OFICINA DE TELEMÁTICA

Bogotá, D.C., 22 JUN 2022

I. ASPECTOS GENERALES DEL ESTUDIO PREVIO.

1. DEFINICIÓN O IDENTIFICACIÓN DE LA NECESIDAD Y ANÁLISIS DEL SECTOR

1.1 DESCRIPCIÓN GENERAL DEL OBJETO

SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM.

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE	PRODUCTO
43233200	Difusión de tecnologías de información y telecomunicaciones	Software	Software de seguridad y protección	

1.2 VALOR ESTIMADO

El valor estimado para el presente proceso de contratación es de MIL CUATROCIENTOS MILLONES DE PESOS ($1.400.000.000,00) MONEDA LEGAL EXENTO DE IVA, discriminado de la siguiente manera:

ÍTEM	RUBRO Y DESAGREGACIÓN PRESUPUESTAL	UNIDAD	DESCRIPCIÓN	RECURSO	CANTIDAD	VALOR UNITARIO ESTIMADO EXENTO DE IVA	VALOR TOTAL ESTIMADO EXENTO DE IVA
1	1501-0100-22-0-1501037-02	000	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM.	11	1	$ 1.400.000.000,00	$ 1.400.000.000,00
VALOR TOTAL ESTIMADO							$1.400.000.000,00

Nota 1: los elementos de acuerdo a su utilización, desde el componente técnico se encuentran catalogados por la Oficina de Telemática en el numeral 3 literal n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional, del artículo 188 de la Ley 1819 del 29/12/2016, el cual modificó el artículo 477 del Estatuto Tributario, son bienes que están exentos del impuesto sobre las ventas.

1.3 CERTIFICACIÓN PLAN ANUAL DE ADQUISICIONES, GASTOS DE FUNCIONAMIENTO Y/O INVERSIÓN.

Certificado Plan de compras No. 057 del 27/01/2022, por valor de MIL CUATROCIENTOS MILLONES DE PESOS ($1.400.000.000,00) Recurso 11.

No	Fecha	No. Plan de compras	Recurso	Descripción	Cantidad	Valor unitario	Valor total
1	27/01/2022	057	11	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM.	1	$ 1.400.000.000,00	$ 1.400.000.000,00
Total							$1.400.000.000,00

1.4 CLASE DE CONTRATO	compraventa
1.5 PERFIL Y CALIDAD DE LOS PROPONENTES	Todas las personas naturales o jurídicas, nacionales o extranjeras, con apoderado o representante legal en Colombia, domiciliadas o con sucursal en Colombia, en forma individual o conjunta (consorcio ó unión temporal), que tengan dentro de su objeto social o actividad la fabricación y/o comercialización y/o distribución autorizada por la casa fabricante de los bienes objeto del presente proceso, siempre y cuando cumplan con todos los requisitos exigidos para el mismo y se encuentren registradas en el SECOP II.

1.6 IDENTIFICACIÓN DE LA NECESIDAD Y JUSTIFICACIÓN

La Oficina de Telemática de conformidad con el Artículo 25, del Decreto 113 del 25 de enero de 2022, tiene entre otras las siguientes funciones:

"(…) 1. Diseñar, implementar, difundir y hacer seguimiento a la Estrategia de Tecnologías de la Información y las Comunicaciones que responda a las necesidades institucionales y del sector defensa, alineada a las políticas establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones o quien haga sus veces. (…) 3. Desarrollar estrategias que contribuyan al fortalecimiento de la seguridad de la información digital en la Institución, mediante el empleo de estándares y buenas prácticas enfocadas a preservar la confidencialidad, integridad y disponibilidad de la información. (…) 6. Promover y facilitar el acceso a las tecnologías de la información y las comunicaciones a los clientes y partes interesadas, dentro de los límites establecidos por la Constitución Política y la ley. (…)"

En virtud de lo anterior, es responsabilidad de la Oficina de Telemática garantizar el óptimo funcionamiento del componente de telecomunicaciones e informática y especialmente su adecuado desempeño en pro del fortalecimiento del servicio policial, siendo de vital importancia la adquisición y/o renovación y mantenimiento de las herramientas de seguridad y controles tecnológicos que garanticen la disponibilidad, integridad y seguridad de las diferentes aplicaciones Institucionales y por ende la información suministrada a través de las mismas.

La Policía Nacional requiere dos (02) soluciones que permitan controlar software malicioso que se mueve a través del internet, evitando afectación en los equipos de cómputo, así:

1. Herramienta que apruebe el licenciamiento de cuarenta y cinco mil (45.000) nodos para controlar de forma centralizada las aplicaciones, permita definir listas blancas y negras del software que podrá hacer parte de la plataforma institucional, con esto cumpliendo uno de los requisitos de la norma ISO 27001-13 para lo cual la Policía Nacional ya cuenta con siete (7) procesos certificados (OFITE, DIJIN, DIPOL, DIASE, DINCO, DIRAN y DIRAF), adicionalmente combatir la defraudación de derechos de autor, al no admitir la instalación de software que no se encuentre licenciado, en segunda medida se necesita adquirir el licenciamiento para cuarenta y cinco mil nodos (45.000) que contaran con la solución antivirus y la herramienta que permita controlar la pérdida o fuga de información que realice control de los dispositivos que se conectan mediante unidades de almacenamiento externo y clasificación mediante palabras claves que permita realizar control sobre la información que se gestiona mediante la red institucional y por último el licenciamiento para quince mil (15.000) nodos que serán cifrados para prevenir la fuga de información.
2. Herramienta que apruebe el licenciamiento de veinte mil (20.000) nodos que permita realizar control perimetral del correo electrónico con el fin de prevenir la propagación de spam o riesgos asociados a archivos maliciosos que se puedan enviar mediante los gestores de correo con los que cuenta la institución, esta solución deberá permitir contar con un panel en el cual se analicen las amenazas encontradas. Estas dos soluciones minimizarán el riesgo de fuga, perdida o daño de la información institucional, y de esta manera se realizará fortalecimiento de la infraestructura tecnológica aumentando el nivel de protección de cada uno de los equipos de cómputo con los que cuenta la

institución; brindando de esta manera un enfoque de continuidad y aplicabilidad hacia el Sistema de Gestión de Seguridad de la Información, específicamente en el pilar de confidencialidad e integridad.

Se considera que, a través de estas soluciones, se podrá minimizar las infecciones y/o ataques de códigos maliciosos, que probablemente pueden irrumpir en los sistemas o bases de datos que se utilizan no solo a nivel local sino también a un nivel descentralizado. Estos aspectos hacen que día a día se busquen nuevos mecanismos para proteger la información de los procesos, logrando así reducir las brechas de seguridad, que puedan facilitar el acceso de personal no autorizado a los sistemas de la institución y la violación al manual de seguridad de la información realizando la instalación de software no licenciado ni autorizado por la Policía Nacional.

Con el fin de identificar una cifra aproximada de nodos a ser soportados por la solución, la Policía Nacional cuenta con herramientas que nos suministran una posible cifra como lo es el reporte de 58.926 equipos en servicio y disponibles generado por la herramienta SINVE con corte a primer trimestre del presente año y el el directorio activo de Microsoft (dominio policía.gov.co) que cuenta con 45.700 equipos registrados. Las cifras antes expuestas, los estudios de mercado realizados y el presupuesto asignado nos generan una necesidad de 45.000 nodos a cubrir con la solución.

El alcance del presente proceso es con el fin de adquirir una solución con la cual se pueda garantizar de forma segura la conexión a los sistemas de información y acceso a los diferentes recursos tecnológicos que aportan significativamente al servicio de Policía desde redes externas.

La Policía Nacional en cumplimiento a la normativa que garantiza la seguridad y protección de la información, en la que se destaca la Ley 1581 de 2012 Protección de datos personales, Decreto Reglamentario 1377 de 2013, el CONPES 3854 del 11/04/2016 y el 3995 del 2020, Modelo de seguridad y privacidad de la Información (MSPI) del MINTIC, la declaración de prácticas de certificación de la plataforma de llave pública otorgada por el Organismo Nacional de Acreditación de Colombia (ONAC), Resolución No. 08310 del 28/12/2016 Manual del sistema de gestión de seguridad de la información, y la normatividad expedida para la protección de la propiedad intelectual.

ÍTEM	DESCRIPCIÓN	NECESIDAD REAL	BIENES A ADQUIRIR	DÉFICIT
1	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM.	1	1	0

Para la consecución de este tipo de bienes se consideran de características técnicas uniformes y de común utilización, porque sus características técnicas son estándar en el mercado de telecomunicaciones e iguales para diferentes fabricantes del mercado, su utilización es común en todas las redes de comunicación corporativas y cumplen con especificaciones de servicios comunes, ofrecidos por los diferentes fabricantes y su utilización está definida con un propósito específico. Por lo anterior, diferentes oferentes pueden presentar los mismos productos y se requiere obtener el costo más favorable para la Entidad.

Verificado el Decreto 397 del 17/03/2022 (plan de austeridad del gasto 2022 para los órganos que hacen parte del presupuesto general de la Nación), los funcionarios dueños de la necesidad que firman el presente estudio previo, se acogen al mismo, teniendo en cuenta la necesidad a adquirir con el presente proceso.

Así mismo se verificó la tienda virtual del estado colombiano https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano, y no se encuentra ningún acuerdo marco de precios, que contemple la adquisición de estos elementos objeto del presente proceso con las especificaciones técnicas requeridas Mediante comunicación oficial No. GS-2022-004681-OFITE, del 07 de Junio de 2022, suscrito por el señor Mayor JANSEN JAIR GONZÁLEZ ARAGÓN, Jefe Grupo Investigación y Proyección Tecnológica, informa que el comité evaluador una vez validados los ajustes requeridos mediante acta No. 245 OFITE-GINTE

2.25 del 07/06/2022, considera viable la adquisición de este componente tecnológico y así fortalecer la parte administrativa y operativa de la Policía Nacional.

En cumplimiento al numeral 8 del Artículo 2.2.1.1.2.1.1 del Decreto 1082 del 26 de mayo de 2015, el Analista Contractual DIRAF el 06/06/2022, certifica que una vez verificados en la página web de Colombia Compra Eficiente y en la del Ministerio de Comercio, Industria y Turismo, los Acuerdos Comerciales y Tratados de Libre Comercio (TLC), negociados por Colombia en los capítulos de contratación pública, se estableció que la "*SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM* ", por un valor de MIL CUATROCIENTOS MILLONES DE PESOS ($1.400.000.000,00); SI está cubierto bajo las obligaciones de carácter internacional derivadas de los Acuerdos: ALIANZA DEL PACÍFICO, (CHILE, MÉXICO Y PERÚ), CANADÁ, CHILE, COREA, ESTADOS UNIDOS, COSTA RICA, MÉXICO, TRIÁNGULO NORTE, ESTADOS AELC, UNIÓN EUROPEA Y CAN; toda vez que:

a. La cuantía del proceso excede los umbrales establecidos en los acuerdos publicados.
b. La Policía Nacional se encuentra incluida en los listados de entidades cubiertas por los acuerdos.
c. Los bienes a contratar no se encuentran cubiertos bajo alguna exclusión de aplicabilidad o excepción.

De acuerdo a lo anterior, se deben tener en cuenta los principios y obligaciones en cuanto a la protección de los principios de derecho internacional, la publicidad de las contrataciones, el uso de medios electrónicos, las modalidades de contratación y la revisión de impugnaciones en la configuración de los documentos del proceso contractual.

La contratación objeto del presente proceso se requiere para el mes de agosto de 2022.

2. ANTECEDENTES ADMINISTRATIVOS DEL PROCESO

Se consultó en la página www.colombiacompra.gov.co, procesos con objeto igual y/o similar al presente estudio previo durante los últimos (3) años celebrados por la Policía Nacional, encontrándo proceso lo siguiente.

UNIDAD CONTRATANTE Y CONTRATISTA	NÚMERO DEL CONTRATO Y FECHA DE SUSCRIPCIÓN	OBJETO	NÚMERO DE PROCESO	ACIERTOS	PROBLEMAS
POLICÍA NACIONAL DIRAF ONA SYSTEMS S.A.S	PN DIRAF 06-2-10124-20 07/10/2020	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM.	PN DIRAF SA 130 2020	PLANEACIÓN Y EJECUCIÓN.	NO SE PRESENTARON PROBLEMAS DURANTE LA EJECUCIÓN DEL CONTRATO

Nota: para las vigencias 2019 y 2021, no se encontraron procesos contractuales iguales y/o similares para la adquisición de solución software antivirus, data lost prevention, control de aplicaciones, cifrado y antispam, que hayan sido realizados por la entidad.

