<table>
<tr><th colspan="3">INVITACIÓN PÚBLICA</th></tr>
<tr><td rowspan="2"></td><td rowspan="2">"CONTRATAR LA RENOVACIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS BITDEFENDER, CON ACTUALIZACION, SOPORTE, CAPACITACION Y ASISTENCIA TECNICA POR EL TERMINO DE UN AÑO, PARA LAS ESTACIONES DE TRABAJO Y SERVIDORES DE LA PLATAFORMA TECNOLOGICA DE LA GOBERNACION DE BOLIVAR"</td><td>DIRECCION LOGISTICA</td></tr>
<tr><td>PROCESO DE SELECCIÓN MC-DAL-041-2023</td></tr>
</table>

## INTRODUCCIÓN

**EL DEPARTAMENTO DE BOLÍVAR** en adelante la "Entidad", pone a disposición de los interesados la presente Invitación Pública para la selección del contratista encargado de ejecutar "**CONTRATAR LA RENOVACIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS BITDEFENDER, CON ACTUALIZACION, SOPORTE, CAPACITACION Y ASISTENCIA TECNICA POR EL TERMINO DE UN AÑO, PARA LAS ESTACIONES DE TRABAJO Y SERVIDORES DE LA PLATAFORMA TECNOLOGICA DE LA GOBERNACION DE BOLIVAR"** en adelante el "contrato".

Los Documentos del proceso de contratación, que incluyen los Estudios y Documentos previos, el Estudio de Sector, así como cualquiera de sus anexos, están a disposición del público en el Sistema Electrónico de Contratación Pública –SECOP II–.

La selección del contratista se realizará a través del proceso de contratación No. **MC-DAL-041-2023.**

La Entidad evaluará las ofertas con base en las reglas establecidas en la Invitación Pública y en la normativa aplicable.

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

## TABLA DE CONTENIDO


**INVITACIÓN PUBLICA No. MC-DAL-041-2023** .....

**CAPÍTULO I INFORMACIÓN GENERAL** ..... **4**

**1.1. OBJETO, PRESUPUESTO OFICIAL, PLAZO Y UBICACIÓN** ..... **4**

**1.2. DOCUMENTOS DEL PROCESO** ..... **4**

**1.3. COMUNICACIONES Y OBSERVACIONES AL PROCESO** ..... **4**

**1.4. CLASIFICADOR DE BIENES Y SERVICIOS DE NACIONES UNIDAS (UNSPSC)** ..... **4**

**1.5. RECURSOS QUE RESPALDAN LA PRESENTE CONTRATACIÓN** ..... **4**

**1.6. REGLAS DE SUBSANABILIDAD, EXPLICACIONES Y ACLARACIONES** ..... **5**

**1.7. CRONOGRAMA DEL PROCESO** ..... **5**

**1.8. IDIOMA** ..... **5**

**1.9. DOCUMENTOS OTORGADOS EN EL EXTERIOR** ..... **8**

**1.10. GLOSARIO** ..... **8**

**1.11. INFORMACIÓN INEXACTA** ..... **8**

**1.12. INFORMACIÓN RESERVADA** ..... **8**

**1.13. MONEDA** ..... **9**

**B. Conversión a Salarios Mínimos Mensuales Legales Vigentes (SMMLV):** ..... **9**

**1.14. CONFLICTO DE INTERÉS DE ORIGEN CONSTITUCIONAL O LEGAL** ..... **10**

**1.15. CAUSALES DE RECHAZO** ..... **10**

**1.16. CAUSALES PARA DECLARAR DESIERTO EL PROCESO DE SELECCIÓN** ..... **11**

**1.17. NORMAS DE INTERPRETACIÓN DE LA INVITACIÓN** ..... **11**

**1.18 RETIRO DE LA PROPUESTA** ..... **11**

**CAPÍTULO II ESPECIFICACIONES TÉCNICAS** ..... **12**

***2.2 ESPECIFICACIONES TECNICAS:*** ..... *12*

***EQUIPO DE TRABAJO*** ..... ***16***

**2.3 OBLIGACIONES DE LAS PARTES** ..... **29**

**2.3.1. OBLIGACIONES GENERALES DEL CONTRATISTA:** ..... **29**

**2.3.2 OBLIGACIONES ESPECIFICAS DEL CONTRATISTA** ..... **16**

**2.3.3. OBLIGACIONES DEL DEPARTAMENTO** ..... **17**

**2.4 ACREDITACIÓN DEL PAGO AL SISTEMA DE SEGURIDAD SOCIAL DURANTE LAEJECUCIÓN DEL CONTRATO** ..... **30**

**2.5 PLAZO PARA EJECUTAR EL CONTRATO** ..... **31**

**2.6 FORMA DE PAGO** ..... **31**

**OTROS MARCO TRIBUTARIO NACIONAL APLICABLE** ..... ¡Error! Marcador no definido.

**CAPÍTULO III ELABORACIÓN, PRESENTACIÓN Y EVALUACIÓN DE LAS OFERTAS** ..... **32**

**3.1. CARTA DE PRESENTACIÓN DE LA OFERTA** ..... **32**

**3.2. APODERADO** ..... **32**

**3.3. ELABORACIÓN Y PRESENTACIÓN DE LA OFERTA** ..... **33**

**3.4. CIERRE DEL PROCESO Y APERTURA DE OFERTAS** ..... **33**

**3.5. INFORME DE EVALUACIÓN** ..... **34**

**3.6. ACEPTACIÓN DE LA OFERTA** ..... **34**

**3.7. PROPUESTAS PARCIALES** ..... **34**

**3.8. PROPUESTAS ALTERNATIVAS** ..... **34**

**3.9. REGLAS PARA LOS PROCESOS ESTRUCTURADOS POR LOTES O GRUPOS** ..... **35**

**CAPÍTULO IV REQUISITOS HABILITANTES Y SU VERIFICACIÓN** ..... **35**

**4.1 GENERALIDADES** ..... **35**

**4.2 CAPACIDAD JURÍDICA** ..... **35**

**4.3 EXISTENCIA Y REPRESENTACIÓN LEGAL ..... 36**
**4.3.1 PERSONAS NATURALES ..... 36**
**4.3.2 PERSONAS JURÍDICAS ..... 36**
**4.3.3 PROPONENTES PLURALES ..... 38**
**4.4 CERTIFICACIÓN DE PAGOS DE SEGURIDAD SOCIAL Y APORTES LEGALES ..... 38**
**4.4.1 PERSONAS JURÍDICAS ..... 38**
**4.4.2 PERSONAS NATURALES ..... 39**
**4.4.3 PROPONENTES PLURALES ..... 39**
**4.4.4 SEGURIDAD SOCIAL PARA LA ACEPTACIÓN DE LA OFERTA ..... 39**
**4.5 EXPERIENCIA ..... 39**
**4.5.1 CARACTERÍSTICAS DE LOS CONTRATOS PRESENTADOS PARA ACREDITAR LAEXPERIENCIA EXIGIDA. 40**
**4.5.2 CONSIDERACIONES PARA LA VALIDEZ DE LA EXPERIENCIA REQUERIDA ..... 40**
**4.5.3 ACREDITACIÓN DE LA EXPERIENCIA REQUERIDA ..... 41**
**4.5.4 DOCUMENTOS VÁLIDOS PARA ACREDITAR LA EXPERIENCIA REQUERIDA ..... 41**
**DOCUMENTOS TECNICOS HABILITADOS ..... 41**
**4.5.5 PARA SUBCONTRATOS ..... 41**
**4.6. CAPACIDAD TECNICA** ..... 31
**CAPÍTULO V CRITERIOS DE EVALUACIÓN, CRITERIOS DE DESEMPATE Y OFERTAECONÓMICA ..... 43**
**5.1. OFERTA ECONÓMICA ..... 43**
**5.1.3 PRECIO ARTIFICIALMENTE BAJO ..... 43**
**5.1.4 CRITERIOS DE DESEMPATE ..... 44**
**CAPÍTULO VI RIESGOS ASOCIADOS AL CONTRATO, FORMA DE MITIGARLOS YASIGNACIÓN DE RIESGOS ..... 44**
**6.1 ASIGNACIÓN DE RIESGOS ..... 44**
**CAPÍTULO VII GARANTÍAS ..... 44**
**7.1 GARANTÍAS DEL CONTRATO ..... 44**
**7.2.1 GARANTÍA DE CUMPLIMIENTO ..... 44**
**CAPÍTULO VIII COMUNICACIÓN DE ACEPTACIÓN DE LA OFERTA Y CLÁUSULASADICIONALES ..... 45**
**8.1. MULTAS ..... 45**
**Causales: ..... 46**
**8.2. CLÁUSULA PENAL ..... 47**
**8.3. CLÁUSULAS EXCEPCIONALES ..... 47**
**8.4. INDEPENDENCIA DEL CONTRATISTA ..... 47**
**8.5. INEXISTENCIA DE RELACIÓN LABORAL ENTRE LA ENTIDAD Y ELCONTRATISTA ..... 47**
**8.6. CESIÓN ..... 48**
**8.7. LIQUIDACIÓN ..... 48**
**8.8. SOLUCIÓN DE CONTROVERSIAS ..... 48**
**CAPÍTULO IX LISTA DE ANEXOS, FORMATOS, MATRICES Y FORMULARIOS ..... 49**
**9.1. ANEXOS ..... 49**
**9.2. FORMATOS ..... 49**
**9.3. MATRICES ..... 49**
**9.4. FORMULARIOS ..... 49**

## CAPÍTULO I INFORMACIÓN GENERAL

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

El objeto, presupuesto oficial estimado, plazo y ubicación del proyecto objeto del presente proceso de contratación se identifican en la siguiente tabla:

| OBJETO DEL PROYECTO | PLAZO DEL CONTRATO | VALOR PRESUPUESTO OFICIAL (PESOS INCLUIDO IVA) | LUGAR(ES) DE EJECUCIÓN DEL CONTRATO |
|---|---|---|---|
| **CONTRATAR LA RENOVACIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS BITDEFENDER, CON ACTUALIZACION, SOPORTE, CAPACITACION Y ASISTENCIA TECNICA POR EL TERMINO DE UN AÑO, PARA LAS ESTACIONES DE TRABAJO Y SERVIDORES DE LA PLATAFORMA TECNOLOGICA DE LA GOBERNACION DE BOLIVAR"** | El plazo oficial de ejecución será hasta el 31 de diciembre de 2023 o hasta agotarse el presupuesto destinado para esta contratación, contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución, término durante el cual el contratista seleccionado deberá cumplir con el objeto contratado y el cual no podrá sobrepasar el 31 de diciembre de 2023. Este plazo se empezará a contabilizar una vez se expida el correspondiente registro presupuestal, y se aprueben las garantías exigidas | **NOVENTA Y CINCO MILLONES DE PESOS M/CTE LEGAL COLOMBIANA ($95.000.000) Incluido IVA**, y demás tasas, contribuciones e impuestos a que haya lugar para la legalización y ejecución del contrato | **CENTRO ADMINISTRATIVO DEPARTAMENTAL DE LA GOBERNACION DE BOLIVAR** |

### 1.2. DOCUMENTOS DEL PROCESO

Los documentos del proceso son los señalados en el capítulo IX, así como todos los señalados en el artículo 2.2.1.1.1.3.1. del Decreto 1082 de 2015

### 1.3. COMUNICACIONES Y OBSERVACIONES AL PROCESO

Las respuestas se comunicarán a través de la plataforma SECOP II, de acuerdo con el Manual de Uso y Condiciones de la plataforma del SECOP II.

Cuando el proponente registre el certificado de indisponibilidad de la plataforma, la entidad pone a disposición el siguiente correo: procesoslogistica@bolívar.gov.co

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

El objeto del presente proceso de contratación está codificada en el Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC, como se indica en la siguientetabla:

| GRUPO | SEGMENTO | FAMILIA | CLASE | PRODUCTO | DESCRIPCIÓN PRODUCTO |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| E | 43 | 23 | 32 | 00 | Software de seguridad y protección |
| E | 43 | 23 | 32 | 05 | Software de seguridad de transacciones y de protección contra virus |
| F | 81 | 11 | 25 | 00 | Servicios de alquiler o arrendamiento de licencias de software de computador |

## 1.5 RECURSOS QUE RESPALDAN LA PRESENTE CONTRATACIÓN

La entidad, para respaldar el compromiso derivado del presente proceso de contratación, cuenta con el siguiente certificado de disponibilidad presupuestal:

| Número certificado disponibilidad presupuestal | Fecha certificado disponibilidad presupuestal | Valor certificado de disponibilidad presupuestal |
|---|---|---|
| **1502** | **22 de noviembre de 2023** | **95,000,000.00** |

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

## 1.5. REGLAS DE SUBSANABILIDAD, EXPLICACIONES Y ACLARACIONES

El proponente tiene la responsabilidad y deber de presentar la oferta en forma completa e íntegra, esto es, cumpliendo el contenido de la Invitación y adjuntando los documentos de soporte o prueba de las condiciones que pretenda hacer valer en el proceso. No será posible subsanar los requisitos de la propuesta que afecten la asignación de puntaje, es decir, la oferta económica.

La entidad, al revisar la oferta de menor precio, verificará que cumpla las condiciones mínimas de la Invitación. Si no cumple solicitará al proponente, mínimo por el término de un (1) día hábil, que aclare, explique o aporte los documentos e información subsanable; en caso de que la entidad no fije un plazo específico, se entenderá que es de un (1) día hábil. No obstante, los proponentes no podrán completar, adicionar, modificar o mejorar la oferta económica, la cual, solo puede ser objeto de aclaraciones y explicaciones. Los proponentes deben aportar las aclaraciones o documentos requeridos hasta el plazo indicado, so pena que la entidad rechace la propuesta y revise la segunda oferta que ofrezca el menor precioy verifique que cumple los requisitos de la invitación. Si la segunda propuesta tampoco cumple se repetirá el procedimiento anterior, continuando con las ofertas que ofrezcan el siguiente menor precio.

En caso de que la entidad advierta la ausencia de requisitos o la falta de documentos referentes a la futura contratación o al proponente, y no los haya requerido durante el proceso de evaluación, podrá requerir al proponente, otorgándole un término mínimo de un
(1) día hábil contado desde el momento en el que advirtió su omisión, con el fin de que los aporte; en caso de que la entidad no fije un plazo específico, se entenderá que es de un (1) día hábil.

En virtud del principio de buena fe, los proponentes que presenten observaciones al procesoo a las ofertas y conductas de los demás oferentes, deben argumentar y demostrar la procedencia y oportunidad de estas.

