.3.38			Los modelos deben especificar para que productor en específico (Workstation/Server/Email/Network) aplica una alerta		-
2.3.39			Los modelos deben especificar y permitir modificar “status”: encendido/apagado		-
2.3.40			Los modelos deben especificar la ultima vez que se actualizó		-

2.3.41			Debe hacer una sección de excepciones dentro de la App de Model Management que despliegue todas las excepciones que se añadieron.		-
2.3.42			La excepcion debe ser granular y debe mostrar lo siguiente: Object: El objeto que se ha añadido como excepción en una investigación Filter: El filtro que identificó el objeto como un indicador de amenaza Type: El atributo del objeto añadido Data field: Log definido por el objeto Match type: Exacto o Parcial (soporta wildcards) Description: Información definida por el usuario para la excepción Created: Fecha y hora en que se añadió la excepción Created by: Usuario que creó la excepción		-
2.3.43			Debe permitir añadir excepciones durante la investigación de una alerta.		-
2.3.44			En el proceso de añadir una excepción se debe poder definir una descripción para documentar la excepción		-
2.3.45			Debe integrar inteligencia al minuto con reportes del vendor y terceras partes confiables para ayudar a identificar amenazas		-
2.3.46			Debe poder analizar los logs, comparar la data contra los reportes de Threat Intelligence automáticamente, y generar alertas basadas en indicadores sospechosos o maliciosos detectados		-

2.3.47			La App de Workbench debe mostrar alertas por los modelos de detección y permitir investigar a más detalle. La data del Workbench debe incluir: Status: New/In Progress/Closed/Closed – False Positive Score: basado en la severidad del modelo de detección y el impacto de la alerta. Workbench ID: identificador único para la alerta Model: Modelo que disparó la alerta Model severity: Severidad asignada al modelo que disparó la alerta Impact scope: Número de entidades afectadas por Servers/Workstations/Users/Cuentas de correo Created: Fecha y Hora que XDR generó la alerta		-
2.3.48			Endpoint Profile: Debe incluir Hostname/IPv4/GUID/MAC Address/OS version/Producto/Último usuario que inció sesión		-
2.3.49			Email Profile: debe incluir: Asunto del correo/Message ID/Risk level/Fecha y hora del correo/Dirección de remitente/dirección de destinatarios/Información de cada adjunto al correo/URLs embebidas/Cabecera del correo		-
2.3.50			Despliega el análisis de causa raíz y provee información adicional que puede ser útil para la investigación.		-
2.3.51			Debe desplegar un análisis visual de los objetos envueltos en un evento		-
2.3.52			Debe resaltar los objetos en la cadena que son posiblemente maliciosos		-

2.3.53			Debe desplegar el objeto o la lista de objetos que coinciden con los criterios de investigación definidos		-
2.3.54			Debe resaltar el objeto “mas probable” que creó el objeto que coincidió con el criterio de investigación.		-
2.3.55			Debe desplegar detalles del endpoint que fue investigado		-
2.3.56			La cadena de análisis debe usar íconos para los distintos tipos de objetos (servidor/endpoint/url/archivos, etc…). La descripción debe estar directamente en la ventana de investigación para entender rápidamente la relación entre los distintos objetos.		-
2.3.57			Debe poder obtenerse una representación visual de correlación de eventos de la perspectiva de la red y no del endpoint.		-
2.3.58			Network Analytics debe usar como sensor al BDS (Breach Detection System) y debe proveer integración nativa para compartir no solo eventos sino el contexto entero (toda la telemetría posible).		-
2.3.59			Debe tener una barra de reproducción (play/pause) con un “time slider” para ver eventos correlacionados vs tiempo		-
2.3.60			Cada gráfica de correlación debe tener 1 o más líneas de correlación que muestran actividad maliciosa o sospechosa entre un origen y destino.		-
2.3.61			Cada línea de correlación representa 1 o más transacciones entre 2 hosts.		-

2.3.62			El grosor de la línea es proporcional al número de transacciones entre los hosts. Al colocar el mouse sobre la línea debe mostrar el número de transacciones para esa línea de correlación		-
2.3.63			La línea de correlación debe poder ser entre host interno y externo. También debe poder ser entre 2 hosts internos (para identificar movimientos laterales).		-
2.3.64			Cada línea de correlación debe indicar los protocolos usados. Y debe existir una flecha para indicar direccionalidad de la comunicación.		-
2.3.65			Debe identificar actividades claves para hosts internos y externos en la gráfica.		-
2.3.66			Debe incluir actividades similares a: Machine Learning, Lateral Activity, Detected Event, C&C Activity, and Malicious Download.		-
2.3.67			Correlation Information Pop-up Window: Debe incluir los sigueintes campos: Source IP/Destination IP/Severity/URLs/Hashes/Protocols/Number of transactions/Reason/Earliest date/Latest date		-
2.3.68			Response Management app: Debe permitir tomar acciones y llevar registro de las acciones tomadas.		-
2.3.69			Debe responder a amenazas sin dejar la consola de XDR.		-

2.3.70			Debe haber distintas acciones que se puedan tomar en los objetos maliciosos/sospechosos. Añadir a lista de bloqueo Eliminar de lista de bloqueo Terminar procesos en endpoints Recolectar archivos en endpoints Bloquear remitente de correo Poner en cuarentana un correo Borrar un correo Aislar un equipo Restaurar la conexión en equipos aislados		-
2.3.71			Después de activar la respuesta a un evento u objeto, debe poderse ver el estado de la tarea de respuesta y los detalles de comando en una tabla de Gestión de Respuesta		-
2.3.72			Debe permitir realizar barridos IoC, personalizar búsquedas por especificación de parámetros, filtros y otros criterios y búsqueda de múltiples eventos que ocurraen en un mismo Endpoint		-
2.3.73			Debe tener un constructor de peticiones que debe permitir combinar atributos de búsqueda, operadores y especificar valores en una misma petición de búsqueda		-
2.3.74			Debe listar busquedas previas		-
2.3.75			Debe permitir guardar búsquedas para encontrar nueva data relacionada a los mismos criterios.		-
2.3.76			El administrador debe poder ver los queries guardados		-
2.3.77			Debe ser fácil limpiar los criterios de búsqueda		-