- **Información verificada y aprobada por los funcionarios dueños de la necesidad que firman el presente estudio previo.**

3. FUNDAMENTOS JURÍDICOS QUE SOPORTAN LA MODALIDAD DE SELECCIÓN

Teniendo en cuenta que los bienes a adquirir poseen características técnicas uniformes, y que además existen varias empresas que están en capacidad de satisfacer la necesidad cumpliendo con las especificaciones

técnicas requeridas, el presente proceso de selección se debe adelantar bajo la modalidad de selecc6n abreviada:

Reglada por el numeral 2 del Artículo 2 de la ley 1150 de 2007 y el Capítulo 2, Sección 1, Subsección 2 del Decreto 1082 de 2015, así:

"(...) La Selección abreviada corresponde a la modalidad de selección objetiva prevista para aquellos casos en que por las características del objeto a contratar, las circunstancias de la contratación o la cuantía o destinación del bien, obra o servicio, puedan adelantarse procesos simplificados para garantizar la eficiencia de la gestión contractual..."

En sujeción a la norma anterior, el numeral 2 del capítulo II de la Resolución No. 03049 de 2014, dispone:

"(...) Es una modalidad de selección objetiva prevista para aquellos casos en que por las características del objeto a contratar, las circunstancias de la contratación o la cuantía o destinación del bien, obra o servicio, pueden adelantarse procesos simplificados. Para efectos de esta modalidad de selección, el numeral 2º del artículo 2º de la Ley 1150 de 2007..."

Son causales de esta modalidad:

- **Selección Abreviada para la adquisición de Bienes y Servicios de Características Técnicas Uniformes:**

El literal a) del Numeral 2 del Artículo 2 de la ley 1150 de 2007, manifiesta:

"(...) La adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades, que corresponden a aquellos que poseen las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos.

Para la adquisición de estos bienes y servicios las entidades deberán, siempre que el reglamento así lo señale, hacer uso de procedimientos de subasta inversa o de instrumentos de compra por catálogo derivados de la celebración de acuerdos marco de precios o de procedimientos de adquisición en bolsas de productos..."

Se aclara que las entidades estatales de la rama ejecutiva del poder público del orden nacional, obligadas a aplicar la ley 80 de 1993 y ley 1150 de 2007 o las normas que las modifiquen, aclaren, adicionen o sustituyan, están obligadas a adquirir Bienes y Servicios de características técnicas Uniformes a través de los Acuerdos marco de Precios vigentes.

Así la cosas y de conformidad con el artículo 2.2.1.2.1.2.9. del Decreto 1082 de 2015, Colombia Compra Eficiente deberá publicar el catálogo para Acuerdos Marco de Precios, y las entidades Estatales en la etapa de planeación del proceso de contratación están obligadas a verificar si existe un Acuerdo Marco de Precios vigente, con el cual la Entidad Estatal pueda satisfacer la necesidad identificada. De encontrarse el bien o servicio dentro del catálogo para Acuerdos Marco de Precios, las entidades Estatales enmarcadas dentro del inciso primero del Artículo 2.2.1.2.1.2.7. del Decreto 1082 de 2015, estarán obligas a suscribir el Acuerdo Marco de Precios, en la forma que Colombia Compra Eficiente disponga.

4. CRITERIOS DE SELECCIÓN

4.1. ESPECIFICACIONES TÉCNICAS MÍNIMAS

Las especificaciones técnicas requeridas están descritas en el Anexo "ESPECIFICACIONES TÉCNICAS MÍNIMAS" del presente estudio previo, las cuales se verificarán como CUMPLE o NO CUMPLE.

4.1.1. EXPERIENCIA PROPONENTE

La experiencia del proponente está descrita en el Anexo "ESPECIFICACIONES TÉCNICAS MÍNIMAS" del presente estudio previo, las cuales se verificarán como CUMPLE o NO CUMPLE.

4.1.2 NIVEL DE EDUCACIÓN O NIVEL ACADÉMICO

No aplica.

4.1.3 EXPERIENCIA

No aplica.

4.1.4 EXPERIENCIA DEL PERSONAL

La experiencia del personal está descrita en el Anexo "ESPECIFICACIONES TÉCNICAS MÍNIMAS" del presente estudio previo, las cuales se verificarán como CUMPLE o NO CUMPLE.

4.1.5 CAPACIDAD OPERATIVA

No aplica.

4.1.6 OTRAS CONDICIONES TÉCNICAS VERIFICABLES

No aplica

4.2 CONDICIONES TÉCNICAS ADICIONALES DE CALIFICACIÓN Y SU JUSTIFICACIÓN

No aplica

4.3 EVALUACIÓN ECONÓMICA Y FINANCIERA

4.3.1 EVALUACIÓN ECONÓMICA

Los factores de evaulacion económico serán establecidos en el sobre numero 2 de la plataforma SECOP II

4.3.2 FACTORES ADICIONALES DE CALIFICACIÓN Y SU JUSTIFICACIÓN:

No aplica.

4.3.3 CRITERIOS DE DESEMPATE

En caso de empate entre dos o más ofertas, se escogerá al oferente que presentó el menor precio inicial, de conformidad con lo establecido en el numeral 9 del artículo 2.2.1.2.1.2.2 del Decreto 1082 de 2015.

Si persiste el empate, en cumplimiento de lo dispuesto en el artículo 35 de la Ley 2069 de 2020, se tendrán en cuenta, en cuanto sean aplicables, las siguientes reglas de desempate, de forma sucesiva y excluyente para adjudicar el proceso, así:

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

b) Preferir la propuesta de la mujer cabeza de familia, mujeres víctimas de la violencia intrafamiliar o de la persona jurídica en la cual participe o participen mayoritariamente; o, la de un proponente plural constituido por mujeres cabeza de familia, mujeres víctimas de violencia intrafamiliar y/o personas jurídicas en las cuales participe o participen mayoritariamente.
c) Preferir la propuesta presentada por el oferente que acredite en las condiciones establecidas en la ley que por lo menos el diez por ciento (10%) de su nómina está en condición de discapacidad a la que se refiere la Ley 361 de 1997. Si la oferta es presentada por un proponente plural, el integrante del oferente que acredite que el diez por ciento (10%) de su nómina está en condición de discapacidad en los términos del presente numeral, debe tener una participación de por lo menos el veinticinco por ciento (25%) en el consorcio, unión temporal o promesa de sociedad futura y aportar mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta.
d) Preferir la propuesta presentada por el oferente que acredite la vinculación en mayor proporción de personas mayores que no sean beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de edad de pensión establecido en la Ley.
e) Preferir la propuesta presentada por el oferente que acredite, en las condiciones establecidas en la ley, que por lo menos diez por ciento (10%) de su nómina pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitanas.
f) Preferir la propuesta de personas en proceso de reintegración o reincorporación o de la persona jurídica en la cual participe o participen mayoritariamente; o, la de un proponente plural constituido por personas en proceso de reincorporación, y/o personas jurídicas en las cuales participe o participen mayoritariamente.
g) Preferir la oferta presentada por un proponente plural siempre que: (a) esté conformado por al menos una madre cabeza de familia y/o una persona en proceso de reincorporación o reintegración, o una persona jurídica en la cual participe o participen mayoritariamente, y, que tenga una participación de por lo menos el veinticinco por ciento (25%) en el proponente plural; (b) la madre cabeza de familia, la persona en proceso de reincorporación o reintegración, o la persona jurídica aporte mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta; y (c) ni la madre cabeza de familia o persona en proceso de reincorporación o reintegración, ni la persona jurídica, ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural.
h) Preferir la oferta presentada por una Mipyme o cooperativas o asociaciones mutuales; o un proponente plural constituido por Mipymes, cooperativas o asociaciones mutuales.
i) Preferir la oferta presentada por el proponente plural constituido por micro y/o pequeñas empresas, cooperativas o asociaciones mutuales.
j) Preferir al oferente que acredite de acuerdo con sus estados financieros o información contable con corte a 31 de diciembre del año anterior, por lo menos el veinticinco por ciento (25%) del total de pagos realizados a Mipymes, cooperativas o asociaciones mutuales por concepto de proveeduría del oferente, realizados durante el año anterior; o, la oferta presentada por un proponente plural siempre que: (a) esté conformado por al menos una MIPYME, cooperativa o asociación mutual que tenga una participación de por lo menos el veinticinco por ciento (25%); (b) la MIPYME, cooperativa o asociación mutual aporte mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta; y (c) ni la MIPYME, cooperativa o asociación mutual ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural .
k) Preferir las empresas reconocidas y establecidas como Sociedad de Beneficio e Interés Colectivo o Sociedad BIC, del segmento MIPYMES.
l) Si persiste el empate, la Entidad convocará a una audiencia de sorteo mediante mensaje público, y se seleccionará en orden de elegibilidad mediante el procedimiento de sorteo por balotas al oferente que obtenga el mayor número.

Los factores de desempate serán aplicables en el caso de las cooperativas y asociaciones mutuales que cumplan con los criterios de clasificación empresarial, definidos por el Decreto 957 de 2019, priorizando aquellas que sean micro, pequeñas o medianas.

Para los criterios enunciados que involucren la vinculación de capital humano, el oferente deberá acreditar una antigüedad igual o mayor a un año. Para los casos de constitución inferior a un año se tendrá en cuenta a aquellos trabajadores que hayan estado vinculados desde el momento de constitución de la misma.

NOTA 1: la condición de mujer cabeza de familia se acreditará con la declaración ante notario de conformidad con lo previsto en el parágrafo del artículo 2 de la Ley 82 de 1993, modificado por el artículo 1° de la Ley 1232 de 2008 – «Por la cual se expiden normas para apoyar de manera especial a la mujer cabeza de familia» – establece que «La condición de Mujer Cabeza de Familia y la cesación de la misma, desde el momento en que ocurra el respectivo evento, deberá ser declarada ante notario por cada una de ellas, expresando las circunstancias básicas del respectivo caso y sin que por este concepto se causen emolumentos notariales a su cargo (...)».

NOTA 2: la condición de mujer víctima de violencia intrafamiliar se acredita con la medida de protección expedida por la autoridad competente de conformidad con lo dispuesto en el artículo 21 de la Ley 1257 de 2008 – «Por la cual se dictan normas de sensibilización, prevención y sanción de formas de violencia y discriminación contra las mujeres, se reforman los Códigos Penal, de Procedimiento Penal, la Ley 294 de 1996 y se dictan otras disposiciones» – , dispone que «Las situaciones de violencia que dan lugar a la atención de las mujeres, sus hijos e hijas, se acreditarán con la medida de protección expedida por la autoridad competente, sin que puedan exigirse requisitos adicionales».

NOTA 3: el proponente que desee acreditar que por lo menos el 10% de la nómina está en condición de discapacidad a que se refiere la Ley 361 de 1997, debe aportar la certificación expedida por el Ministerio de Trabajo, en la cual conste que el personal en condición de discapacidad lo contrató por lo menos con anterioridad a un año. Es importante tener en cuenta que, si el proponente adjudicatario se hizo acreedor a esta regla de desempate, el personal deberá mantenerse por un lapso igual al de la contratación. La constancia correspondiente emitida por el Ministerio de Trabajo deberá estar vigente en el momento en que la Entidad aplique los criterios de desempate.

NOTA 4: para acreditar la vinculación en mayor proporción de personas mayores que no sean beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de edad de pensión establecido en la Ley, el proponente deberá allegar certificación suscrita por el representante legal en la que se relacione el personal vinculado que cumple con estas condiciones indicando: 1) Nombre y apellidos, 2) Edad, 3) No de identificación, 4) Tipo de vinculación, 5) Fecha de vinculación. Igualmente deberá anexar copia de la cédula del personal relacionado y el contrato que soporta la vinculación.

NOTA 5: para acreditar que por lo menos el 10% de sus trabajadores pertenece a las poblaciones indígena, negra, afrocolombiana, raizal, el proponente deberá aportar certificación suscrita por el representante legal en la que se relacione la totalidad del personal vinculado y el personal vinculado que cumpla estas condiciones indicando: 1) Nombre y apellidos, 2) No de identificación, 3) Tipo de vinculación, 4) Fecha de vinculación. Igualmente, por cada persona que reúna estas condiciones deberá anexar copia de la cédula de ciudadanía, el contrato que soporta la vinculación y la acreditación que expide el Ministerio del Interior que acredita la pertenencia a estas poblaciones.

NOTA 6: la condición de persona en proceso de reintegración o reincorporación se acredita con la certificación que expedida la Agencia para la Reincorporación y la Normalización ARN.

NOTA 7: para acreditar que ni la madre cabeza de familia o persona en proceso de reincorporación o reintegración, ni la persona jurídica, ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural. El proponente deberá aportar certificación expedida por el representante legal del integrante del proponente plural que acredite tal condición.