## 1.6. CRONOGRAMA DEL PROCESO

La entidad debe elaborar el cronograma del proceso teniendo en cuenta los términos

legales para cada una de las etapas de proceso.

| ACTIVIDAD | FECHA | LUGAR | NORMA |
|---|---|---|---|
| Publicación de la invitación pública y estudios previos y Documentos del proceso de contratación | 05 de diciembre de 2023 | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Ley 1474/11, art. 94 |
| Plazo para recepción de observaciones | 06 de diciembre de 2023<br>Hasta las 3:00 p. m | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Ley 1474/11, art. 94 |
| Plazo para manifestación de interés de limitar la convocatoria a Mipymes | 06 de diciembre de 2023<br>Hasta las 3:30 p.m | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Fecha definida por la entidad |
| Respuesta a las observaciones a la invitación | 06 de diciembre de 2023<br>Hasta las 6:30 p.m | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Fecha definida por la entidad |
| Publicación del aviso de limitación a Mipymes o si podrá participar cualquier interesado | 06 de diciembre de 2023<br>Hasta las 6:45 p.m | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Fecha definida por la entidad |
| Plazo máximo para expedir adendas | 06 de diciembre de 2023<br>Hasta las 7:00 p.m | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Fecha definida por la entidad |
| **Presentación de Ofertas** | 07 de diciembre de 2023<br>Hasta las 10:00 a.m | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Fecha definida por la entidad |
| Apertura de ofertas | 07 de diciembre 2023<br>Hasta las 10:05 a.m | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Fecha definida por la entidad |
| Evaluación de las ofertas | 11 de diciembre de octubre de 2023 | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Fecha definida por la entidad |
| Publicación del informe de evaluación | 11 de diciembre de 2023<br>Hasta las 11:59 p.m | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Fecha definida por la entidad |
| Presentación de observaciones al informe de verificación o evaluación | 12 de diciembre de 2023<br>Hasta las 11:59 p.m | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Dto.1082/15 art.2.2.1.2.1.5.2., numeral 5 |
| Aceptación de ofertas | 13 de diciembre de 2023<br>Hasta las 7:00 p.m | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Fecha definida por la entidad |
| Entrega de las garantías de ejecución del contrato | 14 de diciembre de 2023<br>Hasta las 5:00 p.m | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Dto. 1082/15 art. 2.2.1.2.1.5.2. |
| Aprobación de las garantías de ejecución del contrato | 14 de diciembre de 2023<br>Hasta las 7:00 p.m | En el SECOP II a través del Portal Único de Contratación, link :::http://community.secop.gov.co/sts/cce/login.aspx | Dto. 1082/15 art. 2.2.1.2.1.5.2. |

## 1.8. LIMITACIÓN A MIPYMES

De conformidad con el numeral 3 del artículo 2.2.1.2.1.5.2. del Decreto 1082 de 2015, modificado por el Decreto 1860 de 2021, dentro del mismo término establecido para realizar observaciones a la invitación pública, los interesados podrán solicitar limitación del mismo a mipymes, de acuerdo con los criterios y requisitos establecidos en el artículo 2.2.1.2.4.2.2. y subsiguientes del Decreto 1082 de 2015, modificado igualmente por el Decreto 1860 de 2021, que establece:

*"Artículo 2.2.1.2.4.2.2. Convocatorias Iímítadas a Mípyme. Las Entidades Estatales independientemente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos, deben limitar la convocatoria de los Procesos de Contratación con pluralidad de oferentes a las Mipyme colombianas con mínimo un (1) año de existencia, cuando concurran los siguientes requisitos:*

*1. El valor del Proceso de Contratación sea menor a ciento veinticinco mil dólares de los Estados Unidos de América (US$125.000), liquidados con la tasa de cambio que para el efecto determina cada dos años el Ministerio de Comercio, Industria y Turismo.*

*2. Se hayan recibido solicitudes de por lo menos dos (2) Mipyme colombianas para limitar la convocatoria a Mipyme colombianas.*

*Las Entidades Estatales independientemente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos, deben recibir estas solicitudes por lo menos un (1) día hábil antes de la expedición del acto administrativo de apertura, o el que haga sus veces de acuerdo con la normativa aplicable a cada Proceso de Contratación.*

*Tratándose de personas jurídicas, las solicitudes solo las podrán realizar Mipyme, cuyo objeto social les permita ejecutar el contrato relacionado con el proceso contractual.*

*Parágrafo. Las cooperativas y demás entidades de economía solidaria, siempre que tengan la calidad de Mipyme, podrán solicitar y participar en las convocatorias limitadas en las mismas condiciones dispuestas en el presente artículo. 5 Artículo 2.2.1.2.4.2.3. Limitaciones territoriales. De conformidad con el parágrafo 1 del artículo 12 de la Ley 1150 de 2007, las Entidades Estatales, independientemente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos, pueden realizar convocatorias limitadas a Mipyme colombianas que tengan domicilio en los departamentos o municipios en donde se va a ejecutar el contrato. Cada Mipyme deberá acreditar su domicilio con los documentos a los que se refiere el siguiente artículo.*

*Artículo 2.2.1.2.4.2.4. Acreditación de requisitos para participar en convocatorias limitadas. La Mipyme colombianas deben acreditar que tiene el tamaño empresarial establecido por la ley de la siguiente manera:*

*1. Las personas naturales mediante certificación expedida por ellos y un contador público, adjuntando copia del registro mercantil.*

*2. Las personas jurídicas mediante certificación expedida por el representante legal y el contador o revisor fiscal, si están obligados a tenerlo, adjuntando copia del certificado de existencia y representación legal expedido por la Cámara de Comercio o por la autoridad competente para expedir dicha certificación. Para la acreditación deberán observarse los rangos de clasificación empresarial establecidos de conformidad con la Ley 590 de 2000 y el Decreto 1074 de 2015, o las normas que lo modifiquen, sustituyan o complementen.*

*Parágrafo 1. En todo caso, las Mipyme también podrán acreditar esta condición con la copia del certificado del Registro Único de Proponentes, el cual deberá encontrarse vigente y en firme al momento de su presentación.*

*Parágrafo 2. Para efectos de la limitación a Mipyme, los proponentes aportarán la copia del registro mercantil, del certificado de existencia y representación legal o del Registro Único de Proponentes, según corresponda conforme a las reglas precedentes, con una fecha de máximo sesenta (60) días calendario anteriores a la prevista en el cronograma del Proceso de*

*Contratación para el inicio del plazo para solicitar la convocatoria limitada.*

*Parágrafo 3. En las convocatorias limitadas, las Entidades Estatales independientemente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos, solo deberán aceptar las ofertas de Mipyme o de proponentes plurales integrados únicamente por Mipyme.*

*Parágrafo 4. Los incentivos previstos en los artículos 2.2.1.2.4.2.2 y 2.2.1.2.4.2.3 de este Decreto no excluyen la aplicación de los criterios diferenciales para los emprendimientos y empresas de mujeres en el sistema de compras públicas. "*

### 1.9. IDIOMA

Los documentos y las comunicaciones entregadas, enviadas o expedidas por los proponentes o por terceros para el proceso de contratación, o para ser tenidos en cuenta enel mismo, deben entregarse en idioma castellano. Los documentos y comunicaciones en un idioma distinto pueden presentarse en su lengua original, pero junto con la traducción simple al castellano.

### 1.10. 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 seanintervenidos por un funcionario público, en cuyo caso requieren apostilla o legalización, enla forma antes indicada.

Para el trámite de apostilla o legalización de documentos otorgados en el exterior y la acreditación de la formación académica obtenida en el exterior, las entidades aplicarán los parámetros establecidos en las normas que regulen la materia.

### 1.11. GLOSARIO

Para los fines de esta Invitación, a menos que expresamente se estipule de otra manera, los términos deben entenderse de acuerdo con la definición contenida en el artículo 2.2.1.1.1.3.1 del Decreto 1082 de 2015, la Ley 1682 de 2013. Los términos no definidos deben entenderse de conformidad con su significado natural y obvio.

### 1.12. INFORMACIÓN INEXACTA

La entidad se reserva el derecho de verificar integralmente la información aportada por el proponente, pudiendo acudir a las autoridades, personas, empresas o entidades respectivas.

Cuando exista inconsistencia entre la información suministrada por el proponente y la verificada por la entidad, la información que se pretende demostrar se tendrá por no acreditada.

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

### 1.13. INFORMACIÓN RESERVADA

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

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

**1.14. MONEDA**

**A. Monedas Extranjeras**

Los valores de los documentos aportados en la propuesta deben presentarse en Pesos Colombianos. Cuando un valor se exprese en moneda extranjera, debe 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 el valor correspondiente al promedio entre la TRM de la fecha de inicio del contrato y la TRMde 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 el Formato 3- Experiencia; la TRM utilizada será la certificada por la Superintendencia Financiera de Colombia.

II. Si los valores del contrato están expresados originalmente en una moneda diferentea 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 delcontrato. Para tales efectos, se puede 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 Dólares de los Estados Unidos de América, 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 decambio entre la moneda y los Dólares de los Estados Unidos de América, el proponente podrá utilizar la página web https://www.oanda.com/lang/es/currency/converter/. Hecho esto se procederá en la forma señalada en el numeral III.

**B. 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) se seguirá el siguiente proceso:

I. Los valores convertidos a Pesos Colombianos, aplicando el proceso descrito en el literal anterior, o cuya moneda de origen sea el peso colombiano, deben ser convertidos a SMMLV, para lo cual se emplearán los valores históricos de SMMLV señalados por el Banco de la República (http://www.banrep.gov.co/es/mercado-laboral/salarios), del añocorrespondiente a la fecha de terminación del contrato.

II. Los valores convertidos a SMMLV se deben ajustar a la unidad más próxima de la siguiente forma: hacia arriba para valores mayores o iguales a cero punto cinco (0.5) yhacia abajo para valores menores a cero punto cinco (0.5).

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

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

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

### 1.15. CONFLICTO DE INTERÉS DE ORIGEN CONSTITUCIONAL O LEGAL

No podrán participar en el procedimiento de contratación, y por lo tanto no serán objeto de evaluación, ni podrán ser adjudicatarios, quienes bajo cualquier circunstancia se encuentrenen situaciones de conflicto de interés, que afecten o pongan en riesgo los principios de la contratación pública, de acuerdo con las causales o circunstancias previstas en la Constitución o la ley.

### 1.16. CAUSALES DE RECHAZO

Son causales de rechazo de las propuestas las siguientes:

**A.** Que el proponente o alguno de los integrantes del proponente plural esté incurso en causal de inhabilidad, incompatibilidad o prohibición previstas en la legislación para contratar.
**B.** Que el proponente o alguno de los integrantes del proponente plural esté reportado en el Boletín de Responsables Fiscales que administra la Contraloría General de la República.
**C.** Que la persona jurídica proponente individual o integrante del proponente plural esté incursa en la situación descrita en el numeral 1 del artículo 38 de la Ley 1116 de 2006, relacionada con la disolución de la persona jurídica.
**D.** Que el proponente no aclare, subsane o aporte documentos necesarios para cumplir un requisito habilitante, o aportándolos no lo haga de forma correcta, en los términos establecidos en la sección 1.6.
**E.** Que el proponente aporte información inexacta sobre la cual pueda existir una posible falsedad en los términos de la sección 1.11.
**F.** Que el proponente se encuentre incurso en un conflicto de interés previsto en una normade rango constitucional o legal.
**G.** Que el objeto social del proponente o el de alguno de sus integrantes no le permita ejecutar el objeto del contrato.
**H.** Que el valor total de la oferta o el obtenido de la corrección aritmética exceda el presupuesto oficial estimado del contrato.
**I.** Presentar la oferta con tachaduras o enmendaduras que no estén convalidadas en la forma indicada en la sección 3.3 de la invitación.
**J.** Que el proponente adicione, suprima, cambie o modifique los ítems, la descripción, las unidades o cantidades señaladas en el Formulario 1– Formulario de oferta económica
**K.** Superar el valor unitario de alguno o algunos de los ítems ofrecidos con respecto al valor establecido para cada ítem promedio del presupuesto oficial en consideración al manejo de precios artificialmente bajo.
**L.** Cuando el proponente omita diligenciar algún ítem o componente de la oferta.
**M.** Cuando el proponente ofrezca por una unidad de medida diferente a la solicitada por la Entidad Estatal.
**N.** Cuando el proponente ofrece condiciones técnicas o de ejecución del contrato que no se ajustan a las especificaciones requeridas por la Entidad Estatal.
**O.** Cuando se presente propuesta condicionada para la aceptación de la oferta.
**P.** Presentar más de una oferta económica.
**Q.** Presentar la oferta extemporáneamente.
**R.** No presentar oferta económica.
**S.** Cuando se determine que el valor total de la oferta es artificialmente bajo, de acuerdo con lo establecido en la sección 5.1.3.
**T.** Cuando se presenten propuestas parciales y esta posibilidad no haya sido establecida en la invitación pública.

**U.** Ofrecer un plazo mayor al previsto por la entidad.
**V.** Cuando una misma persona natural o jurídica, o integrante de un proponente plural, presente o haga parte en más de una propuesta para el mismo proceso. En tal caso todas las propuestas serán rechazadas.
**W.** Cuando el representante legal de la persona jurídica tenga limitaciones para comprometer a la sociedad y no cuente con la autorización suficiente del órgano social.
**X.** Las demás previstas en la ley.

## 1.17. CAUSALES PARA DECLARAR DESIERTO EL PROCESO DE SELECCIÓN

La entidad podrá declarar desierto el procedimiento de selección cuando:

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

## 1.18. NORMAS DE INTERPRETACIÓN DE LA INVITACIÓN

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

Además, se seguirán los siguientes criterios para interpretar y entender la invitación:

**A.** El orden de los numerales, capítulos y cláusulas de esta invitación no deben interpretarse como un grado de prelación entre los mismos.
**B.** Los títulos de los numerales y capítulos utilizados en esta invitación solo sirven como referencia y no afectan la interpretación de su contenido.
**C.** Las palabras en singular se entenderán también en plural y viceversa, cuando lo exija el contexto; y las palabras en género femenino, se entenderán en género masculino y viceversa, cuando el contexto lo requiera.
**D.** Los plazos en días establecidos en esta invitación se entienden como hábiles, salvo que de manera expresa la ley o la entidad indique que se trata de calendario o de meses. Cuando el vencimiento de un plazo corresponda a un día no hábil o no laboral para la entidad, este se trasladará al día hábil siguiente.
**E.** En caso de contradicción entre el contenido establecido en los Documentos Tipo y el incluido por la entidad, por los proponentes o por el contratista en los documentos del proceso, primará lo señalado en los Documentos Tipo.
**F.** Las entidades estatales contratantes no podrán incluir o modificar dentro de los documentos del proceso, las condiciones habilitantes y factores técnicos señalados en los Documentos Tipo.
**G.** Las palabras definidas en esta invitación deben entenderse en dicho sentido.
**H.** Las referencias a normas jurídicas incluyen las disposiciones que las modifiquen, adicionen, sustituyan o complementen.
**I.** Los Documentos Tipo son inalterables y no se podrán incluir o modificar los Anexos, Formatos y Formularios, ni exigir soportes o requisitos adicionales, salvo cuando se permita en forma expresa, es decir, en los aspectos incluidos en corchetes y resaltados en gris.

## 1.19 RETIRO DE LA PROPUESTA

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

Si la propuesta es retirada después del cierre del proceso de selección, la entidad puede siniestrar la garantía de seriedad de la oferta, cuando la haya exigido.

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

## CAPÍTULO II ESPECIFICACIONES TÉCNICAS

**2. DESCRIPCIÓN DEL PROYECTO: CONTRATAR LA RENOVACIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS BITDEFENDER, CON ACTUALIZACION, SOPORTE, CAPACITACION Y ASISTENCIA TECNICA POR EL TERMINO DE UN AÑO, PARA LAS ESTACIONES DE TRABAJO Y SERVIDORES DE LA PLATAFORMA TECNOLOGICA DE LA GOBERNACION DE BOLIVAR"**

**2.2 ESPECIFICACIONES TECNICAS:**
A continuación, se relacionan las condiciones técnicas para cumplir con el objeto del contrato, las que se constituyen en requisitos mínimos de orden técnico que debe ofertar cada proponente al momento de la presentación de su propuesta:

| ITEM | DESCRIPCION | CANT. |
|---|---|---|
| 1 | **SUMINISTRO DE LICENCIAS DE ANTIVIRUS PARA WINDOWS**<br><br>A. Consola de administración que proporciona las funcionalidades básicas y avanzadas de gestión de productos.<br>B. Servicios de seguridad para equipos de escritorio físicos, portátiles y servidores.<br>C. Servicios de seguridad para entornos virtualizados que proporcionan un servicio antimalware creado especialmente para un entorno virtualizado.<br>D. Escalabilidad servicios de seguridad para dispositivos móviles que brindan seguridad y control de cumplimiento para teléfonos inteligentes y tabletas basados en sistemas operativos iOS y Android.<br>E. Servicios de seguridad para la introspección del hipervisor que proporciona la introspección en tiempo real de la memoria de la máquina virtual para prevenir e identificar ataques avanzados.<br>F. Servicios de seguridad para servidores que ofrecen opciones de antimalware, antispam, control de contenido y filtrado de archivos adjuntos<br><br>1. El paquete de instalación debe entregarse como un solo dispositivo virtual (imagen virtual). Las plataformas de virtualización soportadas deben ser:<br><br>a. VMware vSphere, VMware View, VMware Horizon suites<br>b. Citrix XenServer, Citrix XenApp, Citrix XenDesktop<br>c. Microsoft Hyper-V<br>d. Red Hat Enterprise Virtualization<br>e. Kernel-based Virtual Machine or KVM<br>f. Oracle VM<br>g. Nutanix | 800 licencias |