2.3.78			Los resultados deben ser exportables a CSV o JSON		-
2.3.79			Los resultados deben mostrar origen de los datos (workstation/servidor/email/network)		-
2.3.80			El administrador debe ser capaz de ver los logs en RAW		-
2.3.81			debe permitir diferentes tipos de búsquedas, filtros, y un lenguaje de consultas basado en Kibana para identificar, categorizar y obtener los resultados de búsqueda.		-
2.3.82			La configuración administrativa de XDR debe brindar a los usuarios la capacidad de configurar cuentas de usuario, roles y configuraciones, conectar productos adicionales y configurar opciones de monitoreo adicionales. Las siguientes opciones deben estar disponibles: SAML Single Sign-On Account Management Role Management Product Connector Alert Notifications Audit Logs Remote Support		-
2.4.1		GARANTIA	El proveedor de la solución debe suministrar soporte directo de fabricante con una disponibilidad 7x24 para atención de incidentes y contar con actualizaciones de software por la vigencia del contrato		-
2.4.2			Soporte directo de fabricante para la atención de incidentes de forma remota por medio de correo electrónico y telefónico.		-

2.4.3			El fabricante deberá contar con un servicio de laboratorio de investigación en español para proporcionar de forma rápida actualizaciones de bases de firmas de virus sobre amenazas enfocadas en regiones hispanohablantes		-

El proponente deberá presentar las fichas técnicas, url o certificados provistos por el fabricante de la marca representada donde se evidencie el cumplimiento de las características técnicas de carácter obligatorio y de las mejoras a las cuales aplique. Estos documentos técnicos podrán presentarse en idioma inglés.

m) Con la firma del presente documento se expresa el cumplimiento del siguiente requisito:

Requisito	Cumple SI/NO	Observación
Certificación de Fabricante. El oferente deberá presentar un documento emitido directamente por el fabricante de la solución ofertada, donde certifique estar registrado en su programa de canales/partners y donde certifique mínimo 5 años de estar dentro de los tres más altos niveles de canal/partner, y que cuenta con capacidad para: comercializar e implementar las soluciones de dicho fabricante en el territorio colombiano. No se aceptarán certificaciones emitidas por mayoristas, distribuidores u otro tercero diferente al fabricante. Dichas certificaciones deberán contar con fecha de expedición no mayor a 60 días anteriores a la fecha de presentación de la oferta.		

n) Con la firma del presente documento se expresa el cumplimiento de Personal Mínimo Requerido según la siguiente información

Cargo	Nombre del Profesional	Tarjeta Profesional	Folio
Gerente de Proyectos	Profesional en: Ingeniería Electrónica, Eléctrico, Sistemas o Telematico. -Fotocopia de Cedula de ciudadanía -Certificado de vigencia de la tarjeta profesional.	GENERAL: Experiencia general mínima de cinco (5) años contados a partir de la culmnacion de materias. ESPECIFICA: Experiencia específica mínima de cinco (5) años ejerciendo cargos relacionados con funciones de gerencia o dirección en el sector de las TIC.	
Tecnólogo/ Ingeniero Líder diseñador de políticas de seguridad informática	Profesional en: Tecnólogo/Ingeniero Industrial, Electrónico, Sistemas, Telemático o administración de redes. - Fotocopia de Cedula de ciudadanía -Especialización en Seguridad Informática o en su defecto contar con todas las siguientes certificaciones: CISSP y CISM y CEH-Ethical Hacking, e ISO27001:2013, vigentes a la fecha de la presentación de la oferta. - Certificado de fábrica en nivel fundamentos y/o profesional en plataformas de protección de Endpoint, protección de servidores y XDR, con una fecha de expedición no mayor a 2 años, de la misma marca ofertada para el presente proceso.	GENERAL Experiencia general mínima de cinco (5) años trabajando en empresas del sector TIC, contados a partir de la culminación de materias. ESPECIFICA: Experiencia específica mínima de ocho (8) meses ejerciendo funciones como configurador, operador y/o administrador de tecnologías de infraestructura o software.	

Tecnólogo/ Ingeniero de Seguridad de Endpoint y Protección de Información	Profesional en: Tecnólogo/Ingeniero Electrónico, Sistemas, Telemático o administración de redes. -Fotocopia de Cedula de ciudadanía -Certificado de vigencia de la tarjeta profesional Especialización en dirección o gerencia de proyectos. - Certificado de fábrica en nivel fundamentos, esencial o profesional en plataformas de protección de Endpoint, protección de servidores o XDR, con una fecha de expedición no mayor a 2 años de la misma marca ofertada para el presente proceso.	GENERAL -Experiencia general mínima de tres (3) años trabajando en empresas del sector TIC contados a partir de la fecha de expedición de la culminación de materias ESPECIFICA: -Experiencia específica mínima de dos (2) años como implementador, analista o administrador de soluciones de seguridad de endpoint y DLP.	

Nota: Adjuntar comprobantes de pago de aportes a seguridad social de los últimos 3 meses, con el fin de comprobar que el profesional es empleado directo de la empresa oferente, o de una de las empresas que compongan un proponente plural.

m)

FIRMA AUTORIZADA
C.C.NIT

FORMATO No. 2
CONFORMACIÓN DE PROPONENTE PLURAL
(2 A – CONSORCIO)

Nombre del Consorcio: ___

Los suscritos,

Nombre	CC	Actuando en representación de:	
		Nombre o Razón Social	CC o NIT

Debidamente autorizados según consta en las actas que adjuntamos (si de acuerdo con los estatutos de cada miembro se requiere), atentamente les manifestamos que de conformidad con el Artículo 7, Numeral 1o. de la Ley 80 de 1993, conjuntamente formulamos propuesta y suscribiremos el eventual contrato dentro del desarrollo del proceso de Selección Abreviada de Menor Cuantía CVC No. 38 de 2021, cuyo objeto es XXXXX", de acuerdo con las condiciones y especificaciones administrativas, financieras y técnicas contenidas en el Pliego de Condiciones.

En caso que nos sea adjudicado el contrato, responderemos SOLIDARIAMENTE por la celebración y ejecución del Contrato; y declaramos que las actuaciones, hechos y omisiones que se presenten en desarrollo de la propuesta y del contrato, afectarán a todos los miembros que conforman el presente Consorcio.

Manifestamos que designamos como representante del Consorcio para todos los efectos legales a_____, identificado con la cédula de ciudadanía No.____expedida en la ciudad de.___. A pesar de lo anterior, aceptamos que el contrato sea formulado de tal manera que comprometa a todos los miembros del Consorcio.

Declaramos que la duración del Consorcio será de_____días calendario. (Mínimo el plazo de ejecución propuesto más un (1) año).