NOTA 8: la condición de Mipyme se acreditará, conforme a lo dispuesto en el artículo 2.2.1.2.4.2.4 del del Decreto 1082 de 2015, con un certificado expedido por el representante legal y el revisor fiscal, si está obligado a tenerlo, o el contador, en el cual conste que la Mipyme tiene el tamaño empresarial establecido de conformidad con la ley.

NOTA 9: para la aplicación del criterio de desempate establecido en el literal j), el proponente deberá aportar los estados financieros o información contable con corte a 31 de diciembre del año anterior, que permita establecer tal circunstancia.

NOTA 10: para acreditar que ni la MIPYME, cooperativa o asociación mutual ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural. El proponente deberá aportar certificación expedida por el representante legal o el revisor fiscal (si tiene la obligación de tenerlo) del integrante del proponente plural que acredite tal condición.

NOTA 11: para acreditar la condición de Sociedad de Beneficio e Interés Colectivo BIC, bastará con el Certificado de Existencia y Representación Legal de la sociedad en la que se evidencie dicha denominación conforme al artículo 2° de la Ley 1901 de 2018.

5. CONDICIONES DEL CONTRATO

5.1. LUGAR DE ENTREGA

La entrega del objeto del presente proceso, se realizará en las instalaciones de la Oficina de Telemática de la Policía Nacional, ubicada en la Carrera 59 No. 26-21, (Bogotá- Colombia).

5.2. FORMA DE EJECUCIÓN

El oferente deberá entregar instalada y configurada la herramienta de acuerdo con las "ESPECIFICACIONES TÉCNICAS MÍNIMAS" establecidas en el presente estudio previo.

5.3. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de noventa (90) días calendario, previa aprobación de la garantía única, el cual debera quedar instaladas y configuradas la totalidad de las condiciones técnicas del Anexo "ESPECIFICACIONES TÉCNICAS MÍNIMAS".

5.4. FORMA DE PAGO

La Policía Nacional – Dirección Administrativa y Financiera cancelará el valor del contrato de la siguiente forma:

Se realizará un (01) sólo pago contra entrega total, en moneda legal colombiana, dentro de los sesenta (60) días calendario siguientes a la radicación de la factura, junto con el recibo a satisfacción del supervisor del

contrato y los demás documentos requeridos por la Dirección Administrativa y Financiera (cuando los elementos sean de origen extranjero se deberá aportar la declaración de importación), de acuerdo al derecho a turno y a la disponibilidad del Plan Anual de Caja (PAC).

Si los documentos en referencia no se reciben dentro del plazo establecido, o si recibidos son devueltos por inconsistencias tales como la falta de información o mal diligenciamiento de los mismos, la Policía Nacional - Dirección Administrativa y Financiera, programará el valor a cancelar una vez se hubieren subsanado las observaciones, se haya cumplido con el trámite documental dentro del plazo indicado y de acuerdo al derecho a turno y a la disponibilidad del Plan Anual de Caja (PAC).

5.5. SUPERVISOR

El supervisor del contrato será el jefe del Grupo de Seguridad de la Información de la Oficina de Telemática de la Policía Nacional o quien haga sus veces o quien con posterioridad designe el señor Director Administrativo y Financiero, quien verificará la ejecución idónea y el cumplimiento del objeto del contrato de acuerdo con las funciones asignadas para el efecto de la Resolución No. 00090 del 15 de enero de 2018.

El supervisor del contrato deberá presentar informes de supervisión mensual durante la ejecución del mismo además de los que le sean requeridos en la mencionada Resolución, informes que deberán ser cargados en la plataforma de SECOP II.

Email: ofite.jefat@policia.gov.co, teléfono: 601 5159140

5.6. OBLIGACIONES DEL CONTRATISTA

Las obligaciones del contratista están descritas en el Anexo "OBLIGACIONES DEL CONTRATISTA"

5.7. OBLIGACIONES DE LA POLICÍA NACIONAL

Las obligaciones de la Policía Nacional están descritas en el Anexo "OBLIGACIONES DE LA POLICÍA NACIONAL"

6. FORMA Y PROCEDIMIENTO DE ADJUDICACIÓN

La adjudicación del presente proceso de selección se realizará en forma total a través de subasta electrónica, el procedimiento de adjudicación será conforme lo establecido en la plataforma del SECOP II.

7. ESTIMACIÓN, TIPIFICACIÓN, ASIGNACIÓN DE RIESGOS Y DETERMINACIÓN DE GARANTÍAS.

De acuerdo al Manual para la Identificación y Cobertura de Riesgos en los Procesos de Contratación presentado por la Agencia Colombia Compra Eficiente, en el Anexo "ANÁLISIS DEL RIESGO y LA FORMA DE MITIGARLO", se establece la matriz que incluye los riesgos identificados en el proceso de contratación, de acuerdo con la clasificación, probabilidad de ocurrencia estimada, impacto, parte que debe asumir el riesgo, tratamientos que se pueden realizar y características de su monitoreo.

Como quiera que no se han realizado procesos de contratación con el mismo o similar objeto al del presente proceso en los años anteriores, la estimación del riesgo (probabilidad de ocurrencia del siniestro) corresponde a los porcentajes mínimos indicados dentro de la normatividad vigente, el Manual de Contratación para la Policía Nacional y las necesidades de la Institución, los cuales se encuentran en los Anexos "ESTIMACIÓN, TIPIFICACIÓN, ASIGNACIÓN DE RIESGOS Y DETERMINACIÓN DE GARANTÍAS"

II. ESTUDIO DEL SECTOR

1. ANÁLISIS DE LA DEMANDA

Se consultó en la página www.colombiacompra.gov.co, procesos con objeto igual y/o similar al presente estudio previo durante las vigencias 2019, 2020 y 2021 celebrados por la Policía Nacional, y se encontró lo siguiente:

DESCRIPCIÓN	VIGENCIA 2020
MODALIDAD DE SELECCIÓN DEL CONTRATISTA	SELECCIÓN ABREVIADA
NÚMERO Y OBJETO DEL CONTRATO	06-2-10124-20 SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM.
CANTIDAD DEL BIEN, OBRA O SERVICIO	1
AUTORIZACIONES PERMISOS Y LICENCIAS REQUERIDAS PARA SU EJECUCIÓN	NO APLICA
VALOR DEL CONTRATO	$1.242´000.000,00 en pesos colombianos
FORMA DE PAGO- CONDICIONES DE PAGO ESTABLECIDAS	La Policía Nacional – Dirección Administrativa y Financiera cancelará el valor del contrato de la siguiente forma: Se realizará un (01) solo pago contra entrega total, en moneda legal colombiana, dentro de los sesenta (60) días calendario siguientes a la radicación de la factura, junto con el recibo a satisfacción del supervisor del contrato y los demás documentos requeridos por la Dirección Administrativa y Financiera (cuando los elementos sean de origen extranjero se deberá aportar la declaración de importación), de acuerdo al derecho a turno y la disponibilidad del Plan Anual de Caja (PAC). Si los documentos en referencia no se reciben dentro del plazo establecido o, si recibidos son devueltos por inconsistencias tales como la falta de información o mal diligenciamiento de los mismos, la Policía Nacional - Dirección Administrativa y Financiera, programará el valor a cancelar una vez se hubieren subsanado las observaciones, se haya cumplido con el trámite documental dentro del plazo indicado y de acuerdo al derecho a turno y la disponibilidad del Plan Anual de Caja (PAC).
PRESUPUESTO CON CARGO AL CUAL SE HAN SIDO EJECUTADOS	RECURSO 11
OFERENTES QUE HAN PARTICIPADO EN EL PROCESO	ONA SYSTEMS S.A.S
COMPORTAMIENTO DE LOS CONTRATISTAS E IMPOSICIÓN DE SANCIONES	SIN INCONVENIENTES
LUGARES DE ENTREGA ACORDADOS	EL CONTRATISTA DEBERÁ ENTREGAR LOS COMPONENTES DE ACUERDO CON EL ANEXO No. 2 ESPECIFICACIONES TECNICAS MÍNIMAS.
GARANTÍAS EXIGIDAS Y SINIESTROS	CUMPLIMIENTO DEL CONTRATO CALIDAD DE LOS BIENES
VIGENCIA DEL CONTRATO (PLAZO DE EJECUCIÓN)	El plazo de ejecución del contrato será de 90 días calendario, previa aprobación de la garantía única, plazo en el cual deberán quedar instaladas y configuradas la totalidad de las condiciones técnicas del Anexo No. 2
LINK O NUMERO DE PROCESO	PN DIRAF SA 130 2020

Nota: para las vigencias 2019 y 2021, no se encontraron procesos contractuales iguales y/o similares para la adquisición de solución software antivirus, data lost prevention, control de aplicaciones, cifrado y antispam, que hayan sido realizados por la entidad.

2. ANÁLISIS DEL MERCADO

DESCRIPCIÓN DEL MERCADO

Evaluando el mercado actual de empresas que pueden ofertar los bienes requeridos, se verificó que el número de éstas es amplio y que estarían en condiciones de participar en el proceso de contratación de los bienes necesarios para llevar a cabo el objeto del contrato, sin embargo debido a que los bienes a adquirir tienen componentes de hardware y software de procedencia nacional o extrajera es posible que su participación se

realice en asociación ya sea de fabricantes y/o comerciantes y/o distribuidores con empresas desarrolladoras e integradoras.

En el mercado nacional operan organizaciones individuales que prestan servicios en Tecnologías de la Información (TI) para mejorar la eficiencia y calidad de procesos internos con actividades de bajo valor como la gestión de información y datos a través de productos y servicios para hacerlos más sofisticados y eficientes.

Los "mercados finales" para el sector de software, hardware y servicios se enfocan en el cubrimiento de la demanda para mejorar procesos, productos y la interrelación entre proveedores de servicios y sus consumidores a través de plataformas que permitan nuevas formas de prestación de estos.

Los anteriores enfoques se deben a que las organizaciones, empresas o administraciones, modernizan sus procesos con las Tecnologías de la Información. Con relación a este eje de aplicación de las TI, todas las organizaciones son potencialmente mercados relevantes ya que todas las organizaciones demandan la mejora de calidad y productividad de sus procesos empresariales.

El Gobierno está comprometido a apoyar y dar impulso al sector de servicios por medio del Programa de Transformación Productiva, como una estrategia consolidada para su fomento y crecimiento, que en los últimos años han generado un ambiente adecuado para su reconocimiento a nivel mundial.

OPORTUNIDADES EN LA INDUSTRIA LOCAL

El sector financiero es en términos de la demanda de servicios tercerizados uno de los más dinámicos a partir del objetivo del Gobierno de bancarización masiva, que permite a los usuarios el uso de la tecnología para manejar sus finanzas; dicha tendencia ha generado múltiples oportunidades para la prestación de servicios de Backoffice y Call Center en el país.

Esto ha permitido a Colombia convertirse en un hub de distribución de servicios de tercerización y Servicios de TI y Software a nivel regional. A través de una expansión sostenida del sector de la salud, y la creciente demanda de la población (47 millones) que necesita cada vez más un respaldo de servicios en áreas de seguimiento a pacientes (Telemedicina) y consolidación de información (Data Entry). Los sectores de gas y petróleo demandan cada vez más servicios relacionados con el soporte de operación, control de pozos y perforación, extracción de petróleo y los procesos de transporte para sus actividades diarias.1

1http://proyectos.andi.com.co/camarabpo/Inversin%20en%20el%20sector%20de%20servicios%20en%20Colombia%20%20PR/Inversión%20en%20el%20sector%20BPO%202015.pdf

INNOVACIÓN Y APERTURA DE DIVERSOS MERCADOS

Para muchos analistas a nivel nacional e internacional es cada vez más claro que el desarrollo económico es impulsado por la innovación, el conocimiento y el cambio tecnológico. Desde hace varios años se habla de la necesidad de pasar de ventajas comparativas, generalmente asociadas a una dotación de factores o de recursos naturales de un país, a la construcción de ventajas competitivas, a través de mejoras en los niveles de productividad, que permiten ganar espacios en los mercados internacionales (Porter, 1990). Esto ha llevado a cambios importantes en la teoría del comercio internacional: inicialmente esta se basaba en el argumento que el comercio a nivel internacional se daba entre países que producían productos diferentes, precisamente con base en las ventajas comparativas de cada economía (Hanink, 1994). Desde hace un par de décadas se argumenta, con base en los patrones observados en el comercio internacional, que la mayor parte del intercambio en la economía mundial se da realmente entre países que producen productos similares, y que dicho intercambio se basa en diferencias en productividad asociados a innovación, conocimiento y cambio tecnológico (Porter, 1990; Hanink, 1994; Krugman, 1997). 2

2 http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-49932013000100009

Panorama Regulatorio Hardware y Software 2016 – 2017

El tejido empresarial del sector de tecnología en Colombia ha registrado un crecimiento de 44% desde 2016, generando alrededor de 155.000 empleos y ventas aproximadas de $30 billones. Las ventas reales de equipos de informática y comunicaciones en establecimientos especializados en el mes de octubre de 2021 tuvieron una variación positiva de 72,8% frente al mismo mes de 2019. La demanda de los servicios de software y hardware se incrementó durante la cuarentena, ya que esta situación obligó a que las personas interactuaran más a través de dispositivos y plataformas digitales, favorecida por la aceleración de la transformación digital para atender las nuevas demandas de los usuarios. 3

3 https://www.sectorial.co/articulos-especiales/item/496797-ficha-hardware-software-2021

3. ANÁLISIS DE LA OFERTA

IDENTIFICACIÓN DEL PROVEEDOR

Todas las personas naturales o jurídicas, nacionales o extranjeras, con apoderado o representante legal en Colombia, domiciliadas o con sucursal en Colombia, en forma individual o conjunta (consorcio ó unión temporal), que tengan dentro de su objeto social o actividad la fabricación y/o comercialización y/o distribución autorizada por la casa fabricante de los bienes objeto del presente proceso, siempre y cuando cumplan con todos los requisitos exigidos para el mismo y se encuentren registradas en el SECOP II.