| | | |
|---|---|---|
| | Se deben admitir otras plataformas de virtualización si se realiza una solicitud al desarrollador de productos antimalware.<br><br>2. El producto debe permitir la implementación centralizada de máquinas de escaneo dedicadas.<br>3. Para fines de escalabilidad, el producto debe permitir que cualquier componente o servicio se instale de forma independiente o en un método agrupado<br>4. Para propósitos de escalabilidad, el producto debe tener componentes dedicados para servicios de base de datos, servicios de comunicación, actualización y servicios web.<br>5. Para alta disponibilidad y balanceo de carga, el producto debe incluir un módulo dedicado de balanceador de carga disponible.<br>6. Licencia flexible (clave separada para cada servicio de seguridad que permite un número diferente de objetos con licencia y fechas de vencimiento diferentes, historial de todas las claves ingresadas) o licencia única que puede administrar todos los servicios de seguridad.<br>7. Actualización con un clic: un clic para actualizar todos los componentes de la consola de administración, sin depender de su orden de instalación ni de ningún otro requisito.<br>8. Actualizaciones a pedido que permitirán a los administradores elegir qué paquetes de servicios de seguridad se actualizarán para ahorrar ancho de banda.<br>9. Debería usar una base de datos no relacional / no SQL, sin requerir ninguna clave de licencia de terceros para implementaciones mayores que un cierto número de puntos finales.<br>10. Las notificaciones deben mostrarse en el menú principal, con aspectos destacados de los elementos no leídos, con la capacidad de enviarlo por correo electrónico, alertando al administrador sobre problemas importantes: problemas de licencias, alertas de brotes de malware y / o máquinas desactualizadas.<br>11. Capacidad para agregar, eliminar, organizar, configurar y personalizar múltiples portlets de seguridad<br>12. Capacidad de soportar múltiples páginas con múltiples portlets de seguridad.<br>13. Capacidad para ofrecer información de seguridad en tiempo real con gráficos fáciles de leer.<br>14. Capacidad para configurar el destino de los informes, el fondo del tipo de informe de seguridad, el intervalo de tiempo para la información presentada y mostrada y el nombre del portlet.<br><br>15. Integración con Microsoft Active Directory, VMware vCenter, Citrix Xen para importar el inventario e información de estas plataformas.<br>16. Tiempo de sincronización configurable (en horas) con Microsoft Active Directory.<br>17. Integración con Microsoft Hyper-V, RedHat Linux Virtual Machine, Oracle VM, KVM y cualquier otra máquina virtual que se descubra a través del descubrimiento de la red.<br>18. Descubrimiento de redes para máquinas no integradas en Microsoft Active Directory, VMware vCenter, Citrix XenServer, tanto para estaciones de trabajo físicas como virtuales y servidores.<br>19. Búsqueda en tiempo real, clasificación y filtrado por nombre, sistema operativo, dirección IP, FQDN o etiqueta.<br>20. Capacidades de implementación remota y desinstalación del producto antimalware existente.<br>21. Paquetes de instalación manual y configurable para el producto antimalware.<br>22. Capacidad para configurar y ejecutar tareas de escaneo remoto.<br>23. Capacidad para reiniciar remotamente un punto final.<br>24. Capacidad para ver la sección de resultados de tareas centralizada con información detallada de cada subtarea.<br>25. Capacidad para asignar pólizas en todos los niveles de gestión.<br>26. Capacidad para configurar la herencia de políticas y forzar la configuración de políticas. | |

| | | |
|---|---|---|
| | 27. Capacidad para ver las propiedades detalladas de los puntos finales administrados, como el nombre, IP, sistema operativo, grupo, política asignada, estado de las capas de protección, realzar investigación forense de los registros recopilados, resolución de problemas y el estado más reciente del malware, auditoria de seguridad, los últimos registros de análisis y los usuarios conectados al punto final<br>28. Capacidad para aplicar políticas basadas en la ubicación y basadas en el usuario registrado.<br>29. Capacidad para aplicar varias políticas a un único punto final, pero solo una activa a la vez.<br>30. Capacidad para aplicar una política a un grupo de puntos finales.<br>31. Capacidad de permitir Perfiles para reglas de políticas.<br>32. Una plantilla única para cada servicio de seguridad.<br>Cada servicio de seguridad tiene su plantilla de política configurable con opciones específicas para activar / desactivar y configurar funcionalidades como el análisis antimalware, las capacidades de la zona de pruebas en la nube, las opciones de aprendizaje automático, la introspección del hipervisor, el cortafuegos, el control de acceso a la red, la inclusión en la lista blanca de aplicaciones, la lista negra de aplicaciones y el acceso a la web. control, control de dispositivos, ubicación de dispositivos, aplicación de autenticación y acciones a tomar en caso de malware y dispositivos no compatibles detectados, como bloqueo remoto, desbloqueo, borrado, cifrado SD.<br>33. Gran cantidad de informes.<br>34. Fácil de usar desde una vista: resumen y detalles en la misma página, sección de resumen activo (filtra los detalles haciendo clic en la sección de resumen).<br>35. Programado, se puede enviar por correo a cualquier número de destinatarios (no es necesario tener también una cuenta en la consola).<br>36. Filtros para informes programados para recibir por correo únicamente información relevante para cada usuario.<br>37. Archivar con todas las instancias generadas de un informe programado.<br>38. Exportar resumen a archivo .pdf, detalles a archivo .csv.<br>39. Restauraciones remotas, con ubicación configurable y borrar.<br>40. Capacidad de centralizar la cuarentena para archivos infectados.<br>41. Capacidad de aplicar filtro para equipos y maquinas virtuales<br>42. Capacidad de aplicar filtro para servidores Exchange on-premise<br>43. Descargue archivos, disponibles solo para máquinas virtuales integradas con vShield o NSX.<br>44. Personalice la hora en que los archivos se almacenan en cuarentena hasta 90 días.<br>45. Administración basada en roles.<br>46. Múltiples tipos predefinidos:.<br>a. Administrador de Compañía: Configure los ajustes del Centro de control, gestionar las claves de licencia de los servicios de seguridad, administrar usuarios, administrar redes, ver y analizar datos, investigación avanzada.<br>b. Administrador de red: Administrar usuarios, Administrar redes, Ver y analizar datos<br>c. Analista de Seguridad: ver y analizar datos.<br>1. Lista de usuarios que se puede importar desde Microsoft Active Directory (la autenticación AD se usará para iniciar sesión).<br>2. Configuración detallada de los derechos de destino administrativos, para seleccionar qué servicios y objetos puede administrar un usuario. Cierre de sesión automático para cualquier tipo de usuario para mayor seguridad con respecto a la información que se muestra en la consola de administración.<br>47. Registrar las acciones del usuario para su cumplimiento.<br>48. Registros detallados para cada acción del usuario.<br>49. Búsqueda compleja<br>50. El acceso a la consola de administración debe estar protegido (https).<br>51. La solución permite habilitar el acceso con MFA (Múltiple Factor de Autenticación)<br>52. El servidor web, desde la consola de administración central, debe permitir la | |

| | | |
|---|---|---|
| | importación de certificados digitales emitidos por una autoridad de certificación con licencia o por su propia organización. Importar certificados para que sea intuitivo y hecho desde la consola de administración central.<br>53. La gestión y la comunicación con dispositivos móviles (iOS) deben realizarse de forma segura, a través de certificados digitales. Estos certificados serán firmados por una Autoridad de Certificación autorizada o por su propia organización.<br>54. Le permite importar la cadena de certificados de PKI (infraestructura de clave pública).<br>55. Debe admitir claves de cifrado de certificado digital con una longitud mínima de 1024 bits.<br>56. Los certificados digitales, una vez importados, deben ser reemplazables en caso de que caduquen o sean revocados.<br>57. Los certificados aceptados en el proceso de importación deben estar en formato pfx o p12 y protegidos por una contraseña.<br>58. La solución debe ser capaz de generar certificados digitales por sí misma.<br>59. La solución debe poder mostrar en la consola central información sobre los certificados: nombre, autoridad de emisión, fecha de emisión y fecha de vencimiento de los certificados emitidos.<br><br>60. La solución debe permitir la prueba de nuevos kits o actualizaciones de productos en un entorno cerrado.<br>61. La solución permite recibir actualizaciones de manera prioritaria.<br>62. La solución debe tener la capacidad de decidir qué kits se publicarán en la red.<br>63. La solución debe poder definir y aplicar diferentes políticas para los puntos finales críticos de producción y actualizarlos después de que se haya probado el nuevo paquete.<br>64. La solución debe poder desactivar la opción de clasificación.<br>65. La plataforma de ensayo debe entregarse como un dispositivo virtual.<br>66. El servidor de actualización puede actuar como una puerta de enlace para los datos.<br>67. La consola y la plataforma de pruebas deben poder descargar automáticamente nuevos kits.<br>68. La consola debe poder configurar el número máximo de kits que puede almacenar.<br>69. La opción de organización puede definir varios anillos de actualización para aplicar actualizaciones de productos.<br>70. La solución permite asignar un role de Relay a sus agentes con el fin de proveer actualizaciones de seguridad y productos a los demás agentes instalados en los puntos finales de la red.<br><br>71. La solución puede usar actualizaciones fuera de línea en una infraestructura aislada.<br>72. Las actualizaciones se pueden recuperar y transferir a través de USB HDD / USB Stick, File Server, FTP e instalarse en la infraestructura aislada.<br><br>73. La solución debe permitir a los administradores utilizar la llamada a la API.<br>74. La solución debe incluir métodos para administrar cuentas de usuario, configurar notificaciones, administrar grupos, carpetas y puntos finales, administrar políticas, generar informes a través de APIs.<br><br>75. La existencia de un único motor antimalware.<br>76. La solución debe proveer capacidades de protección para Windows, MacOS y Linux.<br>77. La solución debe proveer un único instalador para cada plataforma (por ejemplo un único instalador para sistemas operativos Windows, único instalador para Sistemas operativos MacOS, igual para Linux)<br>78. Para minimizar el consumo de recursos, los productos antimalware deben permitir la instalación de módulos personalizados (por ejemplo, la instalación del producto antimalware sin el módulo de control de acceso web o sin el módulo Firewall).<br><br>2. Requisitos del sistema:<br><br>• Sistemas operativos para estaciones de trabajo: Windows 11, Windows 10, | |

Windows 8.1, Windows 8, Windows 7 Service Pack 3.

- Sistemas operativos de servidor: Windows Server 2022, Windows Server 2019 Core, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2.

3. Administración e instalación remota:

1. Antes de la instalación, el administrador puede personalizar los paquetes de instalación incluyendo solo los módulos deseados: análisis basado en el comportamiento, cifrado completo del disco, firewall, control de contenido, control de dispositivos, control de aplicaciones, administración de parches.
2. La instalación se puede realizar de varias formas:
   a. Al descargar el paquete antimalware directamente a la estación de trabajo donde se instalará.
   b. Mediante la instalación remota, directamente desde la consola web.
3. La instalación en máquinas desde una ubicación remota se realizará utilizando un cliente instalado existente en estas ubicaciones para minimizar el tráfico WAN.
4. La consola de administración informará el número de estaciones de trabajo que tienen el antimalware instalado y el número de estaciones de trabajo que están desprotegidas.
5. La consola de administración incluirá en los paneles / widgets configurables del panel de control.
6. La consola de administración incluirá información detallada sobre las estaciones de trabajo / servidores: nombre, IP, sistema operativo, módulos instalados, política aplicada, información de actualización, etc.
7. La consola de administración permitirá al administrador enviar una política para configurar todo el producto antimalware, tanto para estaciones de trabajo como para servidores.
8. La consola de administración permitirá tres tipos de cuentas, Administrador de compañía, administrador de red y auditor de seguridad, que pueden asignarse a qué grupos de usuarios pueden cambiar la configuración o generar informes.
9. La consola de administración incluirá una sección de registro donde se mencionarán todas las acciones, con información detallada: iniciar sesión, editar, crear, cerrar sesión, mover, etc.
10. La consola de administración permitirá la posibilidad de crear un paquete único, utilizado para sistemas operativos de 32 bits y de 64 bits, Windows, MAC y Linux.
11. La consola de administración permitirá al administrador crear grupos o subgrupos para la administración de estaciones de trabajo.
12. Tenga la posibilidad de seleccionar qué cliente descubrirá las otras computadoras en la red.

4. Las principales características y funcionalidades del antimalware y el módulo antispyware:

1. El administrador de la solución puede configurar el escaneo automático en tiempo real para que no analice archivos o archivos con un tamaño mayor que "x" MB.
2. El escaneo automático en tiempo real puede admitir escanear archivos con hasta 16 niveles de profundidad.
3. Escaneo basado en firmas.
4. Escaneo heurístico del comportamiento y monitoreo de procesos.
5. Escaneo en la nube y tecnología de aprendizaje automático.
6. Tecnología anti-ransomware y anti-exploit para firmas o familias conocidas
7. Tecnologías de Hyperdetect para APT, Ransomware, Exploits Avanzados para ataques de día 0 o desconocidos.
8. Capacidad para detectar ataques sin archivos, incluidos aquellos que utilizan herramientas legítimas del sistema operativo, como Powershell o intérpretes de

| | | |
|---|---|---|
| | scripts. La solución no debe bloquear globalmente los scripts para lograr esto.<br>9. Capacidad de realizar mitigación de ransomware, permitiendo reestablecer archivos afectados a través de los ajustes de políticas definidos por el administrador; la mitigación de ransomware de tener la capacidad de ajustar la recuperación de los archivos ante un incidente de forma manual o automática.<br>10. Capa de seguridad adicional de próxima generación, basada en heurísticas agresivas y tecnología de aprendizaje automático, para detectar y bloquear la nueva generación de ataques avanzados o dirigidos y malware sofisticado antes de la ejecución. Debe proporcionar:<br>a. Clasificación de los tipos de ataque.<br>b. Posibilidad de informar únicamente sobre amenazas detectadas, sin bloquearlas.<br>c. Capacidad para ajustar la agresividad de detección para cada categoría de ataque, con opciones para tomar medidas en detecciones de mayor confianza y también informar todas las demás detecciones de menor confianza. Al menos 3 niveles de detección estarán disponibles.<br>d. Capacidad para realizar diferentes acciones sobre los archivos detectados y las amenazas basadas en la red.<br>11. Escaneo bajo demanda y en acceso de cualquier medio de almacenamiento de información (CD, discos duros externos, disco compartido). Además, el proceso de exploración se puede detener si los dispositivos de medios de almacenamiento contienen información de más de "x" MB.<br>12. Escaneo automático de correos electrónicos a nivel de estación de trabajo, independientemente del cliente de correo electrónico, para los protocolos SMTP y POP3.<br>13. Configuración de las rutas a escanear, hasta el nivel de archivo.<br>14. La solución debe proporcionar Exclusiones incorporadas para roles de servidor de Microsoft (DNS, DHCP, AD, Exchange, Sharepoint).<br>15. El producto antimalware permitirá definir la lista de exclusión del análisis, tanto para el análisis "en acceso" como para el análisis "a pedido", para ciertas carpetas, discos, archivos, extensiones o procesos.<br>16. Con una base de datos completa de firmas de spyware y detección heurística de estos programas, el producto tendrá que ofrecer protección antispyware.<br>17. Para no sobrecargar los recursos del sistema, el producto antimalware debe contener un solo motor de análisis. Podrá ejecutar exploraciones programadas con baja prioridad y puede apagarse automáticamente después de explorar la estación de trabajo.<br>18. Para una mayor protección, antimalware debe tener 4 tipos de detección: basada en firmas, basada en heurísticas, procesos de monitoreo continuo y escaneo en la nube.<br>19. Para una mayor protección, antimalware debería poder escanear HTTP y SSL también.<br>20. Para una mejor administración del antimalware instalado en las estaciones de trabajo, el producto incluirá la opción de establecer una contraseña para la protección de la desinstalación.<br>21. Para la seguridad del usuario, el cliente incluirá un módulo antiphishing que tendrá la opción de verificar los enlaces buscados con los motores de búsqueda (Asesor de búsqueda).<br>22. La aplicación antimalware debería ofrecer acceso para el sistema operativo Linux.<br><br>5. Firewall:<br><br>1. El módulo se puede instalar / desinstalar de acuerdo con las preferencias del administrador.<br><br>6. Cuarentena:<br><br>1. El producto antimalware debe permitir el envío automático de los archivos en | |

cuarentena al laboratorio de virus.

2. El envío de los archivos en cuarentena se realizará automáticamente en un intervalo de tiempo predefinido (número de horas) establecido por el administrador.
3. El producto antimalware debe permitir la eliminación automática de archivos en cuarentena más antiguos que un período determinado, sin ocupar espacio de almacenamiento innecesario.
4. La capacidad de mover un archivo de la cuarentena a su ubicación original.
5. Cuarentena centralizada. La capacidad de recopilar de forma segura todos los archivos en cuarentena desde puntos finales protegidos a una ubicación única para una investigación más profunda.
6. La cuarentena permitirá que los objetos se escaneen después de cada actualización de la firma.
7. El producto antimalware debe poder guardar una copia de un archivo de malware y enviarlo a cuarentena antes de realizar acciones de Eliminar o Desinfectar.

Protección de datos:

1. Permite el bloqueo de datos confidenciales (tarjeta de identificación personal, cuenta bancaria, etc.) tanto para HTTP como para SMTP, mediante la creación de reglas específicas.

7. Control de Usuario:

1. El producto habrá integrado un módulo de control de usuario con las siguientes características:
   a. Bloqueo del acceso a Internet para clientes específicos o grupos de clientes.
   b. Bloqueando el acceso a ciertas aplicaciones.
   c. Bloqueando el acceso a internet por ciertos periodos de tiempo.
   d. Bloqueo de páginas web que contengan determinadas palabras clave.
   e. Permitiendo el acceso a páginas web específicas especificadas por el administrador.
   f. Restringir el acceso a ciertos sitios web por algunas categorías predeterminadas (por ejemplo, citas en línea, violencia, etc.).

8. Control de aplicación e inventario:

1. Capacidad para descubrir aplicaciones y procesos en ejecución y organizarlos en grupos.
2. Organice y busque aplicaciones y procesos por nombre, versión, editor / autor, etc.
3. Permitir o negar que un proceso comience.
4. Autorizar una aplicación basada en un hash.
5. Autorizar una solicitud basada en un certificado.
6. Capacidad para aplicar reglas a procesos secundarios generados, subprocesos.
7. El módulo puede ejecutarse en modo de prueba e informar la aplicación, pero no el bloque.
8. El módulo puede ejecutarse en modo de producción y puede bloquear todas las aplicaciones desconocidas.
9. Excluir automáticamente los procesos del sistema operativo de Microsoft.