Atentamente,

_____
El representante legal y su suplente en el Consorcio, firmarán el presente documento, con C.C. o NIT

FORMATO No. 2
CONFORMACIÓN DE PROPONENTE PLURAL
(2 B - UNIÓN TEMPORAL)

Nombre de la Unión Temporal:

Los suscritos (NOMBRES DE LAS PERSONAS NATURALES O DE LOS REPRESENTANTES DE LAS PERSONAS JURÍDICAS DE LA UNIÓN TEMPORAL), obrando en nombre propio personas naturales) o en nombre y representación de _____(personas jurídicas), debidamente autorizadas según consta en las actas que adjuntamos (si de acuerdo con los estatutos se requiere), atentamente les manifestamos que de conformidad con el artículo 7, numeral 2 de la Ley 80 de 1993, conjuntamente formulamos PROPUESTA, en la modalidad de UNIÓN TEMPORAL para la Selección Abreviada de Menor Cuantía CVC No. 38 de 2021, cuyo objeto es "XXXXXX"

En caso que nos sea adjudicado el Contrato, respondemos solidariamente por el cumplimiento de la propuesta y la celebración y ejecución del contrato. Igualmente,

INTEGRANTE	PORCENTAJE (%) (PROPUESTA)	PORCENTAJE (%) (EJECUCIÓN)

manifestamos que designamos como representante de la Unión Temporal para todos los efectos legales a___, identificado con la cédula de ciudadanía No.____de__. El porcentaje (%) de participación de cada uno de los miembros en el caso de la presente Unión Temporal es:

Cada uno de los participantes, es decir___y_____, aportan los términos y extensión de la participación en la propuesta y en su ejecución (Los cuales no podrán ser modificados sin el consentimiento de La Corporación Autónoma Regional del Valle del Cauca - CVC, como se describe a continuación:

INTEGRANTE_____: INTEGRANTE_____:
Declaramos que la duración de la Unión Temporal será de____días calendario. (Mínimo el plazo de ejecución propuesto más un (1) año).

Atentamente,

_____

El representante legal y su suplente en la Unión Temporal, firmarán el presente documento, con C.C. o NIT

Corporación Autónoma Regional del Valle del Cauca

FORMATO No. 3
EXPERIENCIA DEL PROPONENTE

1	**No. Contrato**		**Fecha inicio**		**Fecha finalización**	
	Contratante		**Teléfono**		**CÓDIGO UNSPSC**	
	Interventor		**Teléfono**			
	Objeto del Contrato					
	CALIDAD DE PARTICIPACIÓN EN EL CONTRATO REPORTADO (Anotar el correspondiente porcentaje)					
	Contratista Directo		**Consorcio**		**Unión Temporal**	
	Fecha Acta de Liquidación Final del Contrato					
	Valor ejecutado ($)					
	Valor ejecutado (SMMLV)					

(1) Se debe diligenciar este formato por cada contrato o experiencia que se quiera reportar. Para los contratos que se encuentren reportados en el RUP como Experiencia Acreditada o a través de certificaciones.

_____

Nombre y firma del representante legal del proponente y CC o NIT.

1) La CVC se reserva el derecho de confrontar esta información.
2) Cualquier inconsistencia en la información suministrada, será motivo de rechazo de la propuesta.
3) Toda esta información se verificará con cada una de las certificaciones aportadas y cumpliendo

Corporación Autónoma
Regional del Valle del Cauca

FORMATO No. 4
CAPACIDAD FINANCIERA Y ORGANIZACIONAL

Ver indicadores de capacidad financiera y organizacional

Corporación Autónoma Regional del Valle del Cauca

FORMATO No. 5
CAPACIDAD RESIDUAL (Cuando se trate de Obra)

No aplica

Corporación Autónoma
Regional del Valle del Cauca

FORMATO No. 6
PAGO DE SEGURIDAD SOCIAL Y APORTES LEGALES
(6 A Persona Natural)

Debe cumplir con lo enunciado en el punto 5.2 del Capitulo III del presente Pliego de Condiciones

FORMATO No. 6
PAGO DE SEGURIDAD SOCIAL Y APORTES LEGALES
(6 B Persona Jurídica)

Ciudad y Fecha

Señores
Corporación Autónoma Regional del Valle del Cauca-CVC
Ciudad

Nombre o razón social del proponente:

CERTIFICACIÓN

Certifico bajo gravedad de juramento que_____con C.C. No. ___o NIT No.____, ha cumplido con el pago de los aportes de sus empleados a los sistemas de salud, riesgos profesionales, pensiones y aportes a Las cajas de compensación familiar, al Instituto Colombiano de Bienestar Familiar y al SENA, Sistema de Seguridad Integral y de Parafiscales, en los últimos seis (6) meses anteriores a la fecha de cierre de la Selección Abreviada de Menor Cuantía No. 38 de 2021.

Expedida a los días del mes de ____

Nombre:

Firma:

(Del proponente, o del representante legal, o del revisor fiscal (cuando el proponente esté obligado a tener revisor fiscal)

Firma del Proponente: _____
C.C. o NIT

FORMATO No. 7
CALIDAD
(7 A Gerencia de Proyectos y Plan de Calidad)
(7 B Maquinaria)
(7C Plan de Calidad)

Factor Calidad: Se asignará un puntaje máximo de 60 PUNTOS al proponente al proponente que oferte:

- Una (1) Capacitación virtual para la mesa de servicio integral de la corporación de ocho (8) horas, orientada a la implementación y soporte técnico de los clientes antivirus.

Lo cual se acreditará mediante una carta firmada por el representante legal del oferente, donde se compromete a dictar la capacitación.

FORMATO No. 8
PUNTAJE DE INDUSTRIA NACIONAL

[Fecha]

Señores
Corporación Autónoma Regional del Valle del Cauca-CVC
Carrera 57 # 11-29, Piso 1 CAC
Cali

Ref.: Selección Abreviada de Menor Cuantía No. 38 de 2021

Objeto:

Por medio de este documento _____ (nombre o razón social del proponente) en adelante el "PROPONENTE", manifiesto que en virtud de lo dispuesto en el artículo 2 de la Ley 816 de 2003, el componente colombiano (de bienes o servicios profesionales, técnicos y operativos que será destinado para la ejecución del contrato, en caso de que se me adjudique, según el caso), será de origen %XX colombiano.