DIRECTORIO DE SECOP II

https://community.secop.gov.co/Directory/CompanyProfiles/Network/Index

Consultado el directorio del SECOP II de las empresas del segmento: Software de seguridad y protección, equipo informático y accesorios, Software, bajo el código UNSPSC 43233200, se encuentran inscritas 904 firmas de origen colombiano, 01 de Japón, 01 de Costa Rica y 01 de Eslovaquia.

consulta realizada el 13/06/2022.

INDICADORES FINANCIEROS

El señor Teniente Coronel OMAR LEONARDO VILLALOBOS RINCÓN, Jefe Contaduría General, el 06 de junio de 2022, mediante oficio electrónico No GS-2022-019120-DIRAF-COGEN -3.1, informa el resultado del análisis del sector con cifras financieras, así:

En atención al oficio de asunto, de manera atenta y respetuosa me permito remitir el resultado del análisis del sector realizado al proceso de "SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST RREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM", esto para tener en cuenta y anexar al estudio previo, así:

1. Consideraciones

- Normativas

a. Decreto 1082 de 2015, artículos 2.2.1.1.1.6.1 y 2.2.1.1.1.53 numerales 3 y 4

b. Guía para la elaboración de Estudios del Sector versión G-EES-02

c. Manual para determinar y verificar los requisitos habilitantes en los procesos de contratación versión MDVRHPC-05

• La información financiera que se tomará para el presente análisis del sector será con cifras 2020 y proviene de fuentes fidedignas tomadas del Registro Único Empresarial y Social de la Superintendencia de sociedades RUES, fundamentados en el Decreto No. 579 del 31 de mayo de 2021 y el concepto C – 288 de 2021 emitido por Colombia Compra Eficiente, así:

"*Dentro de los requisitos habilitantes se destaca la «capacidad financiera» y la «capacidad organizacional». **La entidad, como responsable de la estructuración de su procedimiento de selección, es autónoma para requerir la capacidad financiera y la capacidad organizacional necesarias, de acuerdo con la naturaleza del contrato que se pretende suscribir y a su valor**. Para esto, la entidad, según el artículo 2.2.1.1.1.6.2. del Decreto 1082 de 2015, debe tener en cuenta el estudio del sector y sus componentes, como por ejemplo la identificación de riesgos, así como el precio del bien, obra o servicio a contratar*" (resaltado y subrayado fuera de texto).

• Es de anotar que de acuerdo a lo indicado en la introducción de la Guía para la elaboración de Estudios del Sector versión G-EES-02 se indica en la parte introductoria que ***"El resultado del análisis debe plasmarse en los estudios y documentos previos del Proceso de Contratación."*** (resaltado y subrayado fuera de texto).

2. Elaboración de Estudios:

Patrullera LORENA MARCELA BARRETO TOCARRUNCHO, adscrita a la Oficina de contaduría General Policía Nacional quien realiza el análisis del sector.

3. Metodología y Resultado del Análisis de los Indicadores de Orden Financiero (Índice de liquidez, Cobertura de Intereses) y de Orden Organizacional (Rentabilidad del Patrimonio, Rentabilidad del activo)

La metodología utilizada está sustentada en los manuales y guías elaborados por la Agencia Nacional de Contratación Pública, Colombia Compra Eficiente; partiendo de la obligatoriedad de tener en cuenta los 5 indicadores de orden financiero y organizacional, se tomó información financiera de 10 empresas del sector, ubicadas diez (10) en la Ciudad de Bogotá D.C, las cuales pertenecen al sector de los bienes y/o servicios requeridos; análisis que se realizo mediante la aplicación de seis medidas o promedios estadísticos, así:

a. **Media Aritmética**: para la cual se tuvo en cuenta las diez (10) empresas y se aplicó el promedio ponderado en forma directa.

b. **Media podada**: para la aplicación de esta medida no se tuvieron en cuenta los datos atípicos de cada extremo, es decir el más bajo y el más alto, razón por la cual se tuvo en cuenta ocho (8) y siete (7) empresas por cada indicador, para obtener un resultado objetivo, equilibrado y lineal.

c. **Mediana:** se aplica en forma directa y corresponde a la posición central de cada indicador dentro de las diez (10) empresas de la muestra poblacional.

d. **Mínimo**: promedia el valor del indicador de los diez (10) oferentes asignando el límite inferior, excluyendo los valores en cero (0,00), negativos e indeterminados.

e. **Máximo**: promedia el valor del indicador de los diez (10) oferentes asignando el límite superior.

f. **Promedio Ponderado**: este se aplica ponderando las anteriores medidas estadísticas por cada uno de los indicadores.

Cantidad de proponentes	Índices Capacidad organizacional		Índices Capacidad Financiera	
	Rentabilidad del patrimonio	Rentabilidad del activo	Índice liquidez	Cobertura de Interés
1	0.22	0.17	7.43	16.40
2	0.16	0.08	2.49	3.80
3	0.15	0.06	1.63	3.18
4	0.51	0.24	2.07	22.13
5	0.39	0.14	1.60	INDETERMINADO
6	0.49	0.16	1.27	INDETERMINADO
7	0.41	0.34	9.81	498.88
8	0.22	0.09	1.93	9.48
9	0.03	0.02	3.59	1.53
10	0.47	0.18	1.43	151.21
a. Media Aritmética	0.31	0.15	3.33	70.66
b. Media podada	0.31	0.14	2.77	100.73
c. Mediana	0.31	0.15	2.00	12.94
d. Mínimo	0.03	0.02	1.27	1.53
e. Máximo	0.51	0.34	9.81	498.88
f. Promedio Ponderado	0.29	0.16	3.84	136.95

La asignación de los límites para cada requisito habilitante de orden financiero y organizacional se adopta la medida estadística del Mínimo, cuando el indicador sea cero y/o indeterminado procederá al siguiente ascendentemente a fin de dar libertad en la participación de las empresas que permita mayor pluralidad sin que ponga en riesgo el objeto del proceso y su cuantía para la ejecución fiscal del mismo; para el caso de a cobertura de interés se tomara el mínimo entero en adelante.

4. Metodología y Resultado del Análisis del Indicador de orden Financiero Razón de endeudamiento

Partiendo del resultado obtenido del valor absoluto para cada empresa según metodología anterior se procede a realizar un análisis individual por empresa mediante la aplicación del gráfico de **TALLOS Y HOJAS**. Para en forma posterior aplicar medidas estadísticas como lo son el promedio ponderado, la mediana, la desviación estándar, la media podada.

GRAFICO TALLO Y HOJAS											
Muestra Poblacional	Tallo	Hojas	Bajo, medio y alto nivel de endeudamiento	Mayoría de oferentes están en este rango	Promedio de las 10 muestra poblacional	Mediana	Desviación estándar	Mediana podada 8 ítems de 10	Desviación estándar de la mediana podada	Razón de endeudamiento por encima o debajo de la media podada frente a la desviación estándar	Valor ideal o Límite fijado al indicador
16	0										
24	1	6	16								
32	2	4									
50	3	2									
52	4										

55	5	0258	50 Y 58	50 Y 58	47	54	16	49	13	Entre (49-13)=36 y (49+13)=62	62%
58	6	016									
60	7		66								
61	8										
66	9										

El gráfico anterior permite observar la concentración de los datos delimitando los valores más y menos frecuentes. Los menos frecuentes son los ubicados en los extremos del gráfico y corresponden a aquellos proveedores que tienen un bajo o alto índice de endeudamiento (16% y 66%). Los más frecuentes corresponden a los proveedores que tienen un índice de endeudamiento entre el 50% y 58%. Este último representa el rango donde se encuentra la mayoría de los datos.

Basados en el análisis estadístico se define un índice de endeudamiento máximo de 62%, teniendo en cuenta que es el límite superior de la media podada más dos veces la desviación estándar podada, siendo acorde con el sector económico y la naturaleza del Proceso de Contratación incluyendo los Riesgos, la complejidad y valor del contrato.

5. Consolidado de los 5 indicadores de orden financiero y organizacional

LIMITES DE ORDEN FINANCIERO Y ORGANIZACIONAL				
Rentabilidad del patrimonio	Rentabilidad del activo	Índice liquidez	Razón de endeudamiento	Cobertura de Intereses
>=0,03	>=0,02	>=1,27	<=0,62	>=1,53

Conclusiones y Notas

De todo lo anterior se concluye que los límites fijados a cada indicador son el resultado no solo de la aplicación de fórmulas financieras y estadísticas, sino que también respaldan los dos objetivos principales del Decreto 1082 de 2015, garantizar la pluralidad de oferentes y minimizar el riesgo para la Entidad; se precisa que el resultado del análisis debe tomarse en su integralidad para la estructuración del dueño de la necesidad.

Finalmente, es preciso indicar que se debe realizar la respectiva evaluación económica, basados en el Decreto No. 579 del 31 de mayo de 2021 y el concepto C – 288 de 2021 emitido por Colombia Compra Eficiente, donde se toma en cuenta el mejor año fiscal que se refleje en el registro de cada proponente en atención, así:

"Como el certificado del RUP debe contener la información financiera y organizacional del proponente correspondiente a los últimos tres años o al período transcurrido desde su primer cierre fiscal, según el caso, al momento de evaluar tales indicadores las entidades estatales deberán tener en cuenta «el mejor año fiscal» que refleje el registro. Por «mejor año fiscal» se interpreta la información relativa al año apreciada en su conjunto, o sea, de manera integral, que permita al proponente cumplir los requisitos habilitantes de capacidad financiera y organizacional. Dicho de otro modo, cuando el parágrafo transitorio del artículo 2.2.1.1.1.6.2, adicionado por el artículo 6 del Decreto 399 de 2021, y sustituido por el artículo 3 del Decreto 579 de 2021, establece que « […] las Entidades Estatales evaluarán estos indicadores, teniendo en cuenta el mejor año fiscal que se refleje en el registro de cada proponente», significa que deben examinar los años certificados en el RUP y escoger para ser evaluado el que refleje mejores indicadores de capacidad financiera y

organizacional, que permita al proponente cumplir los requisitos habilitantes de capacidad financiera y organizacional.

Por lo tanto, el parágrafo transitorio, agregado al artículo 2.2.1.1.1.6.2. del Decreto 1082 de 2015 por el artículo 6 del Decreto 399 de 2021 y sustituido por el artículo 3 del Decreto 579 de 2021, no exige que las entidades estatales tengan en cuenta el mejor año por cada indicador ; verbigracia, el mejor año para el índice de liquidez, el mejor año para el índice de endeudamiento o el mejor año para la rentabilidad del patrimonio. Atendiendo a la teleología del Decreto 399 de 2021, por «mejor año» debe entenderse aquel en el que, analizados conjuntamente todos los indicadores de capacidad financiera y organizacional, el proponente podría cumplir con dichos requisitos habilitantes. Ahora bien, del hecho de que la entidad estatal deba evaluar los indicadores de capacidad financiera y organizacional teniendo en cuenta el «mejor año fiscal», no se infiere que el proponente siempre cumplirá tales requisitos habilitantes, pues, precisamente, ese es el análisis que deberá hacer la entidad pública con la información disponible en el RUP"

INDICADOR	FÓRMULA	CRITERIO DE SELECCIÓN
Liquidez	Activo corriente sobre pasivo corriente	>= 1,27
Nivel de Endeudamiento	Pasivo total sobre activo total	<= 0,62
Razón cobertura de intereses	Utilidad operacional dividida por los gastos de intereses	>=1,53
Rentabilidad del patrimonio	Utilidad operacional dividida por el patrimonio	>= 0,03
Rentabilidad del activo	Utilidad operacional dividida por el activo total	>= 0,02

4. MONEDA A CONTRATAR

La contratación se efectuará en moneda legal colombiana (pesos colombianos).