9. Control de dispositivos:

1. Prevenga las fugas de datos confidenciales y las infecciones de malware a través de dispositivos conectados.
2. Aplique reglas de bloqueo y exclusiones a través de políticas a una amplia gama de dispositivos y tipos.

3. Enviará información como el nombre del dispositivo, ID de clase, fecha y hora de conexión.
4. Tenga tipos predefinidos de dispositivos como: CDROM, dispositivos de imagen, unidades de cinta, puertos COM / LPT, incursión SCSI, impresoras, NIC, almacenamiento interno y externo, etc.
5. Admite diferentes configuraciones y privilegios como Permitido, Bloqueado o Personalizado
6. Admite el modo de solo lectura para dispositivos de almacenamiento.
7. Capacidad para bloquear solo el USB y permitir que se utilicen todos los demás puertos.
8. Permitir la configuración de exclusiones para diferentes tipos de dispositivos.
9. Soporte para definir exclusiones de dispositivos:
    a. Por ID de producto
    b. Por ID de dispositivo, ID de hardware
10. Habilidad para descubrir dispositivos.

10. Análisis automático de Sandbox de archivos sospechosos:

1. La solución debe tener la capacidad de realizar un análisis en profundidad de los archivos sospechosos.
2. La solución debe tener la capacidad de enviar archivos de forma automática o manual a los servidores de sandbox.
3. La solución puede configurarse para permitir que los usuarios accedan a los objetos enviados o bloquearlos hasta que se devuelva el análisis.
4. La solución debe permitir diferentes acciones de remediación si un archivo enviado es una amenaza.
5. La solución debe tener la capacidad de usar un servidor proxy para el tráfico de la zona de pruebas.
6. La solución debe tener la capacidad de detonar archivos individualmente o en grupo.
7. La solución ofrece un informe detallado sobre los archivos enviados.

11. Actualizar:

1. Posibilidad de esperar a que se reinicie la computadora después de la actualización, sin notificar al usuario.
2. Sistema de actualización en cascada utilizando un servidor de actualización local (Relay).
3. Actualice los clientes en una ubicación remota a través de un cliente existente con la función de servidor de actualización integrada.
4. La función del servidor de actualización del cliente debe estar disponible para los sistemas operativos Windows y Linux.

12. Gestión de parches:

1. Habilidad para funcionar en modo automático
    a. Evaluación del horario para el parche perdido
    b. Programar la instalación automática separada según la categoría de parches (seguridad / no seguridad)
    c. Posibilidad de posponer el reinicio, si la instalación del parche lo solicita.
2. La solución debe permitir el modo manual: descubrimiento e instalación de parches bajo demanda
3. La solución debe ofrecer la posibilidad de ver todos los parches que faltan en el entorno. Esta información debe ser agregada en un inventario de parches.
    a. La solución ofrecerá visibilidad de los puntos finales que tienen instalados o les falta un parche específico.
    b. La solución ofrecerá información y razones si un parche no se instala.
    c. La solución le dará al usuario la capacidad de instalar rápidamente parches faltantes
    d. El usuario debe poder incluir en la lista negra uno o más parches.

4. La solución ofrecerá informes de los parches faltantes desde la perspectiva del punto final (parches instalados / faltantes en cada punto extremo)
5. La solución enviará notificaciones periódicamente, si faltan parches en los puntos finales del entorno.
6. La solución proporcionará la posibilidad de almacenamiento en caché, de esta manera los parches se descargarán de Internet solo por algunos puntos finales asignados.

13. Módulo de Analizador de Riesgos:

1. Habilidad para identificar y remediar una gran cantidad de riesgos de red y sistema operativos a nivel de endpoint (estaciones de trabajo y servidores). El modulo debe:

   a. Tener Dashboard o tablero de control con información accesible y de manera concreta sobre los indicadores de riesgos globales de la entidad
   b. Validar la puntuación de riesgo de acuerdo a la ponderación de los riegos evidenciados en la entidad.
   c. Proporciona una descripción general de la seguridad de su red y la información de evaluación de riesgos
   d. Enviar tareas de escaneo basadas en indicadores de riesgo en toda su red
   e. Identificar los puntos finales con configuraciones incorrectas.
   f. Posibilidad de realizar acciones para corregir las configuraciones incorrectas de manera asistida por la solución.
   g. Posibilidad En caso de no poderlas corregir las configuraciones incorrectas, muestra las rutas o acciones que se debe realizar para corregir las configuraciones incorrectas.
   h. Identificar los puntos finales con aplicaciones vulnerables
   i. Muestra de manera concreta como corregir los riesgos basados en vulnerabilidades y que tipo de vulnerabilidades afectan el equipo de escritorio o servidor.
   j. Identificar los riesgos ocasionados por factor humano.
   k. Evidenciar la evolución semanal del número de dispositivos afectados detectados como vulnerables tras los análisis de riesgo.
   l. Evidenciar los 15 resultados principales de los indicadores que activaron una alerta de riesgo después de escanear los dispositivos, ordenados por la cantidad de dispositivos afectados para configuraciones erróneas y vulnerabilidad de aplicaciones.
   m. Evidencia los 15 resultados principales de riesgos potenciales causados por el comportamiento no intencional o imprudente de los usuarios activos en su red, ordenados por la cantidad de usuarios vulnerables.
   n. Evidencia la gravedad de los riesgos que amenazan a los servidores y estaciones de trabajo de la entidad.
   o. Evidencia los servidores y estaciones de trabajo más vulnerables de su entorno, según la puntuación general calculada después de escanear en busca de configuraciones erróneas y vulnerabilidades.
   p. Evidenciar los usuarios más vulnerables de su entorno, según la puntuación global calculada tras analizar su comportamiento y actividad.

14. Protección de Servidor Exchange On-premise:

1. La solución debe proporcionar filtrado antimalware para el tráfico de correo electrónico entrante, interno y saliente.
2. La solución debe ser compatible con las capacidades de análisis bajo demanda y programadas para buzones y carpetas públicas, incluida la posibilidad de excluir buzones específicos o carpetas públicas, así como opciones para analizar solo los correos electrónicos con adjuntos o correos electrónicos recibidos en las últimas horas / días.

| | | |
|---|---|---|
| | 3. Posibilidad de configurar diferentes acciones a tomar en archivos infectados, sospechosos o que no se pueden analizar.<br>4. Capacidad para excluir aplicaciones potencialmente no deseadas (PUA) del filtrado de antimalware.<br>5. Capacidad de escanear en busca de malware dentro de los archivos.<br>6. La solución debe proporcionar un filtro antispam para el tráfico de correo electrónico, con la posibilidad de incluir en la lista blanca direcciones de correo electrónico y dominios específicos.<br>7. Capacidad para consultar los servidores de listas de Blackhole en tiempo real (RBL) definidos por los administradores y filtrar los mensajes de correo electrónico como spam según la reputación del servidor del remitente.<br>8. Posibilidad de marcar automáticamente como mensajes de correo electrónico no deseado escritos en Asia o Cirílico.<br>9. Capacidad para realizar consultas basadas en la nube para mejorar la protección contra el nuevo correo no deseado.<br>10. Capacidad para realizar diversas acciones en correos electrónicos no deseados detectados, incluido el prefijo del asunto del correo electrónico con una etiqueta específica, eliminar, poner en cuarentena o redirigir el correo electrónico a un buzón específico.<br>11. La solución debe proporcionar capacidades de filtrado de contenido para el tráfico de correo electrónico entrante, interno y saliente, basado en texto específico o expresiones regulares que coincidan con el asunto del correo electrónico y / o el contenido del cuerpo.<br>12. Capacidad para realizar diversas acciones en los correos electrónicos que coincidan con las reglas de filtrado de contenido, incluido el prefijo del asunto del correo electrónico con una etiqueta específica, eliminar, poner en cuarentena o redirigir el correo electrónico a un buzón específico.<br>13. La solución debe proporcionar capacidades de filtrado de archivos adjuntos para el tráfico de correo electrónico entrante, interno y saliente, según el tipo de archivo adjunto o nombre de archivo.<br>14. Capacidad para realizar diversas acciones en los correos electrónicos que coinciden con las reglas de filtrado de archivos adjuntos, incluida la eliminación o el reemplazo del archivo adjunto, el prefijo del asunto del correo electrónico con una etiqueta específica, la eliminación, la puesta en cuarentena o la redirección del correo electrónico a un buzón específico.<br>15. Capacidad para bloquear conexiones SMTP según la dirección de correo electrónico o el dominio del remitente.<br>16. Capacidad para definir direcciones IP autorizadas para enviar correos electrónicos para dominios propios para chequeos antispoofing.<br>17. Capacidad para definir reglas de filtrado personalizadas basadas en grupos de usuarios.<br>18. Capacidad para ver estadísticas e informes sobre la actividad de filtrado de correo electrónico.<br>19. Capacidad para ver y administrar de manera centralizada los elementos en cuarentena, incluida la capacidad para descargar o restaurar elementos en cuarentena.<br><br>15. Threats Xplorer:<br><br>1. Ofrece una visibilidad sobre las amenazas detectadas en la red. La función centraliza los eventos de detección y los clasifica por categoría, tipo de amenaza, acciones correctivas y muchos otros:<br><br>Identifica y analizar fácilmente cualquier evento de la entidad durante un intervalo de tiempo específico utilizando los filtros disponibles<br><br>a. Centraliza los eventos de detección de los siguientes módulos: antimalware, protección de almacenamiento, Exchange Protection, control de dispositivos, firewall. | |

| | | |
|---|---|---|
| | b. Threats Xplorer proporciona una amplia variedad de columnas y filtros para ayudar a navegar por la lista de eventos. Se puede seleccionar filtros en el menú desplegable o escribir palabras clave que coincidan con los resultados deseados.<br><br>**16.** MODULO DE INCIDENTES:<br><br>1. Solución debe ofrecer un modulo que ayuda a filtrar, investigar y tomar medidas sobre todos los eventos de seguridad detectados por Incidents Sensor durante un intervalo de tiempo específico, el modulo debe ofrecer las siguientes caracteristicas:<br><br>a. Incidentes : ver e investigar incidentes.<br>b. Lista de bloqueo : gestionar archivos bloqueados por incidentes.<br>c. Buscar : consultar la base de datos de eventos de seguridad.<br>d. Reglas personalizadas : crear reglas personalizadas para exclusiones o detecciones.<br>e. El módulo de incidentes debe proporcionar una cuadrícula altamente personalizable que muestre una lista de incidentes de EDR/XDR generados para la organización en los últimos 90 días.<br>f. Debe contar con un botón de alternancia del panel SMART VIEW . Esta función le permite personalizar, guardar y cambiar entre diferentes configuraciones de la página de Incidentes.<br>g. La grilla de incidentes muestra todos los incidentes que no tengan más de 90 días y que se ajusten al filtro aplicado actualmente<br><br>h. Identifica y analizar fácilmente cualquier evento de la entidad durante un intervalo de tiempo específico utilizando los filtros disponibles.<br>i. Centraliza los eventos de detección de los siguientes módulos: antimalware, protección de almacenamiento, Exchange Protection, control de dispositivos, firewall.<br>j. Threats Xplorer proporciona una amplia variedad de columnas y filtros para ayudar a navegar por la lista de eventos. Se puede seleccionar filtros en el menú desplegable o escribir palabras clave que coincidan con los resultados deseados.<br>k. Debe contar con un menú Ver que permite múltiples acciones para trabajar con la vista: guardar, guardar como, descartar cambios, agregar a favoritos, mostrar u ocutar filtros, abrir configuración.<br>l. Debe contar con un menú de Filtros: esta opción debe permitir personalizar los incidentes que se presentan en la grilla con los siguientes filtros: IDENTIFICACION, creado en, ultima actualización, estado, cesido de, prioridad, puntuación de gravedad, incidentes correlacionados, recursos, ultima fase de cadena de muerte, tipo de incidente, parámetros.<br>m. Acciones de incidente . El botón proporciona las siguientes opciones: ver eventos y alertas<br>n. Boton cambiar estado: la solución debe permitir cambiar el estado del incidente: abierto, investigando, falso positivo y cerrado.<br>**16.** MODULO DE EDR:<br><br>1. La solución debe contar con Endpoint Detección y Respuesta ( EDR ) correlación de eventos, capaz de identificar amenazas avanzadas o ataques en progreso.<br><br>a. Sensor de incidentes debe monitorear continuamente la actividad de los terminales<br>b. Sensor de incidentes debe monitorear procesos en ejecución<br>c. Sensor de incidentes debe monitorear cambios en el registro.<br>d. Sensor de incidentes debe monitorear comportamiento de usuarios<br>e. Sensor de incidentes debe recopilar, informar y procesar los datos | |

mediante algoritmos de machine learning y tomar acciones automáticas de las actividades sospechosas detectadas.

f. El sensor de EDR debe entregar las incidencias o comportamientos sospechosos y presentarlas en el panel de Incidentes.

g. El sensor debe ser desplegable desde la administración de los puntos finales.

**B. PROTECCIÓN PARA ESTACIONES DE TRABAJO Y SERVIDORES VIRTUALIZADOS**

**1.** Protección antimalware dedicada a entornos virtualizados: requisitos mínimos:

1. El producto se integra con VMware VShield o VMware NSX y ofrece la posibilidad de escaneo antimalware sin instalar un agente de escaneo en la máquina virtual.
2. El componente de administración central de la solución se integra con varios vCenters de VMware.
3. Para todos los sistemas que ejecutan Windows y Linux, el producto incluye:
   a. Proceso de escaneo;
   b. Escaneo de memoria;
   c. Escaneo en tiempo real de archivos;
   d. Escanear archivos bajo demanda;
4. Exploración en tiempo real y bajo demanda para máquinas virtuales Linux.
5. Introspección de Linux a través de VMware NSX.
6. El producto se integra con varios servidores Citrix Xen (los inventarios se importan en el producto).
7. El producto también es compatible con Microsoft Hyper-V, Red Hat Virtualization, Oracle VM y KVM.
8. El producto debe incluir una única máquina de escaneo virtual que:
   a. Contiene las firmas antimalware;
   b. Proporciona una protección completa, actualizada, al abrir una máquina virtual;
   c. Proporciona escaneo optimizado.
9. El producto de software que se instala en las máquinas virtuales, para facilitar la transmisión de la información que se va a escanear, debe ocupar unos 10 MB de RAM.

**2.** Características generales:

1. Métodos para la detección de virus, spyware, rootkits y otros programas maliciosos.
2. El producto debe permitir la actualización automática del dispositivo virtual de seguridad, para firmas de antimalware y para el sistema operativo del dispositivo virtual de seguridad.
3. El producto debe informar el estado actual del host de seguridad: VMs protegidos / desprotegidos y dispositivos virtuales de seguridad.

**3.** Requisitos mínimos del sistema:

**A. Plataformas de virtualización:**

- VMware vSphere,6.5,6.0, 5.5, 5.1, 5.0 P1 (Patch # 474610-1) or 4.1 P3 (433,742-Patch # 3)

incluyendo ESXi 4.1 and ESXi 5.0 con:

- VMware vCenter Server 6.5,6.0, 5.5, 5.1, 5.0 or 4.1
- VMware VShield Manager 5.5, 5.1, 5.0
- VMware VShield VShield Endpoint Manager instalado en el equipo

- VMware Tools 8.6.0 build 446312 o reciente
- VMware NSX 6.2.4(6.3 para Linux support) o reciente

- VMware View 5.1, 5.0 o reciente
- Citrix XenDesktop 5.5, 5.0 o reciente
- XenServer 7.2, 7.1, 7.0, 6.0, 5.6 or 5.5 (incluyendo Xen Hypervisor)
- Citrix XenApp
- Microsoft Hyper-V Server 2012, Microsoft Hyper-V Server 2008 R2 or Windows 2008 R2 (incluyendo Hyper-V Hypervisor)
- Oracle VM 3.0
- Red Hat Enterprise Virtualization 4.1, 4.0, 3.0 (incluyendo KVM hypervisor)

**B.** Sistemas Operativos para Máquinas Virtuales (32/64 bit):

- Windows 10, 8.1, 8, Windows 7, Windows Vista, Windows XP (SP3)
- Windows Server 2016, Windows Server 2012, Windows Server 2012 R2 Windows Server 2008, Windows Server 2008 R2
- Windows Server 2003, Windows Server 2003 R2
- Oracle Solaris 11, 10
- Distribuciones Linux:
  - Red Hat Enterprise Linux 5.6 o reciente
  - CentOS 5.6 o reciente
  - Ubuntu 12.04 o reciente
  - SUSE Linux Enterprise Server 11 o reciente
  - OpenSUSE 12, 11
  - Fedora 16, 15
  - Debian 7.0 o reciente

**4.** Las principales características y funcionalidades del módulo antimalware:

1. Exploración automática de archivos que se copian en soporte externo y de LAN o WAN.
2. La exploración automática en tiempo real de los archivos se puede configurar para analizar solo tipos de archivos específicos, con extensiones específicas, definidas por el administrador.
3. La exploración automática en tiempo real de los archivos se puede configurar para que no analice archivos con un tamaño superior a «x» Kb, el administrador de la solución puede definir los tamaños de los archivos.
4. El escaneo bajo demanda incluirá las siguientes opciones:
   a. Escanee cualquier medio de almacenamiento conectado a la máquina virtual;
   b. Escaneo de correos electrónicos;
5. Configuración de las rutas a escanear, a nivel de archivo;
6. Debe permitir que el administrador defina ciertas carpetas, discos, archivos y extensiones que se excluirán del análisis en tiempo real y el análisis bajo demanda.
7. Para no sobrecargar los recursos del sistema, el producto antimalware debe contener un solo motor de análisis.
8. Para permitir la optimización de la cantidad de tráfico enviado a la red a través de un mecanismo de almacenamiento en caché en la máquina de escaneo y la máquina virtual.
9. Agente de conmutación por error / conexiones de equilibrio de carga a la máquina de escaneo.
10. Las políticas pueden aplicarse a un grupo de recursos de VMware vCenter.