Nombre del Proponente _____
Nombre del Representante Legal _____
Identificación del extranjero_____

_____
Firma Representante Legal Proponente

FORMATO No. 9
FACTORES DE DESEMPATE

PARTICIPACIÓN MAYORITARIA DE MUJERES CABEZA DE FAMILIA Y/O MUJERES VÍCTIMA DE VIOLENCIA INTRAFAMILIAR (PERSONA JURÍDICA)

[Este formato se diligencia por el representante legal o el revisor fiscal, según corresponda, de la persona jurídica en el que mayoritariamente participen mujeres cabeza de familia y mujeres víctima de violencia intrafamiliar. En el evento que la oferta la presente una entidad privada sin ánimo de lucro, ya sea, fundación, corporación o asociación se ajustará el formato en lo pertinente. La información vertida en este formato contiene datos sensibles la cual está sujeta a reserva legal y, por tanto, no se podrá publicar en el SECOP I y II para su conocimiento]

Señores
[NOMBRE DE LA ENTIDAD]
[Ciudad]

REFERENCIA: Proceso de Contratación [Incluir número del Proceso de Contratación]

Objeto:
[Incluir cuando el Proceso de Contratación sea estructurado por lotes o grupos] Lote: [Indicar el lote o lotes a los cuales se presenta oferta.]

Estimados señores:

[Incluir el nombre del representante legal de la persona jurídica o del revisor fiscal, según corresponda] identificado con [Incluir el número de identificación], en mi condición de [Indicar si actúa como representante legal o revisor fiscal] de [Incluir la razón social de la persona jurídica] identificada con el NIT [Incluir el NIT], certifico bajo la gravedad de juramento que más del cincuenta por ciento (50 %) de la composición accionaria o cuota parte de la persona jurídica está constituida por mujeres cabeza de familia y/o mujeres víctima de violencia intrafamiliar. Esta información está soportada de acuerdo con los libros de comercio de la sociedad, los cuales gozan de reserva legal en los términos del artículo 61 del Código de Comercio.

En el siguiente cuadro señalo las mujeres cabeza de familia o mujeres víctima de violencia intrafamiliar que participan mayoritariamente en la persona jurídica, junto con su respectivo porcentaje de participación:

Identificación de las mujeres cabeza de familia o mujeres víctima de violencia intrafamiliar que participan en la persona jurídica (Incluir nombre y documento de identidad)	**Número de cuotas sociales, acciones que poseen o el alcance o condición de su participación en el caso de las personas jurídicas sin ánimo de lucro**

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

_____

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

FORMATO 9B – VINCULACIÓN DE PERSONAS EN CONDICIÓN DE DISCAPACIDAD

[Tratándose de proponentes plurales, este formato lo presentará el integrante o los integrantes que tengan una participación de por lo menos el veinticinco por ciento (25 %) en el consorcio o en la unión temporal y aporten mínimo el veinticinco por ciento (25 %) de la experiencia general habilitante]

Señores
[NOMBRE DE LA ENTIDAD]
[Ciudad]

REFERENCIA: Proceso de Contratación [Incluir número del Proceso de Contratación]

Objeto:
[Incluir cuando el Proceso de Contratación sea estructurado por lotes o grupos] Lote: [Indicar el lote o lotes a los cuales se presenta oferta.]

Estimados señores:

[Incluir el nombre de la persona natural, el representante legal de la persona jurídica o el revisor fiscal, según corresponda] identificado con [Incluir el número de identificación], en mi condición de [Indicar si actúa como representante legal o revisor fiscal] de [Incluir la razón social de la persona jurídica] [identificada con el NIT _____], certifico que tengo vinculado en la planta de personal un mínimo del diez por ciento (10 %) de empleados en las condiciones de discapacidad enunciadas en la Ley 361 de 1997, contratados [con una anterioridad no inferior a un año o desde la constitución de la sociedad (para sociedades con menos de un año de constitución)], para lo cual adjunto el certificado expedido por el Ministerio del Trabajo.

De igual manera me comprometo en caso de resultar adjudicatario del presente proceso de contratación, a mantener vinculados a los empleados en condiciones de discapacidad por un lapso igual al del plazo de ejecución del contrato.

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

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

FORMATO 9C – VINCULACIÓN DE PERSONAS MAYORES Y NO BENEFICIARIAS DE LA PENSIÓN DE VEJEZ, FAMILIAR O SOBREVIVENCIA
(EMPLEADOR – PROPONENTE)

[Este formato lo diligencia la persona natural, el representante legal o el revisor fiscal de la persona jurídica que tiene en su personal trabajadores mayores de edad vinculados en la planta del personal que no sean beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido la edad de pensión. En el caso de los proponentes plurales, este formato lo diligenciará el representante del proponente plural en el cual certifica la totalidad de los trabajadores vinculados en la planta de personal de cada uno de los integrantes y la totalidad de personas mayores de edad vinculados de cada uno de sus integrantes]

Señores
[NOMBRE DE LA ENTIDAD]
[Ciudad]

REFERENCIA: Proceso de Contratación [Incluir número del Proceso de Contratación]

Objeto:
[Incluir cuando el Proceso de Contratación sea estructurado por lotes o grupos] Lote: [Indicar el lote o lotes a los cuales se presenta oferta.]

Estimados señores:

[Incluir el nombre de la persona natural, el representante legal de la persona jurídica o el revisor fiscal, según corresponda, o el representante del proponente plural] identificado con [Incluir el número de identificación], en mi condición de [Indicar si actúa como representante legal o revisor fiscal o representante del proponente plural] de [Incluir la razón social de la persona jurídica] [identificada con el NIT _____], certifico que el número total de trabajadores personas mayores de edad vinculados en la planta del personal que no son beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de edad de pensión establecido en la ley es el que se relaciona a continuación:

Número total de trabajadores vinculados a la planta de personal	Número de personas mayores no beneficiarias a la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de pensión

[Incluir el siguiente cuadro para los proponentes plurales]

Número total de trabajadores vinculados a la planta de personal de los integrantes del proponente plural	Número de personas mayores, no beneficiarias a la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de pensión de los integrantes del proponente plural

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

_____

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

FORMATO 9D – VINCULACIÓN DE POBLACIÓN INDÍGENA, NEGRA, AFROCOLOMBIANA, RAIZAL, PALENQUERA, RROM O GITANA

[La información de este formato contiene datos sensibles la cual está sujeta a reserva legal y por tanto no se podrá publicar en el SECOP I y II para su conocimiento]

Señores
[NOMBRE DE LA ENTIDAD]
[Ciudad]

REFERENCIA: Proceso de Contratación [Incluir número del Proceso de Contratación]

Objeto:
[Incluir cuando el Proceso de Contratación sea estructurado por lotes o grupos] Lote: [Indicar el lote o lotes a los cuales se presenta oferta.]