5. ANÁLISIS DE PRECIOS

Para realizar el análisis de precios es necesario tener en cuenta los precios referencia de los siguientes aspectos:

- Precios referencia SECOP (otras entidades)
- Precios históricos (anteriores contrataciones: Policía Nacional).
- Precios de catálogo o portales web.
- Precios del mercado (cotizaciones).
-

5.1. PRECIOS REFERENCIA SECOP (OTRAS ENTIDADES)

Se realizó consulta en la página www.colombiacompra.gov.co, para los años 2019, 2020 y 2021, encontrado publicaciones de contratos de otras entidades, con objeto igual o similar al requerido en el presente estudio previo.

ENTIDAD CONTRATANTE Y CONTRATISTA	OBJETO	NÚMERO DEL CONTRATO Y FECHA DE SUSCRIPCIÓN	NÚMERO DE PROCESO	VALOR
Servicio Geológico Colombiano	Contratar la adquisición y renovación de licencias para la solución Mcafee del SERVICIO GEOLÓGICO COLOMBIANO.	SASI 16 DE 2019 16/07/2019	SASI 16 DE 2019	$ 793.998.333,00

Rama Judicial – Dirección Ejecutiva de Administración Judicial	Renovar licencias de antivirus para los equipos de cómputo de propiedad de la rama judicial a nivel nacional.	SI-12-2020 22/12/2020	SI-12-2020	$ 1.378.549.478,00
Agencia para la Reincorporación y la Normalización	Contratar la renovación de las licencias del antivirus actual de la alcaldía distrital de santiago de cali, junto con la adquisición de las licencias adicionales, requeridas para la protección de los equipos de cómputo y servidores que conforman la infraestructura tecnológica a cargo del departamento administrativo de las tecnologías de la información y las comunicaciones (datic)	4134.010.26.1.0418 18/11/2021	4134.010.26.1.0418	$ 1.806.000.000,00

- **Información verificada y aprobada por los funcionarios dueños de la necesidad que firman el presente estudio previo.**

Nota: No se tendrá en cuenta los precios en referencia en SECOP II, debido a que varían factores importantes como: especificaciones técnicas mínimas requeridas, cantidad, capacidad de equipo, la fluctuación del dólar el cual encarecen los de productos tecnológicos.

5.2. PRECIOS HISTÓRICOS

Se realizó consulta en la página www.colombiacompra.gov.co, para los años 2019, 2020 y 2021, encontrándose el contrato PN DIRAF 06-2-10124-20 con objeto similar al requerido en el presente estudio previo, así:

UNIDAD CONTRATANTE Y CONTRATISTA	NÚMERO DEL CONTRATO Y FECHA DE SUSCRIPCIÓN	OBJETO	FECHA	VALOR TOTAL EXENTO DE IVA	VALOR UNITARIO PROYECTADO CON IPC (1,6%)	VALOR UNITARIO PROYECTADO CON IPC (5,62%)
POLICÍA NACIONAL DIRAF ONA SYSTEMS S.A.S	PN DIRAF 06-2-10124-20 07/10/2020	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM.	PN DIRAF SA 130 2020	$ 1.242.000.000,00	$ 1.261.872.000,00	$ 1.332.789.206,04

No se tiene en cuenta el precio histórico toda vez que se evidencia que la información del contrato antes relacionado varía en características técnicas estos requerimientos, no incluye control de aplicaciones que para este proceso será instalado en dieciocho mil (18.000) nodos, adicionalmente difieren la vigencia del soporte y actualizaciones, el proceso actual contempla dieciocho (18) meses de actualizaciones y soporte, por último las amenazas mutan en el tiempo y hacen que las especificaciones técnicas incluyan características técnicas específicas para infecciones de malware que se presentan en la actualidad, por tal razón, no se tendrá en cuenta el valor histórico.

- **Información verificada y aprobada por los funcionarios dueños de la necesidad que firman el presente estudio previo.**

5.3. PRECIOS DE CATÁLOGO O PORTALES WEB

Teniendo en cuenta que el servicio descrito en el presente estudio no se encuentra en las plataformas de grandes marcas o grandes superficies, toda vez que tienen unas características específicas en cuanto a actividades, tiempo, metodología, personal profesional, estas plataformas virtuales no cuentan con esta clase de servicio, por tal motivo no se pueden adquirir o verificar sus precios a través de un catálogo virtual. Así mismo se verificó la tienda virtual del estado colombiano https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano en la cual se establece que esta clase de servicios no está incluido en el catálogo virtual o en proceso de virtualización.

- **Información verificada y aprobada por los funcionarios dueños de la necesidad que firman el presente estudio previo.**

5.4. PRECIOS DE MERCADO

Con el fin de obtener los precios del mercado, se procedió a solicitar cotización mediante comunicación oficial S/N OFITE-GRUSI 29.25 del 27/05/2022, la cual se cargo al SECOP II, el día 27/05/2022 bajo el código (id.CO1.BDOS.2952178), y proceso: SOLUCION SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM cotizando las siguientes empresas:

ÍTEM	DESCRIPCIÓN	COTIZACIÓN No. 1 ONA SYSTEMS	COTIZACIÓN No. 2 M.S.L. DISTRIBUCIONES & CIA S.A.S	COTIZACIÓN No. 3 Nemesis Asociados S.A.	MENOR VALOR COTIZADO EXENTO DE IVA
1	SOLUCION SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM	**$ 1.400.000.000,00**	**$ 4.203.080.000,00**	**$ 1.478.935.200,00**	**$ 1.400.000.000,00**

Nota 1: en atención al mensaje de referencia CO1.AMD.1405200 publicado el 31/05/2022, informando a las empresas la actualización especificaciones y ampliación plazo de cotizacion.

Nota 2: se realizó mensaje CO1.AMD.1406650 publicado el 01/06/2022, informado a las empresas de la actualización ficha técnica.

Nota 3: se realizó mensaje de aclaración de cotización a la empresa ONA SYSTEMS, mediante mensaje de referencia CO1.MSG.3768802 en el cual se solicita que la vigencia de la cotizacion sea de 90 dias calendario, obteniendo respuesta mediante mensaje de referencia CO1.MSG.3769026, frente a la actualización.

Nota 4: se realizó mensaje de aclaración de cotización a la empresa M.S.L Distribuciones y CIA S.A.S, mediante mensaje de referencia CO1.MSG.3768823 en el cual se solicita que se actualice el valor de la cotización sin IVA, en la cual no se obtuvo respuesta.

- **Información verificada y aprobada por los funcionarios dueños de la necesidad que firman el presente estudio previo.**

5.5 ANÁLISIS DEL VALOR ESTIMADO

ÍTEM	DESCRIPCIÓN	PRECIO SECOP	PRECIOS DE CATÁLOGO	PRECIOS HISTÓRICOS PROYECTADOS	PRECIOS DE MERCADO	VALOR ESTIMADO EXENTO DE IVA
1	SOLUCION SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM	N/A	N/A	N/A	$ 1.400.000.000,00	$ 1.400.000.000,00
VALOR TOTAL		N/A	N/A	N/A	**$ 1.400.000.000,00**	**$ 1.400.000.000,00**

El análisis del valor estimado se obtiene del menor valor, producto de la comparación de las cotizaciones allegadas las cuales cumplen con las especificaciones y requerimientos de la entidad.

- **Información verificada y aprobada por los funcionarios dueños de la necesidad que firman el presente estudio previo.**

5.6 VALOR ESTIMADO DE LA CONTRATACIÓN

El valor estimado para el presente proceso de contratación es de MIL CUATROCIENTOS MILLONES DE PESOS MONEDA LEGAL ($1.400.000.000,00) EXENTO DE IVA, discriminado de la siguiente manera:

ÍTEM Y/O LOTE	RUBRO Y DESAGREGACIÓN PRESUPUESTAL	RECURSO	DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO ESTIMADO EXENTO DE IVA	VALOR TOTAL ESTIMADO EXENTO DE IVA
1	1501-0100-22-0-1501037-02	11	SOLUCION SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM	1	$1.400.000.000,00	$1.400.000.000,00
					VALOR TOTAL ESTIMADO	$1.400.000.000,00

Nota 1: los elementos de acuerdo a su utilización, desde el componente técnico se encuentran catalogados por la Oficina de Telemática en el numeral 3 literal n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional, del artículo 188 de la Ley 1819 del 29/12/2016, el cual modificó el artículo 477 del Estatuto Tributario, son bienes que están exentos del impuesto sobre las ventas.

Patrullero **JOJAN DANIEL PRADO FULA**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Patrullero **WILMER ALEXANDER BARACALDO CIFUENTES**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Intendente **ALEXANDER DIAZ CASTILLO**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Teniente **ANA CATHERINE MARIÑO RINCÓN**
Jefe Grupo Seguridad de la Información
Estructurador Estudio Previo

Coronel **CARLOS ALBERTO BENITEZ ROJAS**
Jefe Oficina de Telemática

Documentos Anexos al Estudio Previo:

Los documentos seleccionados en la siguiente lista, aplican para el proceso de Selección Abreviada con Subasta Inversa cuyo objeto es la "SOLUCION SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM"

Aplica	**Anexos**
■	Certificación de la necesidad
■	Especificaciones técnicas mínimas
☐	Constancia de idoneidad y experiencia
■	Estimación, tipificación, asignación de riesgos y determinación de garantías
■	Análisis del riesgo y forma de mitigarlo.
■	Ficha técnica
■	Obligaciones de la Policía Nacional
■	Obligaciones del contratista
☐	Factores de verificación y ponderación.

Aplica	**Formularios adjuntos al estudio previo**
☐	Carta de presentación de la propuesta
☐	Apoyo a la industria nacional
☐	Indicación de trato nacional
■	Experiencia del proponente
■	Certificación de contratos para acreditación de experiencia proponente extranjero sin sucursal o domicilio en Colombia
■	Clasificación proponente extranjero
■	Acuerdo de confidencialidad
■	Sistema de gestión de la seguridad y salud en el trabajo
■	Compromiso anticorrupción
■	Capacidad financiera
☐	Certificación de compromiso del fabricante y/o oferente
☐	Certificación de la capacidad técnica
☐	Personal, experiencia y tiempos de dedicación mínimos
☐	Carta de compromiso postventa

Otros documentos adjuntos al Estudio Previo

- ■ Certificación plan anual de adquisiciones de inversión No. 057 del 27/01/2022
- ■ Viabilidad técnica comunicado Oficial GS-2022-004681-OFITE del 07/06/2022, acta 245 del 07/06/2022.
- ■ Certificación Comercio Exterior del 06 de Junio de 2022
- ■ Concepto Ambiental
- ■ Solicitud de Cotizaciones No. PN DIRAF 009-2022 bajo el código CO1.DBOS.2952178.
- ■ Cotizaciones empresas
- ■ Respuesta a solicitud indicadores financieros GS-2022-019120-DIRAF
- ■ Oficio comité técnico, jurídico y económico GS-2022-004920-OFITE

En mí calidad de Jefe Almacén de Telemática de la Policía Nacional, manifiesto con la suscripción de esta CERTIFICACIÓN, que, consultando el inventario de bienes de los almacenes, no hay existencias de equipos para satisfacer la necesidad de "SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOSS PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM.", por tal razón la única forma de resolver la carencia es mediante la adquisición de estos bienes.

ÍTEM	DESCRICIÓN	NECESIDAD REAL	CANTIDAD ADQUIRIR	DÉFICIT
1	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM.	1	1	0

Intendente **RONAL ANDRES SALAS PEÑA**
Jefe Almacén de Oficina de Telemática de la Policía Nacional

PÁGINA EN BLANCO

Las especificaciones técnicas mínimas requeridas son de obligatorio cumplimiento (excluyentes), por tal motivo el proponente deberá indicar con una "X" y de no hacerlo, la propuesta se considerará no apta técnicamente y debe diligenciarse con las especificaciones técnicas ofertadas.

En una columna CUMPLE/NO CUMPLE, el comité técnico de la Policía Nacional designe, evaluara las especificaciones técnicas ofertadas por la firma.