**5.** Cuarentena:

1. El producto antimalware debe permitir la eliminación automática de archivos en cuarentena más antiguos que un período determinado, sin ocupar espacio

de almacenamiento innecesario.
2. La capacidad de mover un archivo de la cuarentena a su ubicación original.
3. Cuarentena centralizada. La capacidad de recopilar de forma segura todos los archivos en cuarentena desde puntos finales protegidos a una ubicación única en la red para una investigación más profunda.
4. Capacidad para descargar el archivo directamente a la estación de trabajo del administrador (solo para la integración de VMware vShield o NSX).
5. Capacidad para volver a analizar los archivos en cuarentena después de cada actualización de la firma.
6. Posibilidad de envío automático de archivos de cuarentena a los laboratorios del fabricante en un intervalo de tiempo establecido por el administrador.

**7.** Gestión e instalación remota:

1. El dispositivo virtual de seguridad se puede personalizar antes de la instalación. Se escala automáticamente según varias características: número de máquinas virtuales en el host, redes, direcciones IP asignadas a recursos (CPU, memoria), etc.
2. La consola de administración informará el número de máquinas virtuales que han instalado o no la solución de protección antivirus y el estado de la máquina: activado o desactivado.
3. La posibilidad de que la consola de administración informe si el módulo antimalware está habilitado o no en la máquina virtual.

## C. SEGURIDAD PARA DISPOSITIVOS MOVILES

1. Requisitos mínimos del sistema:

- Apple iPhone y tabletas iPad (iOS 8.1+)
- Google Android smartphones y tabletas (2.2+)

2. Caracteristicas:

1. Permite asociar un dispositivo con un usuario de Active Directory.
2. La instalación se realiza enviando un correo electrónico al usuario, con los detalles de la instalación.
3. La activación del dispositivo a la consola de administración se realizará mediante un código QR.
4. Los paquetes de instalación se pueden descargar desde Apple App Store y Google Play.
5. Se pueden tomar las siguientes acciones:
    a. Imponer el bloqueo de pantalla y la autenticación;
    b. Restaurar a la configuración de fábrica;
    c. Localice el dispositivo;
    d. Escaneo de dispositivos (para el sistema operativo Android);
    e. Cifrado de memoria del dispositivo (para el sistema operativo Android).
6. La Consola de administración informará sobre los dispositivos que están activos, inactivos, desconectados o con jailbreak.

3. Configuraciones de seguridad:

1. Si un dispositivo no cumple con la configuración deseada, se pueden realizar las siguientes acciones:
    a. Ignorar;
    b. Bloquear el acceso;
    c. Dispositivo de bloqueo;
    d. Restaurar la configuración de fábrica;
    e. Elimine el dispositivo de la consola de administración.

2. Se pueden realizar dispositivos de bloqueo con una acción de contraseña. Esta contraseña se puede configurar para contener:
    a. Contraseña simple o compleja (específica para el sistema operativo);
    b. Números y caracteres;
    c. Longitud mínima definida por el administrador;
    d. Mínimo de caracteres especiales, definidos por el administrador;
    e. Período de caducidad de la contraseña. El período será definido por el administrador;
    f. Configuración de restricción de reutilización de contraseña;
    g. El número de intentos de entrada de contraseña incorrectos;
    h. Período de bloqueo del dispositivo después de una cantidad de minutos definidos por el administrador.
3. Se pueden generar varios perfiles, que establecerán reglas de seguridad para la conectividad Wi-Fi o VPN (solo para el sistema operativo iOS), pero también algunos relacionados con el acceso a ciertos sitios web.
4. Los perfiles de Wi-Fi contendrán las siguientes opciones:
    a. General: se definirá el SSID, así como el tipo de seguridad de la red;
    b. Configuración de TCP / IP - para los protocolos IPv4 e IPv6;
    c. Configuración de proxy - deshabilitada, automática o configurada manualmente.
5. Los perfiles relacionados con el acceso a sitios web (sistema operativo Android) incluyen características como:
    a. Permitir, bloquear o programar para días y franjas horarias específicos el acceso a ciertos sitios web;
    b. Creación de excepciones para bloquear o permitir el acceso a sitios web específicos.
6. Los perfiles con respecto al acceso a sitios web (sistema operativo iOS) incluyen opciones para habilitar o deshabilitar:
    a. Uso del navegador Safari;
    b. Opciones de autocompletar;
    c. Alertar a los usuarios al acceder a sitios web maliciosos;
    d. JavaScript;
    e. Pop-ups;
    f. Cookies.

## D. INTROSPECCIÓN DE MEMORIA CON HYPERVISORES

Requerimientos mínimos

- CPU microarchitecture: – cualquier Intel® Sandy Bridge processor o reciente, con soporte para Intel® Virtualization Technology. – VT-x or VT-d las extensions deben estar activadas en la BIOS.
- Citrix XenServer 7 Enterprise Edition o reciente.
- Las máquinas deben ejecutar un sistema operativo compatible:
    - ● Windows Desktop Operating Systems – Windows 10 – Windows 8.1 – Windows 8 – Windows 7 ● Windows Server Operating Systems – Windows Server 2016 – Windows Server 2012 / Windows Server 2012 R2 – Windows Server 2008 / Windows Server 2008 R2
    - Linux Operating Systems – Debian 9, 64-bit – Debian 8, 64-bit – Ubuntu 16.04 LTS, 64-bit – Ubuntu 14.04 LTS, 64-bit – CentOS 7, 64-bit – Red Hat Enterprise Linux 7, 64-bit – SUSE Linux Enterprise Server 12, 64-bit – Oracle Linux 7.3, 64-bit

Caracteristicas:

1. La solución se integra con la tecnología de hipervisor para proporcionar protección sin agente para las máquinas virtuales invitadas (no hay agente y / o controlador instalado dentro de la

| | | |
|---|---|---|
| | máquina virtual hosteada)<br>2. La solución protege la memoria de los sistemas operativos Windows y Linux.<br>3. La solución controla el modo de usuario del sistema operativo y la memoria del modo kernel<br>4. La solución supervisa y protege los siguientes componentes del espacio del kernel<br>a. Registros de control<br>b. Registros específicos del modelo<br>c. IDT / GDT integridad<br>d. Drivers cargados<br>5. La solución ofrece detalles forenses adicionales, informados en la consola de administración<br>a. Eventos fallos del sistema operativo<br>b. Eventos del conductor<br>c. Eventos de bloqueo de aplicación<br>6. La solución ofrece mecanismos de introspección de hipervisores para acceder a la memoria de la máquina virtual sin procesar y detecta violaciones de memoria provocadas por técnicas de ataque como el desbordamiento de búfer, el desbordamiento de búfer o la inyección de código.<br>7. La solución ofrece alertas, notificaciones e informes de eventos disponibles en una consola de administración centralizada.<br>8. Sobre la base de la detección de violación de memoria, la solución es capaz de inyectar una herramienta de remediación en la máquina virtual en ejecución para recopilar detalles forenses adicionales y realizar un análisis completo del sistema antimalware; La herramienta de remediación tiene la capacidad de eliminarse una vez que se realiza la remediación.<br>9. La solución permite a los administradores de TI o los equipos de seguridad inyectar herramientas de terceros en máquinas virtuales sin ninguna interacción del usuario o conexión de red.<br>10. Las herramientas de terceros deben tener la opción de ser inyectadas manualmente, automáticamente o programadas. | |
| 2 | **CAPACITACIÓN DE SOFTWARE DE ANTIVIRUS** | |

Se requiere que el contratista realice capacitación del antivirus a suministrar (tanto para las 800 licencias de sistema operativo Windows.

La capacitación se debe realizar en las oficinas de la Dirección TIC de la gobernación, y será dirigida al personal técnico de sistemas.

La capacitación debe abarcar las siguientes temáticas:

- Introducción al antivirus a suministrar
- Mecanismo de instalación, configuración y parametrización segura de antivirus
- Identificación de ataques y vulnerabilidades
- Administración de ambientes
- Protección contra amenazas basada en Aprendizaje automático (Machine Learning – ML)
- Protección de datos
- Capacidad de instalar la solución de seguridad en smartphones y tablets Android, IOS
- Creación de perfiles
- Configuración de seguridad y protección para correos electrónicos
- Capacidad Control de funciones y Control web
- Activación de Cloud
- Políticas y configuraciones

1

**SOPORTE Y ASISTENCIA TÉCNICA DE SOFTWARE DE ANTIVIRUS POR UN (1) AÑO**

Se requiere que el contratista ofrezca el servicio de soporte y asistencia técnica del software antivirus a suministrar.

El servicio de soporte y asistencia técnica debe contar con las siguientes características:

- Jornadas de asistencia técnica de revisión preventiva cada tres (3) meses.
- Soporte técnico por problemas técnicos.
- Habilitación de Help Desk sobre las demandas más comunes de los usuarios, el cual debe contener un centro de ayuda (documento) donde los usuarios encuentran asistencia sobre las funcionalidades y módulos del antivirus a suministrar.
- Posibilidad de ofrecer el servicio de soporte y asistencia técnica habilitado con múltiples canales.
- Atención las expectativas del personal de la dirección TIC con respecto a la experiencia.

3 — 1 año

Tiempo validez de soporte y asistencia técnica (12 meses).

**2.3. EXPERIENCIA DEL PERSONAL TECNICO:**

Debido a los requerimientos técnicos descritos anteriormente se requiere personal altamente calificado que pertenezca al equipo de trabajo del oferente.

Con el objeto de seleccionar un proveedor que garantice estabilidad de los servicios a RENOVACIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS BITDEFENDER, CON ACTUALIZACION, SOPORTE, CAPACITACION Y ASISTENCIA TECNICA POR EL TERMINO DE UN AÑO, PARA LAS ESTACIONES DE TRABAJO Y SERVIDORES DE LA PLATAFORMA TECNOLOGICA DE LA GOBERNACION DE BOLIVAR, los cuales son de misión crítica para el funcionamiento de la entidad, es necesario que el proponente cuente con personal altamente calificado, capacitado y experimentado, para lo cual se requiere, adjuntar las hojas de vida y certificados

Para garantizar la correcta ejecución del contrato, La Gobernación de Bolívar, se requiere que el oferente presente dentro de su equipo de trabajo, un Ingeniero Gerente de Proyectos de TI, con el objeto de servir de enlace entre el supervisor del contrato por parte de La Gobernación de Bolívar y la empresa oferente; realizando entrega de los documentos solicitados en el presente proceso al igual que los informes mensuales de funcionamiento general del antivirus a contratar.

El oferente debe contar con certificado que permita garantizar que cuenta con personal de Bitdefender Certified Technical Specialist.

**Descripción del Personal requerido:**
• **Gerente de proyecto:** ingeniero de sistemas, electrónico, industrial o afín, con estudios en antivirus y cloud computing, especialista en seguridad informática, con 10 años de experiencia en administración y configuración de antivirus, debe contar con certificación BITDEFENDER CERTIFIED TECHNICAL SPECIALIST, con certificación especializada en Cyber Security Foundation, con estudios como auditor en la norma internacional ISO 27001, con estudios en Ethical Hacking, experiencia en administración de servidor y soporte remoto**.**

**2.4. EXPERIENCIA TECNICA:**
**D**ebido a los requerimientos técnicos descritos anteriormente se requiere que el oferente sea altamente calificado. La Gobernación de Bolívar, para garantizar la correcta ejecución del contrato, requiere que el oferente presente certificado que conste que el oferente es categoría GOLD RESELLER STATUS del antivirus Bitdefender.

**2.5 ALCANCE DEL OBJETO:**

**El contratista para cumplir con la ejecución del contrato debe:**

- Efectuar la entrega del servicio contratado de acuerdo con las especificaciones técnicas requeridas y en los tiempos exigidos por la Gobernación de Bolívar.
- Atender las observaciones y requerimientos de la supervisión del contrato.
- Responder por la calidad de los servicios suministrados.
- Responder por el perfecto funcionamiento del servicio de suministro.

**3. OBLIGACIONES DE LAS PARTES**
**3.1 OBLIGACIONES GENERALES DEL CONTRATISTA**
El contratista en desarrollo del objeto contractual se obliga a lo siguiente:

a. Acatar la Constitución, la Ley, las normas legales y procedimientos establecidos por el gobierno nacional y demás disposiciones pertinentes.
b. Cumplir con lo previsto en las disposiciones de las especificaciones esenciales, así como la propuesta presentada.
c. Dar cumplimiento a las obligaciones con los sistemas de seguridad social, salud, pensiones y aportes parafiscales cuando haya lugar, y presentar los documentos respectivos que así lo acrediten, conforme lo establecido por el artículo 50 de la Ley 789 de 2002, la Ley 828 de

2003, la Ley 1122 de 2007, Decreto 1703 de 2002, Decreto 510 de 2003, artículo 3 de la Ley 1150 de 2007, Ley 1562 de 2012 y demás normas que las adicionen, complementen, modifiquen o aclaren.

d. Constituir las garantías requeridas en la invitación en los tiempos estipulados para ello.
e. Acatar las órdenes que durante el desarrollo del contrato le imparta el Supervisor del Contrato, y de manera general obrar con lealtad y buena fe en las distintas etapas contractuales evitando dilaciones y entrabamientos que pudieran presentarse.
f. No encontrarse incurso en ninguna de las causales de inhabilidad e incompatibilidad establecidas en la Ley para contratar con el Estado y con el Departamento de Bolívar.
g. Reportar de manera inmediata cualquier novedad o anomalía al supervisor del contrato.
h. Suscribir las actas a que haya lugar.
i. Las demás que se deriven de la naturaleza del contrato y que garanticen su cabal y oportuna ejecución.

**3.2. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA:**

El futuro contratista tendrá las siguientes obligaciones específicas:

- Entregar bienes y/o servicios que se encuentran relacionados en el estudio previo de acuerdo a las características exigidas y ofertadas.
- Garantizar que los elementos entregados cumplan con los estándares de cantidad y calidad dados para cada producto.
- Brindar garantía y soporte de 1 año.
- Cumplir con el objeto contratado.
- Asumir los costos de transporte y medios para cumplir con la entrega.
- Presentar junto con la factura o cuenta de cobro los soportes exigidos.
- Mantener fijo el precio ofrecido en la propuesta durante la ejecución del contrato.
- Reportar de manera inmediata cualquier novedad o anomalía al supervisor del contrato.
- Cuando el supervisor del contrato lo solicite, en cualquier tiempo y durante la ejecución del contrato, allegar las certificaciones expedidas por el revisor fiscal o representante legal, según el caso, de acuerdo con lo ordenado en el artículo 50 de la Ley 789 de 2002 y demás normas concordantes. además, se debe aportar del revisor fiscal la copia de la cedula y tarjeta profesional.
- Presentar dentro de la propuesta del oferente las acciones a realizar para cumplir con los Requisitos de Calidad descritos en el numeral 3.1 DESCRIPCIÓN TÉCNICA DEL SERVICIO, del presente proceso de selección.
- Certificado soporte y apoyo técnico.

**3.3 OBLIGACIONES DEL DEPARTAMENTO:**

1. Adelantar los trámites y cumplir con los requisitos para la ejecución del contrato.
2. Realizar la Supervisión del contrato.
3. Realizar los pagos con el que se obliga en calidad de contratante.
4. Suscribir la correspondiente acta de liquidación a la terminación del contrato de conformidad con las normas vigentes.
5. Las demás relacionadas con el objeto y naturaleza del presente contrato y garantice el cabal y oportuno cumplimiento del contrato, de acuerdo con las normas vigentes y concordantes**.**

## 4. ACREDITACIÓN DEL PAGO AL SISTEMA DE SEGURIDAD SOCIAL DURANTE LA EJECUCIÓN DEL CONTRATO

El contratista debe acreditar, para realizar cada pago derivado del contrato, que se encuentra al día en el pago de aportes parafiscales relativos al Sistema de Seguridad Social Integral, así como los propios del SENA, ICBF y Cajas de Compensación Familiar, cuando corresponda.