Estimados señores:

[Incluir el nombre del proponente persona natural o del representante legal de la persona jurídica o el revisor fiscal, según corresponda, o el representante del proponente plural] identificado con [Incluir el número de identificación], en mi condición de [Indicar si actúa como representante legal o revisor fiscal] de [Incluir la razón social de la persona jurídica], [identificada con el NIT _____], certifico bajo la gravedad de juramento que:

i) El número total de trabajadores vinculados a la nómina corresponden a [Diligenciar el número de trabajadores vinculados a la nómina]

ii) En la nómina están vinculadas las siguientes personas: [Indicar a continuación el nombre y número de cédula de las personas que se encuentran vinculadas al proponente o integrante de la estructura plural según corresponda y respecto de las cuales se aportan las pruebas correspondientes, para acreditar la pertenencia a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitanas]

Nombre completo	Número de identificación

iii) Así mismo declaramos que las personas señaladas anteriormente se encuentran vinculadas con una antigüedad igual o mayor a un año contado a partir de la fecha del cierre del presente proceso de selección. [Para los casos de constitución inferior a un año se tendrá que indicar que las personas señaladas se encuentran vinculadas desde el momento de constitución de la misma].

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

_____

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

FORMATO 9E – PARTICIPACIÓN MAYORITARIA DE PERSONAS EN PROCESO DE REINCORPORACIÓN EN PROCESO DE REINCORPORACIÓN Y/O REINTEGRACIÓN (PERSONAS JURÍDICAS)

Este formato se diligencia por el representante legal o el revisor fiscal, si están obligados a tenerlo, de la persona jurídica en el que mayoritariamente participan personas en proceso de reintegración o reincorporación de la persona jurídica. En el evento que la oferta la presente una entidad privada sin ánimo de lucro, ya sea, fundación, corporación o asociación se ajustará el formato en lo pertinente. La información de este formato contiene datos sensibles la cual está sujeta a reserva legal y, por tanto, no se podrá publicar en el SECOP I y II para su conocimiento]

Señores
[NOMBRE DE LA ENTIDAD]
[Ciudad]

REFERENCIA: Proceso de Contratación [Incluir número del Proceso de Contratación]

Objeto:
[Incluir cuando el Proceso de Contratación sea estructurado por lotes o grupos] Lote: [Indicar el lote o lotes a los cuales se presenta oferta.]

Estimados señores:

[Incluir el nombre del representante legal de la persona jurídica y el revisor fiscal, si están obligados a tenerlo] identificado con [Incluir el número de identificación], en mi condición de [Indicar si actúa como representante legal o revisor fiscal o ambos] de [Incluir la razón social de la persona jurídica], [identificada con el NIT _____], certifico bajo gravedad de juramento que más del cincuenta por ciento (50 %) de la composición accionaria o cuota parte de la persona jurídica está constituida por personas en proceso reincorporación y/o reintegración. Esta información está soportada de acuerdo con los respectivos certificados de la Oficina del Alto Comisionado para la Paz, o del Comité Operativo para la Dejación de Armas y el documento de identificación de cada una de dichas personas.

En el siguiente cuadro señalo las personas en proceso de reincorporación o reintegración que participan mayoritariamente en la persona jurídica, junto con su respectivo porcentaje de participación:

Identificación de las personas en proceso de reincorporación o reintegración (Incluir nombre y documento de identidad)	Número de cuotas sociales, acciones que poseen o el alcance o condición de su participación en el caso de las personas jurídicas sin ánimo de lucro

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

_____
[Nombre y firma del representante legal de la persona jurídica o revisor fiscal]

FORMATO 9 E – PARTICIPACIÓN MAYORITARIA DE PERSONAS EN PROCESO DE REINCORPORACIÓN EN PROCESO DE REINCORPORACIÓN (PERSONA JURÍDICA INTEGRANTE DEL PROPONENTE PLURAL)

[Este formato se diligencia por el representante legal o el revisor fiscal, si están obligados a tenerlo, de la persona jurídica del proponente plural en el que mayoritariamente participan personas en proceso de reincorporación de la persona jurídica. En el evento que la oferta la presente una entidad privada sin ánimo de lucro, ya sea, fundación, corporación o asociación se ajustará el formato en lo pertinente. La información de este formato contiene datos sensibles la cual está sujeta a reserva legal y, por tanto, no se podrá publicar en el SECOP I y II para su conocimiento]

Señores
[NOMBRE DE LA ENTIDAD]
[Ciudad]

REFERENCIA: Proceso de Contratación [Incluir número del Proceso de Contratación]

Objeto:
[Incluir cuando el Proceso de Contratación sea estructurado por lotes o grupos] Lote: [Indicar el lote o lotes a los cuales se presenta oferta.]

Estimados señores:

[Incluir el nombre del representante legal de la persona jurídica o el revisor fiscal, si están obligados a tenerlo] identificado con [Incluir el número de identificación], en mi condición de [Indicar si actúa como representante legal o revisor fiscal o ambos] de [Incluir la razón social de la persona jurídica], [identificada con el NIT _____], certifico bajo gravedad de juramento que más del cincuenta por ciento (50 %) de la composición accionaria o cuota parte de la persona jurídica está constituida por personas en proceso de reincorporación. Esta información está soportada de acuerdo con los respectivos certificados de la Oficina del Alto Comisionado para la Paz, o del Comité Operativo para la Dejación de Armas y el documento de identificación de cada una de dichas personas.

En el siguiente cuadro señalo las personas en proceso de reincorporación que participan mayoritariamente en la persona jurídica, junto con su respectivo porcentaje de participación:

Identificación de las personas en proceso de reincorporación (Incluir nombre y documento de identidad)	Número de cuotas sociales, acciones que poseen o el alcance o condición de su participación en el caso de las personas jurídicas sin ánimo de lucro

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

_____
[Nombre y firma del representante legal de la persona jurídica o revisor fiscal]

FORMATO 9F – PARTICIPACIÓN MAYORITARIA DE MUJERES CABEZA DE FAMILIA Y/O PERSONAS EN PROCESO DE REINCORPORACIÓN Y/O REINTEGRACIÓN (PERSONAS JURÍDICAS)

[Este formato se diligencia por el representante legal o el revisor fiscal, según corresponda, del integrante del proponente plural (persona jurídica) en el que mayoritariamente participen madres cabeza de familia y/o personas en proceso de reintegración o reincorporación. Este formato lo podrá presentar el integrante o los integrantes que, cumpliendo la condición anterior, tengan una participación de por lo menos el veinticinco por ciento (25 %) en el consorcio o en la unión temporal y aporten mínimo el veinticinco por ciento (25 %) de la experiencia general acreditada en la oferta.