El oferente deberá cumplir estrictamente con las especificaciones solicitadas atendiendo los factores descritos a continuación:

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
1.	**LA SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM**		
1.1	El contratista deberá suministrar una (1) solución con soporte para cuarenta y cinco mil (45.000) equipos de cómputo (que soporte Sistema Operativo Windows, Linux y Macintosh) para uso continuo con derecho a actualizaciones y nuevas versiones (upgrade) por un término de dieciocho (18) meses y que cumpla las siguientes características: • Cuarenta y cinco mil (45.000) deben contar con módulo de Antivirus, Control de Dispositivos, Control de Aplicaciones y Data Lost Prevention (DLP) • Quince mil (15.000) debe contar con módulo de y Cifrado de Disco Duro • Veinte mil (20.000) de antispam para buzones de correo on-premise. La funcionalidad de la consola de administración antivirus, funcionalidad modulo antivirus en Windows server y Linux, La solución para estaciones de trabajo deben ser cumplidas por las cuarenta y cinco mil (45.000) licencias, estas deben ser administradas desde ambientes web, la diferencia en módulos se debe a las funcionalidades de cada uno de los equipos de cómputo, sus sistemas operativos y el nivel de riesgo al que se encuentran expuestos.		
	2. MÓDULO ANTIVIRUS Y CONTROL DE DISPOSITIVOS		
2.1	La solución debe ser desplegada mediante un agente.		
2.2	La protección antivirus debe tener compatibilidad con los sistemas operativos Windows, Linux y Macintosh, incluyendo las nuevas versiones y estaciones de trabajo (45.000), incluyendo servidores de archivos Linux y una herramienta de administración y gestión remota, adicionalmente la solución deberá realizar la identificación de equipos no gestionados y la instalación de la solución en los mismos.		
2.3	El módulo debe ser instalado en cuarenta y cinco mil (45.000) nodos, configurado y deberá quedar funcionando correctamente en los servidores Windows, Linux, así como en los clientes Windows, Linux en las versiones de 32 y 64 bits y Macintosh en las diferentes versiones con los que cuenta la Policía Nacional.		
2.4	La solución de antivirus debe ser además compatible con sistemas Linux CentOS, RedHat, SUSE y Ubuntu.		
2.5	Las políticas de antivirus definidas desde la consola deben poder ser aplicables para cualquier sistema operativo soportado. No se aceptará tener que definir políticas diferentes para diferentes sistemas operativos.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
2.6	La solución debe contar con un mecanismo de actualización que garantice la integridad y minimice la manipulación o alteración de las definiciones de virus por medio de cifrado y firmas digitales. Esta función deberá ser implementada y estabilizada en la solución para la Policía Nacional.		
2.7	La solución debe contar con tecnología de remoción y detección de virus, macros, troyanos, gusanos, ransomware y en general todo tipo de códigos maliciosos. Esta función deberá ser implementada y estabilizada en la solución para la Policía Nacional.		
2.8	El antivirus deberá ser estable, de tal manera que no afecte ni perjudique el rendimiento de las máquinas y/o aplicativos que estén instalados en las mismas, la solución se debe instalar y en máquinas con recursos limitados.		
2.9	La solución debe permitir el aseguramiento de archivos, carpetas, elementos compartidos y evitar el desbordamiento de buffer. Esta función deberá ser implementada y estabilizada en la solución para la Policía Nacional.		
2.10	La solución debe permitir el acceso en demanda, en segundo plano, proactivo, subsistema de prevención de brotes de virus y filtrado de contenido, protección sobre los protocolos HTTP, HTTPS, FTP y SMTP.		
2.11	La solución debe contar y quedar configurado con un módulo de exploración en tiempo real, que ofrezca protección continúa frente a los virus que llegan a través de dispositivos de almacenamiento extraíbles, en la red y de las diversas fuentes en Internet.		
2.12	La solución debe tener la capacidad de explorar los procesos que se encuentren corriendo en memoria.		
2.13	La solución debe tener el control de la utilización de la CPU para tareas de exploración en demanda.		
2.14	La solución debe explorar múltiples formatos de compresión de archivos como: (zip, rar, tar, gzip entre otros).		
2.15	La solución debe permitir y quedar configuradas tareas calendarizadas de revisión y limpieza del sistema de archivos.		
2.16	La solución debe tener la capacidad de analizar Scripts de Java y VBScript antes de que se ejecuten.		
2.17	El antivirus debe contar con un módulo de exploración bajo demanda que permita iniciar una exploración en cualquier momento, especificar los objetivos (discos duros, carpetas, memoria, unidades extraíbles) y las exclusiones de la exploración, así como también determinar cómo debe responder el explorador cuando detecte un virus mostrando el informe detallado.		
2.18	El antivirus debe permitirle al administrador las opciones de preguntas en cuanto a limpiar, borrar, denegar acceso, e inclusive debe manejar una carpeta de cuarentena para archivos infectados que se detecten a través de reglas y lista predefinidas y/o personalizadas por el administrador.		
2.19	El motor de exploración deberá utilizar distintas tecnologías de detección virus: Exploración de firmas y exploración heurística "busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos".		
2.20	La solución debe utilizar detección mediante técnica heurística que permita desenmascarar las amenazas evasivas mediante la combinación de análisis de reputación, con la clasificación dada por el aprendizaje automático y modelos de comportamiento.		
2.21	La solución debe permitir la restauración automática de cambios que pudieran ser ejecutados por elementos considerados maliciosos.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
2.22	Por cada producto debe entregarse una versión vigente en el mercado y soportada por la casa matriz.		
2.23	La solución debe tener soporte para comunicaciones bajo IPv6 y soporte para IPv6 Firewall toda vez que IPv6 es una migración tecnológica que se debe llevar a cabo sobre las arquitecturas actuales.		
2.24	La solución debe poder detectar comunicaciones a sitios de comando y control con el fin de evidenciar pérdidas de información en los clientes.		
2.25	La solución debe contar con los mecanismos de protección para no poder ser desinstalada o desactivada por el usuario.		
2.26	La solución debe avisar sobre los posibles conflictos que existan de la solución a otras soluciones de antivirus y firewall instalados previamente en la máquina.		
2.27	Se deben poder habilitar o deshabilitar los módulos de protección sin ser desinstalados del sistema.		
2.28	La solución debe poder desplegar una aplicación cliente STANDALONE que pueda gestionar cambios localmente en caso de que se necesite.		
2.29	Se debe poder restringir completamente o parcialmente el acceso a la consola cliente para configurar parámetros individuales sobre el host.		
2.30	La desinstalación de la aplicación puede ser protegida mediante contraseñas desplegadas por políticas configuradas por el administrador.		
2.31	Puede existir más de una configuración de idioma para la aplicación cliente.		
2.32	La solución debe permitir a los administradores configurar escaneos bajo demanda en modo "escanear en reposo", para que se ejecuten sólo cuando el sistema esté inactivo.		
2.33	El fabricante debe contar con centros de investigación globales con el objetivo de detectar incidentes en diferentes países/regiones y compartir inteligencia de amenazas con la organización.		
2.34	La solución debe basarse en una plataforma común sobre la cual se incorporan módulos de Prevención de Amenazas, y Firewall de escritorio, y que permita el intercambio de información entre cada uno de los módulos.		
2.35	La solución debe poder configurarse para realizar escaneos por demanda o programados, desde la consola de administración o desde la consola cliente. Dichos análisis pueden ser ejecutados en diferentes niveles de agresividad y umbral de consumos de recursos máximo sobre el sistema.		
2.36	Se debe poder configurar acciones sobre infecciones identificadas: Denegar acceso / limpiar / Eliminar / Ninguna.		
2.37	Se deben reportar eventos de amenazas directamente sobre la consola cliente y visibles desde la consola de administración de la solución.		
2.38	La solución debe poder habilitar la opción de escaneo de clic-derecho sobre archivos y carpetas específicas.		
2.39	Debe contar con mecanismos de protección de Exploits Generic Buffer Overflow Protección (GBOP) o integración con Microsoft DEP (Data Execution Prevention).		
2.40	La solución debe contar con características de protección para navegadores web (Active X).		
2.41	La solución debe contar con mecanismos de protección a ejecución de scripts maliciosos de Internet Explorer, sean JavaScript o VBScript.		
2.42	La solución debe poder configurar mediante reglas o políticas de protección de: • Entradas y llaves de registro de Windows. • Prevención de creación de ejecutables portables (.INI, .PIF)		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
	• Creación de archivos autorun • Prevención de uso de archivos TFTP (Trivial File Transfer Protocol) • Contra lectura de archivos en cache de navegadores de internet • Creación y modificación remota de archivos o carpetas • Acceso remoto de archivos o carpetas. .EXE, .BAT y otros ejecutables bajo la llave de registro HKEY_CLASSES_ROOT • Modificación de procesos Core de Windows • Modificación de configuraciones de exploradores y navegadores web • Proteger procesos con subreglas personalizadas Asignar las reglas por nombre de usuario.		
2.43	Utilizar modelos locales de aprendizaje en combinación con la clasificación de aprendizaje dada desde la nube, para identificar rápidamente el malware de día cero y comenzar la remediación.		
2.44	El sistema debe permitir la detección basada en el comportamiento anómalo en el punto final.		
2.45	Contener aplicaciones desconocidas impidiéndoles realizar cambios a nivel del sistema, mediante reglas de Protección de acceso a aplicaciones y monitoreo de procesos en ejecución desconocidos.		
2.46	La solución debe emplear una arquitectura multicapa, para defenderse de ataques basados en comportamientos, evitando cambios a nivel de sistema, restringiendo el acceso a procesos, archivos, recursos compartidos, valores y claves de registro específicos.		
2.47	La solución debe poder identificar patrones similares de comportamiento dentro de diferentes variantes, usando reglas que pueden configurarse para evitar la instalación y / o la carga de nuevas variantes históricas, actuales y en evolución de amenazas de día cero.		
2.48	La solución debe ser compatible con versiones soportadas de los navegadores Internet Explorer, Google Chrome, Mozilla Firefox.		
2.49	Disponer de un motor antimalware que detecte infecciones y analice virus, gusanos, spyware, malware, ransomware y otras amenazas ubicadas en las estaciones de trabajo.		
2.50	Debe estar diseñado para optimizar el rendimiento de los equipos y el consumo de ancho de banda.		
2.51	Proteger las estaciones de trabajo contra infecciones a través descargas de internet, archivos adjuntos de e-mail, redes, archivos compartidos, CD-ROM, USB, dispositivos extraíbles, carpetas públicas y carpetas personales de todo tipo de correo, almacenadas localmente, mensajes de correo electrónico entrante y saliente, servicios en línea, entre otros tipos de almacenamiento.		
2.52	La solución debe ser instalada, configurado y gestionado en cada estación de forma centralizada desde los servidores, sin tener que hacer un despliegue uno a uno.		
2.53	La solución debe tener la capacidad de generar exclusiones por nombre de archivos, carpetas y tipos de archivos.		
2.54	Debe contar con medidas de seguridad para que el usuario o cliente no pueda modificar políticas corporativas efectuadas desde la consola de administración.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
2.55	La solución debe ser capaz de detectar el 100% de los virus conocidos (reportados en listas), contra programas malignos especificados.		
2.56	Debe anticiparse a los virus desconocidos e intrusos mediante herramientas que supervisen los procesos en ejecución en busca de comportamientos maliciosos.		
2.57	La solución de protección de endpoint debe tener la capacidad de detectar, detener y eliminar códigos o aplicaciones maliciosas como: gusanos, troyanos, spyware, ad-ware, keyloggers, ramsonware y cualquier otro programa potencialmente peligroso.		
2.58	Debe permitir generar informes detallados con los datos referentes a la detección de virus tanto en tiempo real, como del análisis bajo demanda y programado.		
2.59	Análisis en tiempo real de amenazas sobre los dispositivos extraíbles antes de tener acceso a los archivos en ellos almacenados.		
2.60	La solución debe contar con mecanismos de protección de amenazas avanzadas tipo ransomware.		
2.61	La solución debe contar con mecanismos de borrado seguro de malware residente en memoria que sean difíciles de erradicar, evitando el reinicio de servidores críticos.		
2.62	La solución debe contar con tecnología de prevención/mitigación de EXPLOITS, que ataquen soluciones comúnmente usadas y que pueden no estar actualizadas, como acrobat, flash player, entre otras.		
2.63	La solución debe mitigar la explotación de vulnerabilidades sobre sistemas operativos cliente y servidor.		
2.64	La solución debe contar con mecanismos que permitan prevenir un evento destinado a aprovechar la ausencia de configuraciones y/o parches específicos de sistema operativo.		
2.65	La solución debe contar con funcionalidades de detección de amenazas avanzadas sin necesidad de requerir actualizaciones frecuentes de firmas de virus, de manera que se pueda garantizar la protección en máquinas que se encuentren desconectadas de la red la policía y/o internet por largos periodos de tiempo.		
2.66	La solución debe contar con la aplicación de políticas de acuerdo con la identificación de la red a la cual se encuentre conectada la máquina.		
2.67	La solución o servicio ofrecido deberá realizar la desinstalación de los productos de protección actualmente instalados sobre los dispositivos de la organización en caso de ofrecer una solución o versión de producto diferente a la utilizada.		
2.68	El módulo de Control de Dispositivos debe permitir la creación de excepciones para un usuario, maquina o dispositivo especifico.		
2.69	El módulo de Control de Dispositivos debe permitir asignar reglas y políticas para usuarios y grupos de Directorio Activo.		
2.70	El módulo de Control de Dispositivos debe tener la capacidad de monitorear las actividades del usuario relacionadas al dispositivo removible de manera silenciosa.		
2.71	El módulo de Control de Dispositivos debe tener la capacidad de bloquear los dispositivos de almacenamiento extraíbles, incluyendo CD / DVD y USB entre otras.		
2.72	El módulo de Control de Dispositivos debe tener la capacidad de bloquear los dispositivos "Plug and Play".		