## 5. PLAZO PARA EJECUTAR EL CONTRATO

El plazo oficial de ejecución será hasta el 31 de diciembre de 2023 o hasta agotarse el presupuesto destinado para esta contratación, contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución, término durante el cual el contratista seleccionado deberá cumplir con el objeto contratado y el cual no podrá sobrepasar el 31 de diciembre de 2023. Este plazo se empezará a contabilizar una vez se expida el correspondiente registro presupuestal, y se aprueben las garantías exigidas

## 6. FORMA DE PAGO

LA GOBERNACIÓN DE BOLÍVAR reconocerá a EL CONTRATISTA en contraprestación al cumplimiento del objeto derivado del contrato la suma que resultare de la propuesta presentada la cual será máximo de **NOVENTA Y CINCO MILLONES DE PESOS M/CTE LEGAL COLOMBIANA ($95.000.000) Incluido IVA**, y demás tasas, contribuciones e impuestos a que haya lugar para la legalización y ejecución del contrato.

**DE LA FORMA DE PAGO**: EL DEPARTAMENTO DE BOLÍVAR cancelará al contratista el valor del objeto contratado en un único pago, previa presentación de certificado de entrega a satisfacción, del objeto contratado y entregado.

Para tal efecto EL CONTRATISTA deberá acompañar la respectiva facturación, el acta de entrega a satisfacción suscrita por el supervisor del contrato, certificado de paz y salvo del cumplimiento de las obligaciones parafiscales (salud, riesgos profesionales, pensiones, aportes a las cajas de compensación familiar, ICBF y SENA), para lo cual debe tenerse en cuenta lo señalado en el artículo 50 de la ley 789 de 2002 y artículo 23 de la ley 1150 de 2007 de acuerdo a lo requerido en el contrato.

**MARCO TRIBUTARIO DEPARTAMENTAL APLICABLE:** todos los impuestos, tasas y contribuciones que hayan de causarse y pagarse para la ejecución del presente contrato corren por cuenta del adjudicatario y no habrá lugar a reclamar ningún pago adicional a los precios pactados. La entidad aplicará las retenciones en la fuente a que haya lugar dependiendo del objeto del contrato y la calidad del contribuyente.

El Contratista debe indicar el número de cuenta activa y el nombre del titular de la misma en donde LA GOBERNACIÓN DE BOLÍVAR consignará los respectivos pagos, asimismo indicar en la facturación que presente, el régimen tributario que lo regula.

En la propuesta económica el oferente debe discriminar con exactitud el precio correspondiente a los bienes y servicios objeto de la oferta y el valor del impuesto sobre las ventas que afecte la misma. En caso de que el oferente no discrimine el impuesto a las ventas y el valor de los servicios ofrecidos causen dicho impuesto el Departamento de Bolívar lo considerara incluido en el valor de la oferta, cuando el producto o bien no esté excluido.

Todos los pagos estarán sujetos al Programa Anual Mensualizado de Caja - PAC y al cumplimiento de los procedimientos presupuestales. El pago lo realizará la tesorería, con abono en cuenta al Contratista adjudicado, previo cumplimiento de los requisitos descritos anteriormente.

LA GOBERNACIÓN DE BOLÍVAR no se responsabilizará por la demora en el pago al CONTRATISTA,

cuando ella fuere provocada por encontrarse incompleta la documentación que sirva de soporte para el trámite de las facturas y no se ajuste a cualquiera de las condiciones establecidas en el presente contrato.

**El CONTRATISTA** indicará en la facturación que régimen tributario lo regula y deberá realizar el pago de los impuestos departamentales, para la presentación de la cuenta de cobro del pago del contrato. A manera informativa se señala que dentro de los impuestos a pagar se encuentran:

**ESTAMPILLA PRODESARROLLO**: 2% sobre el valor del contrato.
**ESTAMPILLA PROCULTURA**: 2% sobre el valor del contrato.
**ESTAMPILLA UNIVERSIDAD DE CARTAGENA**: 1% sobre el valor del contrato. **ESTAMPILLA CONTRIBUCIÓN**: 1% sobre el valor del contrato.
**ESTAMPILLA PROANCIANATO**: 3% sobre el valor del contrato.

Se aclara que es responsabilidad de cada interesado en participar, verificar los anteriores impuestos, y la existencia de otros, en la Secretaría de Hacienda de la entidad, con el propósito de tenerlo en cuenta dentro de su propuesta económica.

- **OTROS MARCO TRIBUTARIO NACIONAL APLICABLES**
  **IVA:** En la propuesta económica el oferente debe discriminar con exactitud el precio correspondiente a los bienes y servicios objeto de la oferta y el valor del impuesto sobre las ventas que afecte la misma. En caso de que el oferente no discrimine el Impuesto a las ventas, y el valor de los bienes ofrecidos causen dicho impuesto **LA GOBERNACIÓN DEL DEPARTAMENTO DE BOLIVAR** lo considerará incluido en el valor de la oferta, **CUANDO EL PRODUCTO O BIEN NO ESTE EXCLUIDO.**

  **RETENCIÓN EN LA FUENTE:** Se practicarán las retenciones a este contrato, en las tasas señaladas por las tablas oficiales de la ley que la reglamenta.

## CAPÍTULO III ELABORACIÓN, PRESENTACIÓN Y EVALUACIÓN DE LAS OFERTAS

### 3.1. CARTA DE PRESENTACIÓN DE LA OFERTA

El proponente debe presentar el Formato 1 – Carta de Presentación de la Oferta, el cual debe ir firmado por la persona natural proponente o por el representante legal del proponente individual o plural o por el apoderado.

La carta de presentación de la oferta debe suscribirse por la persona correspondiente facultada legalmente para tal fin.

Con la firma de este documento se entiende que el proponente conoce y acepta los requisitos contenidos en el mismo.

El proponente debe diligenciar el formato obligatoriamente. Todos los espacios en blanco deben diligenciarse con la información solicitada

### 3.2. APODERADO

Los proponentes podrán presentar ofertas directamente o suscritas por intermedio deapoderado, evento en el cual deben anexar el poder, otorgado en legal forma (artículo 5 delDecreto – Ley 019 de 2012), en el que se confiera al apoderado de manera clara y expresa facultades amplias y suficientes para actuar, obligar y responsabilizar a quien(es) representa en el trámite del presente proceso y en la aceptación de la oferta. No obstante,la simple entrega física o radicación de la oferta en la entidad puede realizarla cualquier persona, sin necesidad de poder u autorización.

El apoderado que firma la oferta podrá ser una persona natural o jurídica, que en todo caso debe tener domicilio permanente, para efectos de este proceso, en la República de Colombia, y debe estar facultado para representar al proponente y/o a todos los integrantesdel proponente plural, a efectos de adelantar en su nombre de manera específica las siguientes actividades: (i) presentar oferta para el proceso de contratación de que trata estainvitación; (ii) responder los requerimientos y aclaraciones solicitados la entidad en el curso del presente proceso; (iii) recibir las notificaciones a que haya lugar dentro del proceso (iv) suscribir el acta de terminación y liquidación, si a ello hubiere lugar.

Las personas extranjeras que participen mediante un proponente plural podrán constituir unsolo apoderado común y, en tal caso, bastará para todos los efectos la presentación del poder común otorgado por todos los integrantes con los requisitos de autenticación, legalización o apostilla y traducción exigidos en el Código de Comercio, incluyendo los señalados en la invitación. El poder a que se refiere este párrafo podrá otorgarse en el mismo acto de constitución del proponente plural.

### 3.3. ELABORACIÓN Y PRESENTACIÓN DE LA OFERTA

Para los procesos en SECOP II, los documentos se adjuntarán de acuerdo con el orden requerido en el cuestionario por la entidad estatal, los cuales deben ser legibles y escaneados correctamente-La entidad solo recibirá una oferta por proponente, salvo los procesos estructurados por lotes o grupos. En caso de presentarse para varios procesos de contratación con la entidad, el proponente debe dejar constancia para qué proceso presenta su ofrecimiento. La presentación de la propuesta implica la aceptación y conocimiento de la legislación colombiana acerca de los temas objeto del presente proceso y de todas las condiciones y obligaciones contenidas en el mismo. Adicionalmente si se hace a través del SECOP II el proponente debe cumplir con el Manual de Usos y Condiciones de la plataforma.

El proponente asumirá todos los costos asociados a la elaboración y presentación de su oferta. La entidad en ningún caso será responsable de los mismos.

Toda tachadura y/o enmendadura que presente algún documento de la oferta debe estar salvado con la firma de quien suscribe el correspondiente documento al pie de la misma y nota al margen del documento donde manifieste clara y expresamente la corrección realizada.

Los proponentes adjuntarán el formulario de la propuesta económica con el valor discriminado de cada ítem en el SECOP II, junto con su propuesta, teniendo en cuenta el formulario de propuesta económica publicado por la entidad. Por tanto, la oferta económica no debe estar firmada.

### 3.4. CIERRE DEL PROCESO Y APERTURA DE OFERTAS

Se entienden recibidas por la entidad las ofertas que se encuentren en la plataforma del SECOP II a la fecha y hora indicada en el cronograma del proceso, después de este momento el SECOP II no permitirá recibir más propuestas por excederse del tiemposeñalado en el cronograma.

Vencido el término para presentar ofertas, la entidad estatal debe realizar su apertura y publicar la lista de oferentes. Luego de la apertura, las propuestas son públicas y cualquier persona puede consultarlas.

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

Sin embargo, cuando haya una indisponibilidad del SECOP II, la cual ha sido confirmada por Colombia Compra Eficiente mediante Certificado de Indisponibilidad, la entidad estatalpuede recibir ofertas en los términos y condiciones establecidos en el "Protocolo para actuarante una indisponibilidad del SECOP II" o en el documento que Colombia Compra Eficiente determine para ello. [Puede consultarlo en el siguiente enlace: https://www.colombiacompra.gov.co/secop-

ii/indisponibilidad-en-el-secop-ii].

### 3.5. INFORME DE EVALUACIÓN

La entidad evaluará la oferta de menor precio y verificará que cumpla las condiciones mínimas de la Invitación. Si no cumple solicitará al proponente, mínimo por el término de un (1) día hábil, que aclare, explique o aporte los documentos e información subsanable; encaso de que la entidad no fije un plazo específico, se entenderá que es de un (1) día hábil. No obstante, los proponentes no podrán completar, adicionar, modificar o mejorar la oferta económica, la cual solo puede ser objeto de aclaraciones y explicaciones. Los proponentes deben aportar las aclaraciones o documentos requeridos hasta el plazo indicado, so pena que la entidad rechace la propuesta y revise la segunda oferta que ofrezca el menor precioy verifique que cumple los requisitos de la invitación. Si la segunda propuesta tampoco cumple se repetirá el procedimiento anterior, continuando con las ofertas que ofrezcan el siguiente menor precio.

En caso de que la entidad advierta la ausencia de requisitos o la falta de documentos referentes a la futura contratación o al proponente, y no los haya requerido durante el proceso de evaluación, podrá requerir al proponente, otorgándole un término mínimo de un
(1) día hábil contado desde el momento en el que advirtió su omisión, con el fin de que los aporte; en caso de que la entidad no fije un plazo específico, se entenderá que es de un (1) día hábil.

Una vez se identifica la oferta de menor valor que cumple los requisitos mínimos de la Invitación, la entidad publicará el informe de evaluación en el cual constará la evaluación delas ofertas. Allí se indicará, entre otros aspectos, cuál oferente ofreció el menor precio y cumplió con los requisitos de la Invitación.

El informe de evaluación permanecerá publicado en el SECOP y a disposición de losinteresados por un término no inferior a un (1) día hábil, término hasta el cual losproponentes podrán hacer las observaciones que consideren procedentes. Al finalizar el término de traslado, la entidad contestará las observaciones, y en caso de que sea necesario modificar la evaluación, publicará un informe de evaluación ajustado.

En virtud del principio de buena fe, los proponentes que presenten observaciones al procesoo a las ofertas y conductas de los demás oferentes, deben argumentar y demostrar la procedencia y oportunidad de estas.

### 3.6. ACEPTACIÓN DE LA OFERTA

La entidad estatal aceptará la oferta de menor precio, siempre que cumpla con las condiciones establecidas en la invitación.

La comunicación de aceptación junto con la oferta constituye para todos los efectos el contrato celebrado, con base en lo cual se efectuará el respectivo registro presupuestal.

### 3.7. PROPUESTAS PARCIALES

No se admitirá la presentación de propuestas parciales, esto es, las presentadas para una parte del objeto o del alcance del contrato, a menos que se establezca esta posibilidad en lainvitación.

### 3.8. PROPUESTAS ALTERNATIVAS

Los proponentes pueden presentar alternativas técnicas y económicas siempre y cuando ellas no signifiquen condicionamientos para la aceptación de la oferta y cumplan con los siguientes requisitos:

A. Que el proponente presente una propuesta básica que se adecúe a las exigencias fijadas en la invitación, de forma que pueda ser evaluada la oferta inicial con base en las reglas de

selección objetiva allí contenidas.

B. Que la oferta alternativa, o las excepciones económicas, se enmarquen en el principio de selección objetiva, de tal manera que no se afecten los parámetros neutrales deescogencia del contratista y no se desconozca el principio de igualdad.

Cuando un proponente presente una alternativa deberá adjuntar toda la información necesaria para su análisis y una descripción detallada del proceso de construcción, características de los materiales y equipos y análisis de costos. Todas las expensas necesarias para desarrollar la alternativa, incluso los de transferencia tecnológica, deben incluirse en los respectivos ítems de la oferta. Solo serán consideradas las propuestas alternativas del proponente favorecido con aceptación de la oferta y la selección de la alternativa será potestad de la entidad.

Las propuestas alternativas se deben presentar en SECOP II como "otros anexos", el proponente en el documento debe hacer la claridad de su intención de presentar una propuesta alternativa.

### 3.9. REGLAS PARA LOS PROCESOS ESTRUCTURADOS POR LOTES O GRUPOS

N/A.

## CAPÍTULO IV REQUISITOS HABILITANTES Y SU VERIFICACIÓN

La entidad verificará los requisitos habilitantes dentro del término señalado en el cronograma de la invitación, de acuerdo con los soportes documentales que acompañan la propuesta presentada.

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

### 4.1 GENERALIDADES

**a)** Únicamente se consideran habilitados aquellos proponentes que cumplan todos los requisitos habilitantes, según lo señalado en la presente Invitación.

**b)** En el caso de proponentes plurales, los requisitos habilitantes serán acreditados por cada uno de los integrantes de la figura asociativa, salvo que se dé a entender algo distinto y, en todo caso, se realizará de acuerdo con las reglas de la invitación.

**c)** Cuando la entidad exija el requisito habilitante de capacidad financiera, los proponentes deben diligenciar el Formato 4 Capacidad Financiera con los soportes que ahí se definen.

### 4.2 CAPACIDAD JURÍDICA

Los interesados podrán participar como proponentes bajo alguna de las siguientes modalidades siempre y cuando cumplan los requisitos exigidos en la invitación:

**a)** Individualmente como: a) personas naturales nacionales o extranjeras, b) personas jurídicas nacionales o extranjeras.

**b)** Conjuntamente, como proponentes plurales en cualquiera de las formas de asociación previstas en el artículo 7 de la Ley 80 de 1993.

Los proponentes deben:

**a)** Tener capacidad jurídica para la presentación de la oferta.

**b)** Tener capacidad jurídica para la celebración del contrato y ejecución de la oferta.

**c)** No estar incursos en ninguna de las circunstancias de inhabilidad, incompatibilidad, conflicto de interés o prohibición para contratar previstas en la Constitución y en la ley.

**d)** No estar reportado en el último Boletín de Responsables Fiscales vigente publicado por la Contraloría General de la República. Esta disposición aplica para el proponente e integrantes de un proponente plural con domicilio en Colombia. Tratándose de proponentes extranjeros sin domicilio o sin sucursal en Colombia, deben declarar que no son responsables fiscales por actividades ejercidas en Colombia en el pasado y que no tienen sanciones vigentes en Colombia que impliquen inhabilidad para contratar con el Estado.

La entidad consultará los Antecedentes Judiciales en línea en los registros de las bases de datos, al igual que el Certificado de Antecedentes Disciplinarios conforme el artículo 1 de la Ley 1238 de 2008 y el Registro Nacional de Medidas Correctivas del Ministerio de Defensa Nacional – Policía Nacional, de acuerdo con lo dispuesto en el artículo 183 de la Ley 1801 de2016 –Código Nacional de Seguridad y Convivencia–.

## 4.3 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:

### 4.3.1 PERSONAS NATURALES

Deben presentar los siguientes documentos en copia simple:

A. Persona natural de nacionalidad colombiana: cédula de ciudadanía.
B. Persona natural extranjera con residencia en Colombia: cédula de extranjería vigente expedida por la autoridad competente.
C. Persona natural extranjera sin domicilio en Colombia: pasaporte.