En el evento que la oferta la presente una entidad privada sin ánimo de lucro, ya sea, fundación, corporación o asociación se ajustará el formato en lo pertinente. La información de este formato contiene datos sensibles la cual está sujeta a reserva legal y, por tanto, no se podrá publicar en el SECOP I y II para su conocimiento]

Señores
[NOMBRE DE LA ENTIDAD]
[Ciudad]

REFERENCIA: Proceso de Contratación [Incluir número del Proceso de Contratación]

Objeto:
[Incluir cuando el Proceso de Contratación sea estructurado por lotes o grupos] Lote: [Indicar el lote o lotes a los cuales se presenta oferta.]

Estimados señores:

[Incluir el nombre del representante legal de la persona jurídica o del revisor fiscal, según corresponda] identificado con [Incluir el número de identificación], en mi condición de [Indicar si actúa como representante legal o revisor fiscal] de [Incluir la razón social de la persona jurídica], [identificada con el NIT _____], certifico bajo la gravedad de juramento que más del cincuenta por ciento (50 %) de la composición accionaria o cuota parte de la persona jurídica del proponente plural está constituida por madres cabeza de familia y/o personas en proceso de reintegración o reincorporación.

En el siguiente cuadro señalo las madres cabeza de familia y/o personas en proceso de reincorporación o reintegración que participan mayoritariamente en la persona jurídica, junto con su respectivo porcentaje de participación:

Identificación de las madres cabeza de familia o personas en proceso de reincorporación o reintegración (Incluir nombre y documento de identidad)	**Número de cuotas sociales, acciones que poseen o el alcance o condición de su participación en el caso de las personas jurídicas sin ánimo de lucro**

[Para la acreditación de desempate establecida en el literal (c), numeral 7, del numeral 4.6 del documento tipo incluir la siguiente redacción:]

Adicionalmente, los abajo firmantes, certificamos que ni la madre cabeza de familia o la persona en proceso de reincorporación o reintegración, ni la persona jurídica, ni sus accionistas, socios o representantes legales son empleados, socios o accionistas de los miembros del proponente plural.

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

_____

[Nombre y firma del representante legal de la persona jurídica o revisor fiscal]

FORMATO 9 G – ACREDITACIÓN MIPYME

Señores
[NOMBRE DE LA ENTIDAD]
[Ciudad]

REFERENCIA: Proceso de Contratación [Incluir número del Proceso de Contratación]

Objeto:
[Incluir cuando el Proceso de Contratación sea estructurado por lotes o grupos] Lote: [Indicar el lote o lotes a los cuales se presenta oferta.]

Estimados señores:

[Incluir el nombre o integrante persona natural y contador público o del representante legal de la persona jurídica y el revisor fiscal para las personas obligadas por ley o del representante legal y contador público, según corresponda,] identificados con [Incluir el número de identificación], actuando en representación de [Indicar nombre del proponente, o integrante de proponente plural] declaramos bajo la gravedad de juramento que la sociedad se encuentra clasificada como: [Indicar si es micro, pequeña y mediana empresa] de acuerdo con los criterios definidos por las normas legales vigentes.

[Para la acreditación de desempate establecida en el literal (c), literal 10, del numeral 4.6 del documento tipo incluir la siguiente redacción:]

Adicionalmente, los abajo firmantes certificamos que ni la Mipyme, cooperativa o asociación mutual ni sus accionistas, socios o representantes legales son empleados, socios o accionistas de los miembros del proponente plural.

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

[En el evento que sea un proponente persona natural quien presente la oferta, incluir las firmas de la siguiente manera:]

_____

[Nombre y firma del proponente o integrante persona natural y contador público]

[En el evento que sea un proponente persona jurídica quien presente la oferta, incluir las firmas de la siguiente manera:]

_____

[Nombre y firma del representante legal y revisor fiscal para las empresas obligadas por ley o del representante legal y contador público, según corresponda]

FORMATO 9 H – PAGOS REALIZADOS A MIPYMES, COOPERATIVAS O ASOCIACIONES MUTUALES

Señores
[NOMBRE DE LA ENTIDAD]
[Ciudad]

REFERENCIA: Proceso de Contratación [Incluir número del Proceso de Contratación]

Objeto:
[Incluir cuando el Proceso de Contratación sea estructurado por lotes o grupos] Lote: [Indicar el lote o lotes a los cuales se presenta oferta.]

Estimados señores:

[Incluir el nombre del proponente persona natural y contador público, o el representante legal y revisor fiscal para las empresas obligadas por ley, o del representante legal y contador público, según corresponda] identificados con [Incluir el número de identificación], en nuestra condición de [Indicar si actúa como representante legal o revisor fiscal] de [Incluir la razón social de la persona jurídica], [identificada con el NIT _____], declaramos bajo la gravedad de juramento, que de acuerdo con nuestros estados financieros o información contable con corte al 31 de diciembre del año anterior, por lo menos el veinticinco por ciento (25 %) del total de pagos fueron realizados a Mipymes, cooperativas o asociaciones mutuales por concepto de proveeduría del oferente, realizados durante el año anterior.