ÍTEM	CONDICIONES TECNICAS MINIMAS	CUMPLE	NO CUMPLE
2.73	El módulo de Control de Dispositivos debe tener la capacidad de poner como de solo lectura a los dispositivos de almacenamiento removible.		
2.74	El módulo de control de dispositivos debe tener la capacidad de integrarse con el módulo de cifrado.		
2.75	El módulo de Control de Dispositivos debe permitir la creación de categorías de dispositivos a necesidad/personalizados.		
2.76	La solución debe permitir compartir de forma instantánea la información sobre amenazas con otras soluciones de seguridad conectadas, incluidas las de terceros.		
2.77	La solución de Control de Dispositivos debe permitir la protección de toda la red contra acceso y uso de los dispositivos USB, permitiendo solo los autorizados por la organización.		
2.78	El módulo de Control de Dispositivos debe permitir auditar la conectividad de los dispositivos de almacenamiento externo.		
2.79	El módulo de Control de Dispositivos debe poder ser desplegado de manera centralizada, a través de la consola de administración o a través de herramientas de distribución de software suministrada.		
2.80	El módulo de Control de Dispositivos debe tener la capacidad de inspeccionar en tiempo real, la carga de información hacia un medio removible, con el objetivo de identificar documentos confidenciales y tomar acciones tales como bloqueo, registro, notificación.		
2.81	El módulo de Control de Dispositivos debe permitir la creación y manejo de listas blancas y negras de dispositivos tomando en cuenta atributos tales como VID (Vendor ID) y PID (Product ID).		
2.82	El módulo de Control de Dispositivos debe tener la capacidad de permitir los dispositivos de almacenamiento removible al menos que se encuentren permitido a través de listas blancas.		
3. FUNCIONALIDAD MÓDULO ANTIVIRUS EN WINDOWS SERVER Y LINUX			
3.1	Disponer de un motor antimalware o antispyware que detecte infecciones y analice virus, gusanos, y otras amenazas ubicadas en los servidores.		
3.2	La remediación o creación de firmas para las amenazas de día cero no deberán superar veinticuatro (24) horas una vez reportada al fabricante.		
3.3	Actualización diaria, incremental y automáticamente, así como patrones de comportamiento de los nuevos virus.		
3.4	Gestión centralizada y remota de la red con múltiples vistas gráficas de los servidores para un fácil reparto de las tareas entre los administradores.		
3.5	Exclusión del análisis en base a extensiones o ficheros que no se desee ser analizados.		
3.6	Debe permitir definir el umbral de consumo de recursos del sistema analizado al momento de programación un análisis del sistema.		
3.7	Debe realizar el análisis de archivos comprimidos por demanda.		
3.8	En los casos que un fichero no se pueda desinfectar, en análisis de tiempo real o bajo demanda, debe permitir borrar y/o enviar a cuarentena dicho fichero.		
3.9	Debe disponer de un producto especializado para ser implementado en los servidores virtuales existentes en infraestructura tecnológica de la Policía Nacional (Oracle, Hyperv). que suman 200 servidores virtuales y 200 físicos.		
3.10	Debe quedar instalado en los servidores de archivos y sharepoint.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
4. FUNCIONALIDAD DE LA CONSOLA DE ADMINISTRACIÓN ANTIVIRUS			
4.1	Despliegue, actualización, administración y soporte a toda la solución de seguridad ofertada; funcionalidades que deben efectuarse a través de una consola de gestión de políticas de seguridad y tareas.		
4.2	Debe interactuar con las consolas de administración que tiene actualmente la Policía Nacional (Directorio Activo – Microsoft), a fin de poder forzar el despliegue de políticas de seguridad e instalación hacia los dispositivos a ser protegidos.		
4.3	Debe disponer de un filtrado de vistas de las estaciones de trabajo y servidores instalados como mínimo con las siguientes características: • Estado del cliente • Ultimas Conexiones • Dirección IPv4/IPv6		
4.4	Debe permitir la detección y bloqueo remoto de equipos infectados, evitando, de esta manera, la propagación de amenazas a través de la red.		
4.5	Permitir la ejecución de tareas de instalación, despliegue o desinstalación de forma remota, reconociendo a los equipos por su dirección o rango de direcciones IP, nombre, pertenencia a dominio, lista plana.		
4.6	La solución debe poder ser administrada de forma segura vía web utilizando el protocolo HTTPS		
4.7	Capacidad de detectar equipos no gestionados en la red y sobre los cuales no se ha desplegado las técnicas de protección requeridas.		
4.8	Capacidad para descargar las actualizaciones desde Internet a través de las versiones seguras de los protocolos FTP y/o HTTP, colocándolas en múltiples repositorios distribuidos donde los clientes puedan buscar las definiciones de manera local, lo cual permite un ahorro en el ancho de banda.		
4.9	Capacidad de programar las actualizaciones para que sean realizadas en diferentes momentos y horas específicas (diaria, semanal, mensual, cuando la máquina este inactiva, inmediatamente, entre otras).		
4.10	Capacidad de actualizar automáticamente los archivos de definiciones de virus, motor antivirus, ficheros de firmas y actualizaciones del producto antivirus de forma: automática, centralizada e incremental.		
4.11	Capacidad de generar reportes ilimitados, detallados y personalizados por fecha, tipo de amenaza, amenazas detectadas y/o eliminadas, equipos infectados y/o desinfectados.		
4.12	La solución debe quedar instalada en modo alta disponibilidad y balanceo de cargas, con el fin de garantizar un plan de recuperación y continuidad en caso de desastre. El oferente deberá garantizar todos los requerimientos para esta instalación.		
4.13	La solución deberá permitir manejar una estructura distribuida donde los sistemas en diferentes locaciones puedan replicar políticas y eventos desde un punto hacia la consola de gestión. La solución deberá permitir la instalación de múltiples consolas para mantener un esquema de gestión independiente en caso sea requerido.		
4.14	Disponer de información que permita ver el estado de seguridad y mantenimiento de los productos de toda la solución.		
5. MÓDULO CONTROL DE APLICACIONES			
5.1	El módulo de control de aplicaciones debe ser instalado para Dieciocho mil (18.000) nodos.		