### 4.3.2 PERSONAS JURÍDICAS

Deben presentar los siguientes documentos:

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

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

**a.** Fecha de expedición del certificado no mayor a treinta (30) días calendario anterioresa la fecha de cierre del proceso de contratación. En caso de modificarse la fecha de cierre del proceso, se tendrá como referencia para establecer el plazo de vigencia del certificado de existencia y representación legal la fecha originalmente establecida en la invitación.

**b.** Que el objeto de la sociedad permita ejecutar las actividades descritas en el objeto del presente proceso de contratación.

**c.** Las personas jurídicas nacionales y extranjeras deberán acreditar que su duración no será inferior a la del plazo del contrato y un año más. Para efectos de la evaluación, este plazo será contado a partir de la fecha del cierre del proceso de contratación.

**d.** Si el representante legal de la sociedad tiene restricciones para contraer obligacionesen

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.

**e.** El nombramiento del revisor fiscal en caso de que exista.

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

**III.** Fotocopia del documento de identificación del representante legal.

En el caso de las sucursales de las personas jurídicas extranjeras y como quiera que la sucursal en Colombia no es una persona jurídica diferente a la matriz, se tendrá en cuentala 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 el certificado de existencia y representación legal con fecha de expedición máximo de 30 días antes de la fecha de cierre del presente proceso de selección por la Cámara de Comercio. Cuando el representante legal de la sucursal tenga restricciones para contraer obligaciones, deberá acreditar autorización suficiente del órgano competente social respectivo para contraer obligaciones en nombre de la sociedad. La ausencia definitiva de autorización suficiente o no aportar dicho documento, una vez solicitado por la entidad, determinará la falta de capacidad jurídica para presentar la oferta.

**B.** Persona jurídica extranjera sin sucursal o domicilio en Colombia: Documentos que acrediten la existencia y representación legal de la sociedad extranjera, legalizados de conformidad con lo establecido en la presente invitación, en los que debe constar como mínimo los siguientes aspectos:

**I.** Nombre o razón social completa.

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

**III.** Que el objeto de la sociedad permita ejecutar las actividades descritas en el objeto del presente proceso de selección.

**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 por el cual se reconoce la personería jurídica.

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

Si no existiera ninguna autoridad o entidad que certifique la totalidad de la información de existencia y representación legal, el proponente o miembro extranjero del proponente plural debe presentar una declaración juramentada de una persona con capacidad jurídica para vincular y representar a la sociedad en la que conste que: (i) no existe autoridad u organismo que certifique lo solicitado en el presente numeral; (ii) la información requerida

en el presente literal, y (iii) la capacidad jurídica para vincular y representar a la sociedad de la persona que efectúa la declaración, así como de lasdemás personas que puedan representar y vincular a la sociedad, si existen.

**C.** Las entidades estatales deben presentar los siguientes documentos para acreditar su existencia:

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

### 4.3.3 PROPONENTES PLURALES

El documento de conformación de proponentes plurales debe:

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

**B.** Acreditar el nombramiento de un representante y un suplente, este último en casode considerarlo conveniente, cuya intervención deberá quedar definida en el Formato 2 – Conformación de Proponente Plural (Formato 2A- Consorcios) (Formato 2B- Uniones Temporales), 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 presentar 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.** El proponente plural debe señalar expresamente cuál es el porcentaje de participación de cada uno de sus miembros. La sumatoria del porcentaje de participación nopodrá ser diferente al 100%.

**E.** En la etapa contractual, no podrán modificarse los porcentajes de participación sin el consentimiento previo de la entidad.

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

## 4.4 CERTIFICACIÓN DE PAGOS DE SEGURIDAD SOCIAL Y APORTES LEGALES

### 4.4.1 PERSONAS JURÍDICAS

El proponente persona jurídica debe presentar el Formato 4 – Pagos de seguridad social y portes legales suscrito por el revisor fiscal, de acuerdo con los requerimientos de ley, o por el representante legal, bajo la gravedad del juramento, cuando no se requiera revisor fiscal,en el que conste el pago de los aportes de sus empleados a los sistemas de salud, riesgos profesionales, pensiones y aportes a las cajas de compensación familiar, al Instituto Colombiano de Bienestar Familiar, al Servicio Nacional de Aprendizaje y al Fondo Nacional de Formación Profesional para la Industria de Construcción, cuando a ello haya lugar.

La entidad no exigirá las planillas de pago. Basta el certificado suscrito por el revisor fiscal, en los casos requeridos por la ley, o por el representante legal que así lo acredite, de acuerdo al párrafo anterior.

Cuando la persona jurídica está exonerada de estas obligaciones en los términos previstos en el artículo 65 de la Ley 1819 de 2016 debe indicarlo en el Formato 4 – Pagos de seguridad social y aportes legales.

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

### 4.4.2 PERSONAS NATURALES

El proponente persona natural debe acreditar la afiliación a los sistemas de seguridad social en salud y pensiones aportando los certificados de afiliación respectivos o con el certificado de pago de la correspondiente planilla.

Los certificados de afiliación se deben presentar con fecha de expedición no mayor a treinta (30) días calendario, anteriores a la fecha del 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 la invitación.

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

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

### 4.4.3 PROPONENTES PLURALES

Cada uno de los integrantes del proponente plural debe suscribir por separado la declaración de la que tratan los numerales anteriores.

### 4.4.4 SEGURIDAD SOCIAL PARA LA ACEPTACIÓN DE LA OFERTA

El proponente seleccionado debe presentar, para la aceptación de la oferta, ante la dependencia respectiva, la declaración donde acredite el pago correspondiente a seguridad social y aportes legales cuando a ello haya lugar.

En caso de que la persona natural o jurídica no tenga o haya tenido dentro de los seis (6) meses anteriores a la fecha de aceptación de la oferta personal a cargo, y por ende no esté obligado a efectuar el pago de aportes legales y seguridad social debe indicar esta circunstancia en la mencionada certificación, bajo la gravedad de juramento.

### 4.4.5 REGISTRO ÚNICO TRIBUTARIO (RUT)

Si el proponente es colombiano o extranjero con sucursal o domicilio en Colombia, con la propuesta deberá aportar el Registro Único Tributario (RUT) actualizado. Para Uniones Temporales y Consorcios cada uno de sus integrantes deberá aportar el mencionado registro y el del Consorcio o Unión Temporal después de la adjudicación.

## 4.5 EXPERIENCIA

Los proponentes deben cumplir con el requisito habilitante de experiencia, el cual seacreditará mediante: i) la presentación del Formato 3 – Experiencia y ii) copia de alguno de los documentos válidos para acreditar la experiencia requerida señalada en el numeral 4.5.4. y 4.5.5

Los proponentes podrán acreditar experiencia proveniente de contratos celebrados con

particulares o entidades estatales.

Por regla general, el proponente solo puede acreditar la experiencia que ha obtenido y no la experiencia de su matriz, subsidiaria o integrante del mismo grupo empresarial.

### 4.5.1 CARACTERÍSTICAS DE LOS CONTRATOS PRESENTADOS PARA ACREDITAR LA EXPERIENCIA EXIGIDA

Los contratos para acreditar la experiencia deben cumplir las siguientes características:

**A.** Que las actividades ejecutadas correspondan a experiencia relacionada con "RENOVACIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS BITDEFENDER".

**B.** Estar relacionados en el Formato 3 – Experiencia. Los proponentes plurales deben indicar qué integrante aporta cada uno de los contratos señalados en el Formato 3 - Experiencia. Este documento debe presentarlo el proponente plural y no cada integrante.

**C.** El proponente podrá acreditar la experiencia con máximo DOS (02) Contratos o certificados de cumplimiento de contrato ejecutado o acta de terminación o liquidación del mismo, cuyo valor debe ser una suma igual o superior al cien por ciento (100%) del valor del presupuesto oficial del presente proceso de selección, expresado en SMMLV.

**D.** Debe haber terminado antes de la fecha de cierre del presente proceso de contratación.

**E.** No debe haberse impuesto alguna multa, cláusula penal, caducidad o haberse declarado algún siniestro, so pena de que dichos contratos no se tengan en cuenta para acreditar la experiencia. Esta regla no se aplicará en caso de que solo se haya declarado el siniestro de la póliza de responsabilidad civil extracontractual.

**F.** Para el contrato que sea aportado por socios de empresas que no cuentan con más de tres (3) años de constituidas, deben adjuntar un documento suscrito por elrepresentante legal y el revisor fiscal o contador público (según corresponda) donde se indique la conformación de la empresa. En estos casos, la entidad no tendrá en cuenta la experiencia aportada cuando los socios se encuentren inhabilitados. La entidad tendrá en cuenta la experiencia individual de los accionistas, socios o constituyentes de las sociedadescon menos de tres años de constituida.

**G.** La experiencia a la que se refiere este numeral podrá acreditarse mediante los documentos establecidos en la invitación en el numeral 4.5.4.

### 4.5.2 CONSIDERACIONES PARA LA VALIDEZ DE LA EXPERIENCIA REQUERIDA

La entidad tendrá en cuenta los siguientes aspectos para analizar la experiencia acreditaday que la misma sea válida como experiencia requerida:

**A.** Si el proponente relaciona o anexa más de un (1) contrato en el Formato 3 - Experiencia, para efectos de evaluación de la experiencia se tendrán en cuenta el contrato aportado de mayor valor.

**B.** Cuando el contrato que se pretenda acreditar como experiencia hayan sido ejecutado en consorcio o unión temporal, el porcentaje de participación del integrante será el registrado en el documento de conformación de la estructura plural en el respectivo procesode contratación, el contrato o en alguno de los documentos válidos para la acreditación de experiencia.

**C.** Cuando el contrato que se pretenda acreditar como experiencia hayan sido ejecutado en consorcio o unión temporal, el valor a considerar será el registrado en el documento válido para la acreditación de experiencia multiplicada por el porcentaje de participación que tuvo el

integrante o los integrantes.

**D.** Si el contrato aportado para acreditar la experiencia se ejecutó bajo la modalidad de consorcio o unión temporal, el plazo a considerar será el plazo total ejecutado, sin afectarse por el porcentaje de participación que tuvo el integrante que pretenda hacer valer la experiencia.

**E.** Cuando el contrato que se aporten para la experiencia haya sido ejecutado por un consorcio o unión temporal, y dos (2) o más de sus integrantes conformen un proponente plural para participar en el presente proceso, dicho contrato se entenderá aportado como un (1) solo contrato y se tendrá en cuenta para el aporte de la experiencia la sumatoria de los porcentajes de los integrantes del consorcio o unión temporal que ejecutaron el contrato y que están participando en el presente proceso.

### 4.5.3 ACREDITACIÓN DE LA EXPERIENCIA REQUERIDA

Los proponentes acreditarán para cada uno de los contratos aportados la siguiente información mediante alguno de los documentos señalados en la sección 4.5.4 y 4.5.5 de la invitación:

**A.** Contratante.

**B.** Objeto del contrato.

**C.** La fecha de iniciación de la ejecución del contrato.

**D.** La fecha de terminación de la ejecución del contrato.

**E.** Nombre y cargo de la persona que expide la certificación.

**F.** El porcentaje de participación del integrante del contratista plural.

### 4.5.4 DOCUMENTOS VÁLIDOS PARA ACREDITAR LA EXPERIENCIA REQUERIDA

El proponente debe aportar uno o algunos de los documentos que se establecen a continuación con el fin de acreditar la información solicitada. Los mismos deben estar debidamente diligenciados y suscritos por el contratante. En caso de existir discrepancias entre dos (2) o más documentos allegados por el proponente para probar experiencia, se tendrá en cuenta el orden de prevalencia establecido a continuación:

**A.** Acta de Liquidación.

**B.** Acta de entrega y acta de terminación.

**C.** Certificación de experiencia. Expedida con posterioridad a la fecha de terminación del contrato en la que conste el cumplimiento del objeto contratado debidamente suscrita por quien esté en capacidad u obligación de hacerlo.

**D.** Para los contratos que hayan sido objeto de cesión se debe aportar alguno de los documentos anteriores, donde se indique el porcentaje del contrato ejecutado por elcedente o por el cesionario, según el caso. La experiencia se valdrá afectada por elporcentaje del contrato ejecutado por el cedente o el cesionario, dependiendo de quien pretenda acreditar la experiencia.

### DOCUMENTOS TECNICOS HABILITADOS
### 4.5.5 PARA SUBCONTRATOS

Para acreditar la experiencia de subcontratos, cuyo contrato principal fue suscrito con particulares, se aplicarán las disposiciones establecidas en el numeral anterior.

Para demostrar la experiencia de los subcontratos derivados de contratos suscritos con entidades estatales el proponente debe aportar los documentos que se describen a continuación:

**A.** Certificación del subcontrato. Certificación expedida con posterioridad a la fecha de terminación del subcontrato, la cual debe estar suscrita por el representante legal del contratista del contrato principal, del cocesionario, o del EPC o consorcio constructor. Así mismo, debe contener la información requerida en la presente invitación para efectos de acreditar la experiencia.

**B.** Certificación expedida por la entidad estatal del contrato principal del cual se derivóel subcontrato.

Tratándose de subcontratos, cuando el contratista principal y el subcontratista se presenten al procedimiento de selección, las actividades subcontratadas solo serán válidas para el subcontratista; es decir, dichas actividades no serán tenidas en cuenta para acreditar experiencia del contratista principal.

En todo caso, la experiencia será válida para quien efectivamente haya ejecutado las actividades exigidas.

Los proponentes deben advertir a la entidad cuando en otros procesos el contratista originalhaya certificado que, dentro de su contrato, se llevó a cabo la subcontratación, por cuanto tales actividades no serán tenidas en cuenta para efectos de acreditar la experiencia del contratista original. Para tal fin, deberán informar a la entidad, mediante comunicación escrita, indicando el proceso en el cual el contratista certificó la respectiva subcontratación.

La obligación de informar las situaciones de subcontratación recae en los proponentes y de ninguna manera dicha obligación será de la entidad. En aquellos casos en los que el proponente no advierta tal situación, la entidad no tendrá responsabilidad alguna por cuanto no fue informada. En ese caso, el contrato se contabilizará como un todo y no se tendrá en cuenta lo relacionado con la subcontratación.

**4.6. CAPACIDAD TÉCNICA**: En consideración al objeto a contratar los proponentes deberán contar los siguientes requisitos los cuales se deberán evidenciar al momento de la presentación de propuesta dentro de la plataforma del SECOP II:

### 4.6.1. EXPERIENCIA DEL PERSONAL TECNICO:

Debido a los requerimientos técnicos descritos anteriormente se requiere personal altamente calificado que pertenezca al equipo de trabajo del oferente.

Con el objeto de seleccionar un proveedor que garantice estabilidad de los servicios a RENOVACIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS BITDEFENDER, CON ACTUALIZACION, SOPORTE, CAPACITACION Y ASISTENCIA TECNICA POR EL TERMINO DE UN AÑO, PARA LAS ESTACIONES DE TRABAJO Y SERVIDORES DE LA PLATAFORMA TECNOLOGICA DE LA GOBERNACION DE BOLIVAR, los cuales son de misión crítica para el funcionamiento de la entidad, es necesario que el proponente cuente con personal altamente calificado, capacitado y experimentado, para lo cual se requiere, adjuntar las hojas de vida y certificados

Para garantizar la correcta ejecución del contrato, La Gobernación de Bolívar, se requiere que el oferente presente dentro de su equipo de trabajo, un Ingeniero Gerente de Proyectos de TI, con el objeto de servir de enlace entre el supervisor del contrato por parte de La Gobernación de Bolívar y la empresa oferente; realizando entrega de los documentos solicitados en el presente proceso al igual que los informes mensuales de funcionamiento general del antivirus a contratar.

El oferente debe contar con certificado que permita garantizar que cuenta con personal de Bitdefender Certified Technical Specialist.

Descripción del Personal requerido:

- **Gerente de proyecto**: ingeniero de sistemas, electrónico, industrial o afín, con estudios en antivirus y cloud computing, especialista en seguridad informática, con experiencia en administración y configuración de antivirus, debe contar con certificación BITDEFENDER CERTIFIED TECHNICAL SPECIALIST, con certificación especializada en Cyber Security Foundation, con estudios como auditor en la norma internacional ISO 27001, con estudios en Ethical Hacking, experiencia en administración de servidor y soporte remoto.

### 4.6.2. EXPERIENCIA TECNICA:

Debido a los requerimientos técnicos descritos anteriormente se requiere que el oferente sea altamente calificado. La Gobernación de Bolívar, para garantizar la correcta ejecución del contrato, requiere que el oferente presente certificado que conste que el oferente es categoría GOLD RESELLER STATUS del antivirus Bitdefender.

## CAPÍTULO V CRITERIOS DE EVALUACIÓN, CRITERIOS DE DESEMPATE Y OFERTA ECONÓMICA

La entidad estatal revisará las ofertas económicas y verificará que la de menor precio cumpla con las condiciones de la invitación. Si cumple, aceptará la oferta de menor precio e informará al contratista en el documento de aceptación el nombre del supervisor delcontrato.