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

[En el evento que sea un proponente persona natural quien presente la oferta, incluir las firmas de la siguiente manera:]

_____

[Nombre y firma del proponente o integrante persona natural y contador público]

[En el evento que sea un proponente persona jurídica quien presente la oferta, incluir las firmas de la siguiente manera:]

_____

[Nombre y firma del representante legal y revisor fiscal para las empresas obligadas por ley o del representante legal y contador público, según corresponda]

FORMATO No. 10
AUTORIZACION PARA EL TRATAMIENTO DE DATOS PERSONALES

El presente Formato lo diligenciará toda persona (proponente, socia o trabajador) que al momento de presentar su oferta contenga datos sensibles, para que la Entidad Estatal contratante garantice el tratamiento adecuado a estos datos]

Señores
[NOMBRE DE LA ENTIDAD]
[Dirección de la Entidad]
[Ciudad]

Cumpliendo la Ley 1581 de 2012 "Por el cual se dictan disposiciones para la protección de datos personales" y conforme al Decreto 1377 de 2013, con la firma de este documento manifiesto que he sido informado por [Incluir el nombre de la Entidad] de lo siguiente:

1) La [Incluir el nombre de la Entidad Estatal] actuará como responsable del tratamiento de datos personales de los cuales soy titular y que, conjunta o separadamente podrá recolectar, almacenar y usar mis datos personales para hacer efectivo el factor de desempate previsto en el numeral 4.6, numerales 2, 5, 6 y 7 del pliego de condiciones, relacionados con la acreditación de ser víctima de violencia intrafamiliar, persona en proceso de reintegración o reincorporación, o persona perteneciente a la población indígena, negra, afrocolombiana raizal, palenquera, Rrom, o gitanas.

Finalidad	**Autoriza**	
	SÍ	**NO**
Hacer efectivo el factor de desempate para la acreditación de una mujer víctima de violencia intrafamiliar, persona perteneciente a la población indígena, negra, afrocolombiana raizal, palenquera, Rrom, o gitanas, o persona en proceso de reintegración o reincorporación.		

2) Entiendo que son datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos con la salud, la vida sexual y los datos biométricos.

3) Manifiesto que me informaron que los datos sensibles que se recolectarán serán utilizados para hacer efectivo el criterio de desempate previsto en el numeral 4.6, numerales 2, 5, 6 y 7 del pliego de condiciones, relacionados con la acreditación de ser víctima de violencia intrafamiliar, integrante de la población indígena, negra, afrocolombiana raizal, palenquera, Rrom, o gitanas, o persona en proceso de reintegración o reincorporación.

Derechos del titular

Sus derechos como titular de los datos son los previstos en la Constitución y en la Ley 1581 de 2012, especialmente los siguientes:

a) Acceder en forma gratuita a los datos proporcionados que hayan sido objeto de tratamiento.

b) Solicitar la actualización y rectificación de su información frente a los datos parciales, inexactos, incompletos.

c) Solicitar prueba de la autorización otorgada.

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la normatividad vigente.

e) Revocar la autorización y/o solicitar la supresión del dato, a menos que exista un deber legal o contractual que haga imperativo conservar la información.

f) Abstenerse de responder las preguntas sobre datos sensibles o sobre datos de las niñas y niños y adolescentes.

Estos derechos los podré ejercer mediante los canales o medios dispuestos por [Incluir nombre de la Entidad] para la atención al público, la línea de atención nacional [incluir número de atención de la Entidad], el correo electrónico [incluir el correo electrónico] y las oficinas de atención al cliente a nivel nacional, cuya información puedo consultar en [incluir página web de la Entidad], disponibles de [lunes a viernes de 8:00 am a 6:00 p.m].

Por todo lo anterior, he otorgado mi consentimiento a [Incluir nombre de la Entidad] para que trate mi información personal de acuerdo con la Política de Tratamiento de Datos Personales dispuesta en [Incluir el link en donde se encuentra la Política de Tratamiento de Datos Personales] y que me dio a conocer antes de recolectar mis datos personales.

Manifiesto que la presente autorización me fue solicitada y puesta de presente antes de entregar mis datos y que la suscribo de forma libre y voluntaria una vez leída en su totalidad.

Nombre: [Incluir nombre del titular de la autorización datos sensibles para la autorización de datos]

Firma: [Incluir firma del titular]

Identificación: [Incluir número de identificación del titular de datos sensibles]

Fecha: [Fecha en que se puso de presente la autorización y entregó

Corporación Autónoma
Regional del Valle del Cauca

FORMULARIO No. 1

A. FORMULARIO DE PRESUPUESTO OFICIAL

Incluir aquí presupuesto oficial

FORMULARIO No. 1

B. PROPUESTA ECONOMICA DEL PROPONENTE

Ciudad y Fecha

Señores:
CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA - CVC
Oficina Tecnologías de la Información
Santiago de Cali

ITEM	DESCRIPCION	UNID.	CANT.	VALOR UNITARIO	VALOR TOTAL
1	Licenciamiento software en nube Antivirus con XDR (Antimalware, Reputación Web, Firewall, Machine Learning, IDS/IPS, Control de aplicaciones, Data Loss Prevention DLP, Control de dispositivos) a 1 año.	UND	836		
2	Licenciamiento software en nube integración con Plataforma XDR para equipos con licenciamiento antivirus existente con una vigencia de 1 año.	UND	166		
			VALOR TOTAL LICENCIAMIENTO SIN IVA		
			IMPUESTO AL VALOR AGREGADO (IVA) 0%		
			VALOR TOTAL DE LA PROPUESTA LICENCIAMIENTO		
3	Servicio de implementación consola antivirus	GLOBAL	1		
			VALOR TOTAL SERVICIOS SIN IVA		
			IMPUESTO AL VALOR AGREGADO (IVA) 19%		
			VALOR TOTAL DE LA PROPUESTA SERVICIOS		
			VALOR TOTAL OFERTA		

CONCEPTO	VALOR
Valor de la Propuesta sin IVA	
Impuesto al Valor Agregado (IVA)	
VALOR TOTAL DE LA PROPUESTA	
Valor Total de la Propuesta en Letras	

El valor de la propuesta (antes de IVA), incluyendo todos los servicios, es de ---------- (VALOR EN LETRAS) PESOS M/CTE. ($-----).

Atentamente,

Firma del Representante Legal
Nombre
Nit / C.C.
Empresa

NOTA IMPORTANTE: LA PROPUESTA DEBE PRESENTARSE EN PESOS COLOMBIANOS

- **La propuesta económica deberá presentarse teniendo en cuenta el presupuesto que la Corporación ha definido para el total a adquirir de licencias antivirus el cual se encuentra contemplado en concepto de gasto "paquetes de software" por valor de $134.580.490 incluido IVA y el presupuesto establecido para los servicios objeto del contrato contenido en el concepto de gasto "honorarios" por valor total de $26.904.666. Todo lo cual coincide con la forma de pago establecida. (ver cuadro de localización de recursos en el presupuesto de la CVC)**

MATRIZ No. 1
EXPERIENCIA
(JUSTIFICAR LAS CONDICIONES TECNICAS DE LA OBRA DE ACUERDO CON LA COMPLEJIDAD)

No aplica

MATRIZ No. 2
INDICADORES FINANCIEROS Y ORGANIZACIONALES
(JUSTIFICAR LAS CONDICIONES TECNICAS DE LA OBRA DE ACUERDO CON LA COMPLEJIDAD)

No aplica


CVC
Corporación Autónoma
Regional del Valle del Cauca

MATRIZ No. 3
RIESGOS

Frente a la contratación que pretende satisfacer la Corporación, se procede a asignar los riesgos entre las partes contratantes y la forma de mitigarlo, siguiendo el “Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación M-ICR-01” expedido por Colombia Compra Eficiente.

No.	Clase	Fuente	Etapa	Tipo	Descripción (qué puede pasar y cómo puede ocurrir)	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración del riesgo	Categoría	¿A quién se le asigna?	Tratamiento / Controles a ser implementados	Impacto después del tratamiento				¿Afecta la ejecución del contrato?	Persona responsable por implementar tratamiento	Fecha estimada en que se inicia el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración del riesgo	Categoría				¿Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?
1	Especifico	Externo	Ejecución	Riesgos económicos	Variación en los precios ofertados por el Contratista	Variación en las ganancias obtenidas por el contratista	3	3	6	Riesgo Alto	Contratista	El contratista debe prever en los costos de su oferta directos e indirectos que demandan su ejecución tales como honorarios, subcontratos, garantías, seguros, dirección y administración; utilidades e imprevistos ordinarios o normales dentro de las condiciones técnicas y económicas y financieras, existentes al momento de presentación de la oferta; el Contratista no recibirá contraprestación alguna adicional y cualquier	1	2	3	Moderado	Si	Contratista y CVC	El contratista de acuerdo con la organización de la empresa	Informes	Fecha del suministro

												variación del mismo deberá ser asumida por él								
2	General	Externo	Ejecución	Operacional	Retraso en la ejecución del contrato.	Problemas para el importe de los suministros de insumos necesarios para la ejecución del contrato	1	2	4	Bajo	Contratista	El Contratista debe tomar las medidas para garantizar el correcto suministro de insumos necesarios para la ejecución del contrato	1	1	3	Bajo	Si	Contratista	Inmediato	seguimiento	Una vez se presente
3	Específico	Externo	Ejecución	Operacional	Que no se entreguen productos ajustados a las condiciones técnicas exigidas	Declaración de Incumplimiento del contrato	2	4	6	Alto	Contratista	El supervisor y contratista deben estar al tanto de los productos que se van a recibir	1	1	2	Bajo	Si	Contratista	Fecha del suministro	seguimiento	Una vez se presente
4	Específico	Interno	Ejecución	Operacional	Fallas en la plataforma Tecnológica que soporta el servicio	Falencias en la resolución de problemas y entrega de información de alertas generadas por diferentes eventos en la infraestructura de TI.	2	4	5	Alto	Contratista	El Contratista debe garantizar el correcto cumplimiento de los ANS definidos. Documentar lecciones aprendidas de las fallas en las plataformas de TI	2	2	4	Bajo	si	Contratista	Fecha del suministro	seguimiento	Una vez se presente
5	Específico	Externo	Ejecución	Operacional	Equipo de trabajo con el que obtuvo el puntaje para ganar el contrato es diferente al equipo de trabajo para la ejecución	Retrasos en la ejecución del contrato	2	2	4	Bajo	Contratista	Tomar medidas necesarias para el cumplimiento de las obligaciones del contrato	1	1	2	Bajo	NO	Contratante	Inicio de contrato	Inicio de contrato	Verificación por parte del Interventor
6	Específico	Externo	Ejecución	Operacional	Bajo desempeño del personal	Deficiencias en la calidad de	2	2	4	Bajo	Contratista	Tomar medidas necesarias para el cumplimiento de las obligaciones del contrato	1	1	2	Bajo	NO	Contratante	Durante la	Con la	Diario

					del contratista	los trabajos													
7	Específico	Externo	Ejecución	Operacional	Incumplimiento del protocolo de bioseguridad para el manejo y control del riesgo del Coronavirus COVID-19 (Resolución 899 de 2020)	Contagio por COVID-19 y retrasos en la ejecución del contrato	3	3	6	Alto	Contratista	Tomar las medidas necesarias garantizar el cumplimiento del protocolo de bioseguridad para el manejo y control del riesgo del Coronavirus COVID-19 por parte del personal del consultor	1	1	2	Bajo	SI	Contratista	Durante la ejecución del contrato	Con la terminación del contrato	Diario
8	Específico	Externo	Ejecución	Operacional	Retraso o imposibilidad de entrega del producto o servicio contratado, a causa de medidas decretadas por el gobierno para controlar y manejar el riesgo del Coronavirus COVID-19	Retrasos o no entrega de productos del contrato	3	3	6	Alto	Contratista	Tomar las medidas pertinentes que permitan dar cumplimiento a la entrega de los productos del contrato	1	1	2	Bajo	SI	Contratista	Durante la ejecución del contrato	Con la terminación del contrato	Diario
9	General	Externo	Selección, Ejecución	Regulatorio	Nuevas cargas tributarias	Variación en el precio del contrato	2	2	4	Bajo	Contratante, Contratista	Si durante la etapa de selección y ejecución del contrato se impone nuevas cargas tributarias ya sea del orden nacional, departamental o municipal, se entiende que los gravámenes que sean aprobados antes de la presentación de la oferta, se encuentran incluidos en la misma, por lo cual no habrá lugar a reclamaciones a cargo del oferente. Por el contrario, si durante la etapa de selección luego de presentada la oferta y durante la ejecución del contrato, se imponen nuevas cargas tributarias de orden nacional, departamental o municipal, la misma deberá ser	1	1	2	Bajo	Si	Contratante	Durante la ejecución del contrato	Con la terminación del contrato	Una vez se presente

												compensada por el contratista								
10	General	Externo	Ejecución	Sociales o Políticos	Retraso o imposibilidad de entrega del producto o servicio contratado, por alteraciones del orden publico	Retraso en la ejecución del Contrato	3	2	5	Medio	Contratante, Contratista	El Contratista y Contratante deben tomar las medidas necesarias para garantizar el correcto desarrollo del objeto de presente contratación, velando por la integridad del personal de ambas partes.	2	2	4	Bajo	Si	Contratante, Contratista	Durante la ejecución del contrato	Con la terminación del contrato	Una vez se presente


CVC
Corporación Autónoma
Regional del Valle del Cauca