Por el contrario, si la oferta de menor precio no cumple con las condiciones señaladas en la Invitación, la Entidad Estatal debe verificar el cumplimento de los requisitos de la Invitación de la oferta con el segundo mejor precio, y así sucesivamente, sin perjuicio de lo señalado en el numeral 1.6.

Si hay empate, la entidad debe aceptar la oferta presentada primero en el tiempo.

La oferta y la comunicación de aceptación de la misma conforman el contrato y los dos documentos serán publicados en el SECOP en la fecha establecida en el cronograma.

### 5.1. OFERTA ECONÓMICA

El proponente deberá diligenciar en su totalidad y consignar el valor de su oferta en el formato señalado. Dicho diligenciamiento es de carácter obligatorio.

**Validez de la oferta:** Los valores deberán expresarse en pesos colombianos, a precios fijos inmodificables. Si la oferta presenta diferencias entre los precios unitarios y los totales, para efectos de la evaluación y adjudicación se tendrá en cuenta los precios unitarios, incluyendo dentro de ellos el IVA si aplica, si no lo especifican por aparte.

Si el oferente mejora las especificaciones y condiciones técnicas en los servicios cotizados, esto no será considerado como error, ni como otro servicio cotizado.

### 5.1.3 PRECIO ARTIFICIALMENTE BAJO

En el evento en el que el precio de una oferta no parezca suficiente para garantizar una correcta ejecución del contrato, de acuerdo con la información recogida durante la etapa de planeación

y particularmente durante el estudio del sector, la entidad aplicará el proceso descrito en el artículo 2.2.1.1.2.2.4. del Decreto 1082 de 2015; además, podrá acudir a los parámetros definidos en la Guía para el manejo de ofertas artificialmente bajas en procesos de contratación de Colombia Compra Eficiente, como criterio metodológico.

### 5.1.4 CRITERIOS DE DESEMPATE

En caso de empate en el valor propuesto, la entidad estatal aceptará la oferta que haya sido presentada primero en el tiempo.

## CAPÍTULO VI RIESGOS ASOCIADOS AL CONTRATO, FORMA DE MITIGARLOS Y ASIGNACIÓN DE RIESGOS

### 6.1 ASIGNACIÓN DE RIESGOS

La Matriz 3 - Riesgos, en la cual se tipifican los riegos previsibles, elaborada por la entidad, hace parte de la presente invitación y los interesados podrán presentar observaciones sobre su contenido.

Los proponentes deben realizar todas las evaluaciones y estimaciones que sean necesarias para presentar su propuesta sobre la base de un examen cuidadoso de sus características, incluyendo los estudios, diseños, evaluaciones y verificaciones que consideren necesarios para formular la propuesta con base en su propia información, de manera que el proponente debe tener en cuenta el cálculo de los aspectos económicos del proyecto, los cuales, deben incluir todas las obligaciones y asunción de riesgos que emanan del contrato.

## CAPÍTULO VII GARANTÍAS

### 7.1 GARANTÍAS DEL CONTRATO

### 7.2.1 GARANTÍA DE CUMPLIMIENTO

Para cubrir cualquier hecho constitutivo de incumplimiento, el contratista debe presentar la garantía de cumplimiento en original a la entidad dentro de los **UN (01) DÍA** hábilsiguientes contados a partir de la aceptación de la oferta y esta requerirá la aprobación dela entidad. Esta garantía tendrá las siguientes características:

| Característica | Condición | | |
|---|---|---|---|
| **Clase** | Cualquiera de las clases permitidas por el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015, a saber: (i) contrato de seguro contenido en una póliza para entidades Estatales, (ii) patrimonio autónomo, (iii) garantía Bancaria. | | |
| **Asegurado/ beneficiario** | **DEPARTAMENTO DE BOLÍVAR** identificada con NIT 890480059-1. | | |
| **Amparos, vigencia y valores** | **Amparo** | **Vigencia** | **Valor Asegurado** |

| | | | |
|---|---|---|---|
| **asegurados** | **Cumplimiento General** del contrato y el pago de las multas y la cláusula penal pecuniaria que se le impongan | Por el término de ejecución del contrato y cuatro (04) meses más. | Diez por ciento (10%) del Valor del contrato |
| | **calidad de los bienes suministrados** | vigente por el término de ejecución del contrato y cuatro meses más. | por el 10% del valor del contrato |
| **Tomador** | Para las personas jurídicas: la garantía debe tomarse con el nombre o razón social y tipo societario que figura en el Certificado de Existencia y Representación Legal expedido por la Cámara de Comercio respectiva, y no solo con su sigla, a no ser que en el referido documento se exprese que la sociedad puede denominarse de esa manera. | | |
| | No se aceptan garantías a nombre del representante legal o de alguno de los integrantes del consorcio. Cuando el contratista sea una unión temporal o consorcio, se debe incluir su razón social, NIT y porcentaje de participación de cada uno de los integrantes. | | |
| | Para el contratista conformado por una estructura plural (unión temporal, consorcio): la garantía deberá ser otorgada por todos los integrantes del contratista, para lo cual se debe relacionar claramente los integrantes, su identificación y porcentaje de participación, quienes para todos los efectos serán los otorgantes de esta. | | |
| **Característica** | **Condición** | | |
| Información necesaria dentro de la póliza | ✓ Número y año del contrato | | |
| | ✓ Objeto del contrato | | |
| | ✓ Firma del representante legal del contratista | | |
| | ✓ En caso de no usar centavos, los valores deben aproximarse al mayor. Ej. Cumplimiento si el valor a asegurar es $14.980.420,20 aproximar a $14.980.421 | | |

El contratista está obligado a restablecer el valor de la garantía cuando esta se reduzca por razón de las reclamaciones que efectúe la entidad, así como ampliar las garantías en los eventos de adición y/o prórroga del contrato. No restablecer la garantía, no adicionarla o prorrogarla, según el caso, constituye causal de incumplimiento del contrato y se iniciarán los procesos sancionatorios a que haya lugar.

## CAPÍTULO VIII COMUNICACIÓN DE ACEPTACIÓN DE LA OFERTA Y CLÁUSULAS ADICIONALES

Las condiciones de ejecución están previstas en el Anexo 2 – Comunicación de aceptación de la oferta y en esta invitación. Dentro de estas condiciones se incluye la forma de pago, anticipo, obligaciones y derechos generales del contratista, obligaciones de la entidad, garantías, multas, cláusula penal y otras condiciones particulares aplicables al negocio jurídico a celebrar.
El proponente a quien se acepte la oferta debe presentar el Registro Único Tributario – RUT.

### 8.1. MULTAS

Se causarán multas equivalentes a 5 SMMLV, por cada día calendario transcurrido a partir del tercer día hábil siguiente al momento en que se verifique la existencia de investigaciones penales, medidas de aseguramiento o condenas proferidas en Colombia o enel extranjero en contra de cualquiera de los directivos, representantes legales, accionistas o integrantes del

Contratista, sin que estas hayan sido notificadas a la Entidad. La sumatoria de estas multas no podrá ser superior al 5% del valor del contrato.

Si durante la ejecución del Contrato se generaran incumplimientos del Contratista, secausarán las siguientes multas:

**Causales:**

1. Por no mantener en vigor, renovar, prorrogar, obtener para la etapa siguiente, corregir o adicionar las garantías, en los plazos y por los montos establecidos en la cláusula 18, de acuerdo al contrato inicial o sus modificaciones, se causará una multa equivalente al 1% del valor del contrato, por cada día calendario de atraso en el cumplimiento; sin perjuicio de que con esta conducta se haga acreedor a otras sanciones más gravosas.
2. Si el Contratista no entrega la información completa que le solicite al supervisor, que se relacione con el objeto del contrato, dentro de los plazos y en los términos de cada requerimiento, se causará una multa equivalente al 0,2 del valor del contrato. Estas multas se causarán sucesivamente por cada día de atraso, hasta cuando el Contratista demuestre que corrija el incumplimiento respectivo a satisfacción del interventor.
3. Por atraso imputable al Contratista en la firma del acta de inicio o no iniciar la ejecución en la fecha pactada, se causará una multa diaria equivalente al 0,3% del valor delcontrato, por cada día calendario de atraso. Igual sanción se aplicará en caso de que el Contratista no inicie efectivamente con la ejecución del contrato en la fecha acordada.
4. Por atraso en el cumplimiento de las obligaciones relacionadas con la seguridad social, parafiscales, o pago de salarios o honorarios de alguno o algunos de sus empleados o Contratistas, al Contratista se le impondrá una multa equivalente a 5salarios mínimos diarios legales vigentes, por cada día calendario de atraso en el cumplimiento de dicha obligación.

**Parágrafo 1.** Las multas son apremios al Contratista para el cumplimiento de sus obligaciones y, por lo tanto, no tienen el carácter de estimación anticipada de perjuicios, de manera que pueden acumularse con cualquier forma de indemnización, en los términos previstos en el artículo 1600 del Código Civil.

**Parágrafo 2.** En caso de que el Contratista incurra en una de las causales de multa, este autoriza a la Entidad Contratante para descontar el valor de la misma, la cual se tomará directamente de cualquier suma que se le adeude al Contratista, sin perjuicio de hacer efectiva la cláusula penal o la garantía de cumplimiento del contrato.

**Parágrafo 3.** El pago en cualquier forma, incluyendo la deducción de los valores adeudadosal Contratista, realizado con fundamento en las multas impuestas, no exonerará al Contratista de continuar con la ejecución del contrato ni de las demás responsabilidades y obligaciones que emanen del contrato.

**Parágrafo 4.** En caso de que el Contratista reincida en el incumplimiento de una o de varias obligaciones se podrán imponer nuevas multas.

**Parágrafo 5.** Para efectos de la imposición de las multas el Salario Mínimo Diario o Mensual Vigente, será aquel que rija para el momento del incumplimiento del contrato.

**Parágrafo 6.** El monto de ninguna de las sanciones asociadas a cada causal de multa, aplicada de forma independiente, podrá ser superior al 5% del valor del contrato, particularmente frente a aquellas que se imponen de forma sucesiva. Lo anterior, sin perjuicio de que se inicie un nuevo procedimiento sancionatorio para efectos de imponer nuevas multas.

## 8.2. CLÁUSULA PENAL

Las partes acuerdan que la aplicación de la cláusula penal no exime el cumplimiento de las obligaciones contractuales y podrá exigirse al Contratista la pena y la indemnización de perjuicios.

En caso de incumplimiento por parte del Contratista, no subsanado en un plazo de cinco (5)días hábiles contados a partir de la fecha de incumplimiento, sin necesidad de previo requerimiento, por el simple retardo en el cumplimiento, por el cumplimiento imperfecto o por la inejecución total o parcial de las obligaciones a su cargo contraídas en virtud del presente acuerdo, el Contratista pagará a la Entidad, una suma equivalente al treinta por ciento (30%) del valor del contrato. La presente cláusula penal no tiene el carácter de estimación anticipada de perjuicios.

**Parágrafo 1.** El pago de la presente cláusula penal no extinguirá las obligaciones contraídas por el Contratista en virtud del presente contrato. En consecuencia, la estipulación y el pago de la pena dejan a salvo el derecho de la Entidad de exigir acumulativamente con ella el cumplimiento o la resolución del contrato, en ambos casos, con la correspondiente indemnización de perjuicios ocasionados en virtud del incumplimiento total o parcial o del cumplimiento tardío o imperfecto de las obligaciones a cargo del Contratista.

**Parágrafo 2.** El Contratista manifiesta y acepta que la Entidad compense el valor correspondiente que eventualmente resulte de la pena estipulada con las deudas queexistan a su favor y que estén a cargo de la Entidad, ya sea en virtud de este contrato o de cualquier otro contrato o convenio que se haya suscrito entre las mismas partes, o por cualquier otro concepto.

**Parágrafo 3.** Esta misma sanción se aplicará en caso de declararse la caducidad del contrato.

## 8.3. CLÁUSULAS EXCEPCIONALES

Se entienden incorporadas al contrato las cláusulas excepcionales a que se refiere el Estatuto General de Contratación de la Administración Pública.

## 8.4. INDEPENDENCIA DEL CONTRATISTA

El contratista es independiente de la entidad y, en consecuencia, el contratista no es su representante, agente o mandatario. El contratista no tiene la facultad de hacer declaraciones, representaciones o compromisos en nombre de la entidad, ni de tomar decisiones o iniciar acciones que generen obligaciones a su cargo.

## 8.5. INEXISTENCIA DE RELACIÓN LABORAL ENTRE LA ENTIDAD Y EL CONTRATISTA

El contratista ejecutará el presente contrato con sus propios medios y con plena autonomía técnica y administrativa y el personal que vincule durante la ejecución del contrato será de su libre escogencia, debiendo cumplir con todos los requisitos exigidos en los Documentos del proceso de contratación. Entre el contratista, el personal que éste contrate y la entidad no existe, ni existirá vínculo laboral alguno. En consecuencia, el contratista responderá de manera exclusiva por el pago de honorarios, salarios, prestaciones e indemnizaciones de carácter laboral y contractual a que haya lugar. Así mismo, el contratista debe verificar y/o cumplir con la afiliación de dicho personal al Sistema de Seguridad Social Integral (salud, pensiones y riesgos profesionales) y a la Caja de Compensación Familiar, ICBF y SENA, cuando haya lugar, de acuerdo con lo dispuesto en la ley.

El contratista solo podrá subcontratar con la autorización previa y expresa de la entidad. El empleo de tales subcontratistas no relevará al contratista de las responsabilidades que asume por las labores de la construcción y por las demás obligaciones emanadas del presente contrato. La entidad no adquirirá relación alguna con los subcontratistas y la responsabilidad de los trabajos que éstos ejecuten seguirá a cargo del contratista. La entidad podrá exigir al contratista la terminación del subcontrato en cualquier tiempo y el cumplimiento inmediato y directo de sus obligaciones o el cambio de los subcontratistas cuando, a su juicio, éste (os) no cumpla(n) con las calidades mínimas necesarias para la ejecución de la(s) labor(es) subcontratada(s).

## 8.6. CESIÓN

El contratista no podrá ceder los derechos y obligaciones emanados del contrato, sin el consentimiento previo y expreso de la entidad, pudiendo este reservarse las razones que tenga para negar la cesión. La cesión se efectuará de conformidad con lo establecido en el artículo 893 del Código de Comercio en concordancia con las demás disposiciones vigentes sobre la materia.

## 8.7. LIQUIDACIÓN

El contrato será objeto de liquidación de acuerdo con lo establecido en las normas que regulan la materia. El término para la liquidación del contrato será del definido en el Estatuto de Contratación de la Administración Pública.

Para la liquidación se exigirá al contratista la ampliación de la garantía, si es del caso, a fin de avalar las obligaciones que éste deba cumplir con posterioridad a la extinción del presente contrato.

Si el contratista no se presenta para efectos de la liquidación del contrato o las partes no llegan a ningún acuerdo, la entidad procederá a su liquidación, por medio de resolución motivada susceptible del recurso de reposición. Así mismo, y de conformidad con lo previstopor el artículo 11 de la Ley 1150 de 2007, si el contratista deja salvedades en la liquidación bilateral, la entidad podrá liquidar unilateralmente, caso en el cual, esta solo procederá en relación con los aspectos que no hayan sido objeto de acuerdo, siempre que la liquidación unilateral pueda contener decisiones nuevas frente a la liquidación acordada o que no hayansido respondidas por la entidad con anterioridad a la liquidación.

## 8.8. SOLUCIÓN DE CONTROVERSIAS

Las controversias o diferencias que surjan entre el contratista y la entidad con ocasión de la firma, ejecución, interpretación, prórroga o terminación del contrato, así como de cualquier otro asunto relacionado con el presente contrato, serán sometidas a la revisión de las partespara buscar un arreglo directo, en un término no mayor a **QUINCE (15)** días hábiles a partir de la fecha en que cualquiera de las partes comunique por escrito a la otra parte la existencia de una diferencia y la explique al menos someramente.

Las controversias que no puedan ser resueltas de forma directa entre las partes, seresolverán empleando las instancias y procedimientos contemplados en los artículos 68 y siguientes de la Ley 80 de 1993 y demás normas concordantes.

## CAPÍTULO IX LISTA DE ANEXOS, FORMATOS, MATRICES Y FORMULARIOS

### 9.1. ANEXOS

1. Anexo 1 – Anexo técnico
2. Anexo 2- Pacto de transparencia

### 9.2. FORMATOS

1. Formato 1 – Carta de presentación de la oferta
2. Formato 2 – Conformación de proponente plural (Formato 2A- Consorcios) (Formato 2B- Unión Temporal)
3. Formato 3 – Experiencia
4. Formato 4 – Pagos de seguridad social y aportes legales

### 9.3. MATRICES

1. Matriz 1 – Riesgos

### 9.4. FORMULARIOS

1. Formulario 1– Formulario de Oferta económica