ÍTEM	CONDICIONES TÉCNICAS MINIMAS	CUMPLE	NO CUMPLE
5.2	El módulo de control de aplicaciones debe proporcionar un módulo de descubrimiento de aplicaciones instaladas en cada uno de los hosts, este reporte debe ser entregado al momento de la instalación, por demanda y/o definido a criterio del administrador, adicionalmente debe permitir la desinstalación remota desde la consola de administración del software que el administrador defina.		
5.3	La solución debe estar en la capacidad de generar lista blanca de aplicaciones, ejecutables y librerías independientemente si se encuentran instaladas y/o en uso.		
5.4	El módulo de control de aplicaciones debe permitir definir listas blancas de aplicaciones que pueden ser ejecutadas en los equipos de cómputo protegidos, esta lista podrá ser modificada en cualquier momento sin restricción.		
5.5	Las listas deben ser creadas de forma independiente por cada uno de los equipos protegidos, deben ser usadas para la realización de inventario de software y para el control de la ejecución de las mismas.		
5.6	El módulo de control de aplicaciones debe permitir definir listas negras de aplicaciones que no pueden ser ejecutadas, ni instaladas en los equipos de cómputo protegidos (de forma global para toda la plataforma), esta lista podrá ser modificada en cualquier momento sin restricción.		
5.7	La solución debe poder realizar inventario de las estaciones de trabajo el cual permitirá conocer las aplicaciones instaladas en estos.		
5.8	La solución permitirá proteger estaciones de trabajo mediante el control de la ejecución de aplicaciones, realizado a través de listas blancas y negras, por medio de la prevención de modificaciones hacia los archivos del punto final.		
5.9	La solución debe emplear un modelo de confianza y/o monitoreo de comportamiento para bloquear las aplicaciones no autorizadas o maliciosas.		
5.10	Debe contar con mecanismos de protección de memoria para contrarrestar los ataques de buffer overflow sobre las aplicaciones en lista blanca.		
5.11	Debe proteger contra las amenazas persistentes avanzadas y de tipo zero-day sin actualizaciones de firmas.		
5.12	La solución deberá permitir a los usuarios ser notificados sobre la razón por la cual la aplicación ha sido bloqueada.		
5.13	La solución deberá permitir a usuarios específicos que puedan instalar nuevo software en caso de que sea necesario, sin necesidad de autorización adicional.		
5.14	La solución deberá tener protección contra lectura y escritura de archivos.		
5.15	La solución deberá soportar los siguientes sistemas operativos Microsoft Windows server: 2008, 2008 R2, 2012, 2012 R2, y posteriores Además de los siguientes para estación de trábajo: 7, 8, 8.1, 10, 11 y posteriores.		
5.16	La solución deberá soportar los siguientes Sistemas Operativos de Microsoft los cuales ya no cuentan con soporte del fabricante: 2003, 2003 R2, Windows XP.		
5.17	La solución deberá soportar los siguientes sistemas operativos de Microsoft Windows Embedded: XPE, 7E, WEPOS, POS Ready 2009, WES 2009, 8 Industry, 8.1.		
5.18	La función de protección de escritura y cambios a los sistemas deberá proteger de: • Eliminar • Modificar Contenido • Cambiar Propietario • Truncar		
5.19	La solución debe proveer un panel de monitoreo para poder visualizar los cambios y violaciones en los equipos finales.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
5.20	El control de aplicaciones debe permitir realizar la desinstalación de software de forma remota.		
5.21	Reconocimiento de anomalías, detección y bloqueo de ataques de tipo Host Sweep, TCP or UDP port Scan, CGI Holes, entre otros.		
5.22	Detección de ataques de tipo Exploits hacia vulnerabilidades de sistema operativo como también de aplicaciones diferentes de Microsoft.		
5.23	El módulo de control de aplicaciones debe incluir un sistema de detección y prevención de intrusos basados en host que proteja los recursos del sistema y las aplicaciones de ataques internos y externos.		
5.24	El módulo de control de aplicaciones debe contar con una consola de administración o integrarse con la consola general de administración de la solución, adicionalmente deberá poder integrarse con sistemas de colección de eventos vía syslog o enviadas al SIEM (Enterprise Security manager McAfee) de la Policía Nacional.		
5.25	El módulo de control de aplicaciones debe contar con un Firewall personal para los equipos Windows.		
5.26	El módulo de control de aplicaciones debe permitir obtener estadísticas del software instalado en los equipos de cómputo, intentos de instalación de aplicativos que se encuentren en listas negras, entregando hora, máquina y usuario que intenta realizar la instalación.		
5.27	El módulo de control de aplicaciones debe contar con la opción de bloquear todas las aplicaciones por defecto y generar listas blancas creadas por la casa matriz de acuerdo a reputación del sitio de descarga, hash, checksum, nombre, lista blanca, definición del administrador, entre otros. Adicionalmente La solución deberá permitir a los usuarios ser notificados sobre la razón por la cual la aplicación ha sido bloqueada.		
5.28	Capacidad de generar reportes ilimitados, detallados y personalizados por fecha, tipo de amenaza, amenazas detectadas y/o eliminadas, equipos infectados y/o desinfectados.		
6. DATA LOST PREVENTION - DLP			
6.1	El módulo Data Lost Prevention - DLP debe ser instalado para Cuarenta y Cinco Mil (45.000) nodos.		
6.2	La solución debe basarse en un agente que se instala en cada computadora y servidor que servirá como medio de comunicación entre las estaciones de trabajo y la consola de administración.		
6.3	La solución debe tener una base de datos de Microsoft SQL u Oracle en la cual deberá guardar todos los informes sobre la detección de violaciones de políticas.		
6.4	La solución deberá permitir crear diferentes sets de permisos para asignar diferentes tipos de administración a usuarios y grupos.		
6.5	La solución deberá contar con un tablero de Analíticos, este tablero podrá mostrar los incidentes basados en la clasificación.		
6.6	La solución de protección de fuga de información del endpoint deberá contar con un agente para sistemas operativos MAC donde los usuarios de dicha plataforma puedan aplicar: Reglas de acceso por medio de aplicaciones, reglas de protección Cloud, reglas para protección de compartir en red y dispositivos removibles.		
6.7	La solución deberá integrarse con Active Directory y permitir hacer inicio de sesión a la consola de administración utilizando las credenciales de red con sus respectivos permisos.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
6.8	La solución debe tener la capacidad de administrar, configurar, instalar, desinstalar, actualizar, asignar políticas para el software de Control de dispositivos y Prevención de Fuga de Información (DLP).		
6.9	La solución debe llevar como minimo 6 años consecutivos como líder en el cuadrante de Gartner de prevención de fuga de datos.		
6.10	La solución debe identificar contenidos basados en tipo de contenido/documento.		
6.11	La solución debe monitorear el contenido que viaje a través del ENDPOINT, por dirección IP y protocolo.		
6.12	La solución debe monitorear el contenido que viaje a través el ENDPOINT, debido al acceso de aplicaciones.		
6.13	La solución debe permitir crear políticas para dispositivos extraíbles de almacenamiento, por fabricante.		
6.14	La solución debe poder identificar contenido usando expresiones regulares, palabras clave, las funciones hash, y la coincidencia de patrones.		
6.15	La solución debe poder identificar el contenido basado en localización.		
6.16	La solución debe poder identificar el contenido usando FINGERPRINT.		
6.17	La solución debe cumplir las políticas aplicadas de protección de fuga de información, sin importar que el equipo final se encuentre fuera de la red corporativa.		
6.18	La solución debe contar con una funcionalidad de Soporte de virtualización mejorada. Es decir que cada política por usuario debe ofrecer flexibilidad y un mejor control de los datos que fluyen a las terminales compartidas e infraestructuras de escritorio virtual (VDI). Así, las políticas por usuario deben aplicar a múltiples sesiones.		
6.19	La solución debe brindar protección a nivel de portapapeles para ambos: "copia de" y "pegar", además de protección de captura de pantalla para proteger el diseño de productos y códigos fuente contra la pérdida de datos intencional y no intencional. Garantizando esta protección incluso si se utilizan métodos alternativos como aplicaciones de recortes de office, one note, navegadores, entre otros.		
6.20	La solución debe permitir la configuración de incidentes de acuerdo con sus propiedades para una revisión posterior. Las propiedades deben ser como mínimo: • Severidad • Estatus • Resolución • Revisor		
6.21	La solución debe contar con mecanismos que prevengan la vista no autorizada de información confidencial, a través del módulo de manejo de incidentes, limitando la vista de incidentes sólo a revisores o administradores con un rol cuyos privilegios se lo permitan.		
6.22	La solución de contar con reglas de protección que estén basadas en: tipo de archivo, extensiones de archivo, propiedades de documento, tipos de encripción y asignación de usuarios o grupos.		
6.23	La solución debe permitir usar repositorios para evidencia.		
6.24	La solución deberá replicar de forma manual o automática a través de tareas el software para las actualizaciones e instalaciones.		
6.25	La solución deberá permitir crear políticas para clasificar el contenido sensible por medio de categorización de aplicaciones como; editores, exploradores, confiables y archivadores.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
6.26	La solución debe tener la capacidad de obtener información completa sobre las propiedades del documento sensible como; quien lo grabo de último, el título, autor, comentarios, etc.		
6.27	La solución debe permitir crear configuraciones por grupo, dominio o maquina sin afectar la estructura del árbol de administración.		
6.28	La solución debe controlar la impresión usando impresoras locales, en red, print screen e impresión en PDF.		
6.29	La solución no debe de requerir el reinicio de la computadora al instalar o hacer actualización.		
6.30	La solución debe controlar la carga de información sensible hacia aplicaciones de la nube como Box.inc, Dropbox, Google Drive, iCloud, OneDrive (personal) OneDrive for Business (groove.exe) y Simplicity.		
6.31	La solución debe contar con una lista de reglas de acción para realizar como mínimo lo siguiente: • Sólo lectura • Reportar a la consola central • Poner en cuarentena • Cifrar • Guardar la evidencia • Solicitar justificación • Notificar al usuario • Monitorear • Bloquear		
7. ARQUITECTURA			
7.1	La solución debe contar con una arquitectura distribuida para optimización de funcionalidades.		
7.2	Deberá contar con la creación de patrones avanzados para reducir los falsos positivos.		
7.3	La solución deberá tener mecanismos de control de incidentes para su revisión y operaciones como; Manejo de caso, comentarios, envió por correo, etc.		
7.4	La solución debe presentar un flujo de trabajo que debe contar con una fase de clasificación o definición, una fase de identificación y registro, una fase de protección y una fase de monitoreo.		
7.5	La solución debe integrarse con soluciones de Rights Management (IRM) como: • Microsoft Windows Rights Management Services • Seclore FileSecure information Rights Management Con el objetivo de aplicar políticas de RM a archivos detectados en escaneos de descubrimiento y poder incluir o excluir archivos protegidos por RM, de las reglas de protección de correo, almacenamiento removible, sistemas de archivos y web posting.		
7.6	Debe de permitir la integración con etiquetado de terceros como: • TITUS • Boldon James		
7.7	La solución debe contar con una consola de gestión centralizada, desde la cual sea posible gestionar políticas, reglas de protección de información.		
7.8	La interfaz de monitoreo de la solución debe proveer un panel para el manejo de incidentes, separado de un panel para eventos operacionales, donde se muestren eventos administrativos.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
7.9	La solución debe contar con la posibilidad de hacer control de acceso basado en roles.		
7.10	Se requiere que la solución posea una consola de administración vía web.		
7.11	Los revisores o administradores de la consola deberán poder auditar las siguientes acciones: • Entrada al servidor de administración • Cambio de perfiles o roles • Cambio de contraseñas • Cambios de políticas Esta característica es importante cuando se desea descubrir cambios ocurridos en el servidor de administración.		
7.12	El agente debe registrar todas las violaciones e informes en la base de datos central de la consola, cuando se establece una conexión a la red corporativa.		
7.13	La solución deberá contar con reportes predefinidos y la posibilidad de crear nuevos a partir de queries personalizados.		
7.14	La solución debe soportar reglas y exclusiones basadas en directorio de datos para reforzar las políticas basándose en cualquier atributo del documento y/o receptor.		
7.15	La solución debe incluir una biblioteca de plantillas predefinidas de detección orientadas al cumplimiento con regulaciones locales y globales como la Ley de protección de datos (Ley 1581, SOX, PCI y HIPAA.), Si la solución no incluye la plantilla el proveedor deberá crear dicha plantilla y dejarla en operación.		
7.16	La solución debe permitir detectar y analizar archivos y anexos de correo de tamaños mayores a 20 MB sin verse afectado el rendimiento de los equipos.		
7.17	La solución debe permitir especificar el grado de proximidad como una condición de una coincidencia para un incidente.		
7.18	La solución debe detectar la información sin importar que el orden de los datos haya sido alterado.		
7.19	La solución deberá estar en la capacidad de detectar contenido confidencial incluso si el nombre o tipo de archivo es modificado.		
7.20	La solución debe soportar la detección de coincidencias en un contenido con exactitud del 100% para documentos específicos tales como código fuente, documentos financieros, etc.		
7.21	Debe ser posible definir un umbral o porcentaje mínimo requerido de coincidencia de un documento para considerar que existe una violación a la política configurada.		
7.22	La solución debe permitir la detección basada en expresiones regulares.		
7.23	La solución debe permitir la detección o presencia de archivos cifrados.		
7.24	La herramienta podrá ser integrada con herramientas de cifrado de datos, para que en el caso de detectar contenido sensible tenga como respuesta el cifrado de la información.		
7.25	La solución debe permitir notificar automáticamente a remitentes administradores y jefes inmediatos de un usuario cuando este ha violado una política.		
8. CIFRADO			
8.1	El módulo de cifrado debe ser licenciado y configurado para quince mil (15.000) nodos.		
8.2	La solución de cifrado de discos debe permitir el cifrado en los sistemas operativos Microsoft, Linux y MAC.		
8.3	La solución debe permitir la integración con el directorio activo.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
8.4	La solución de cifrado debe permitir la creación de políticas a través de grupos del directorio activo.		
8.5	La solución de cifrado debe contar con una consola de administración centralizada.		
8.6	La solución debe permitir el envío de tareas remotas tales como cifrar y descifrar desde la consola de administración.		
8.7	La solución de cifrado debe permitir tener una recuperación centralizada a través de la consola de administración.		
8.8	La solución de cifrado debe permitir tener SSO (Single Sign-On) con el directorio activo para el acceso a las maquinas cifradas.		
8.9	La solución de cifrado de discos deberá integrar en el mismo licenciamiento la funcionalidad de cifrado de archivos que se copian a medios removibles.		
8.10	La solución de cifrado de discos debe tener una funcionalidad que se copie en los medios extraíbles para ver la información cifrada en equipos que no tengan ninguna solución de cifrado. Esta funcionalidad debe poder abrirse en Windows y MacOSX.		
8.11	La solución de cifrado debe permitir crear una contraseña para el cifrado de todos los archivos que se copian a los medios extraíbles o tener una contraseña según las preferencias del usuario.		
8.12	Las contraseñas que se crean para la copia de archivos a medios extraíbles deben permitir configurar complejidad.		
8.13	La solución de cifrado debe permitir generar informes del estado de los discos administrados y cifrados.		
8.14	La solución de cifrado debe permitir la configuración de un método de seguridad cuando se ingrese la contraseña incorrectamente un determinado número de veces. Ejemplo evitar la autenticación durante determinado tiempo.		
8.15	La solución de cifrado debe permitir configurar un tiempo de expiración de las contraseñas.		
8.16	La solución debe permitir la configuración del periodo de conexión entre los agentes de cifrado y la consola centralizada.		
8.17	La solución de cifrado debe permitir la autenticación en las maquinas cifradas con password, token o token y password.		
8.18	La solución de cifrado debe tener métodos de recuperación ante desastres, en caso de que exista daño en el sistema operativo, el usuario olvide su contraseña y/o los métodos de recuperación no funcionen.		
8.19	La solución de cifrado debe soportar cifrado AES 256 Bits.		
8.20	La ventana de Preboot debe permitir la personalización de logo y mensaje de bienvenida.		
8.21	La solución de cifrado de discos debe permitir el cifrado de solo el Boot de inicio o de todos los discos según se requiera.		
8.22	La consola de administración de cifrado de discos duros debe permitir visualizar las particiones cifradas y las no cifradas.		
8.23	El agente de cifrado de discos debe permitir visualizar las unidades que están cifradas y descifradas en la máquina.		
8.24	El agente de cifrado de discos debe permitir ver un porcentaje del proceso de cifrado de discos.		
8.25	La solución de cifrado de medios removibles debe permitir crear exclusiones para evitar que determinadas extensiones de archivos se cifren automáticamente.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
8.26	La solución de cifrado de medios extraíbles debe permitir crear exclusiones de dispositivos que no se cifraran.		
8.27	El producto debe soportar las siguientes maquinas clientes: • Windows 7 and SP1 (32- and 64-bit), (Not XP Mode) • Windows 8 • windows 10 • Windows 11 y posteriores		
8.28	La solución debe poseer al menos las siguientes certificaciones: • Common Criteria EAL2 +, FIPS 140-1, FIPS 140-2 • AES CBC (e/d; 256).		
8.29	La solución debe soportar al menos los siguientes algoritmos de Encriptación: • AES-256.		
8.30	La solución de cifrado debe permitir el cifrado de archivos que sean transferidos a dispositivos de almacenamiento extraíble.		
8.31	La solución de cifrado debe permitir generar excepciones sobre dispositivos donde no se debe aplicar el cifrado.		
8.32	Debe tener la capacidad de cifrar el disco completo, reemplazando el Master Boot Record (MBR).		
8.33	La solución debe proveer mecanismos seguros que garanticen la recuperación del acceso en caso de pérdida de la contraseña. Estos mecanismos deben requerir la intervención y el intercambio de información con la consola de administración.		
8.34	Debe ser capaz de descifrar el disco en forma automática, desde la consola de administración y mediante mecanismos manuales.		
8.35	La solución debe solicitar autenticación al usuario antes de iniciar la carga del sistema operativo (SO). Luego de iniciar el SO, la solución debe poder configurarse de manera que solicite o no, nuevamente, las credenciales de autenticación del usuario.		
8.36	Las actualizaciones de la solución deberán realizarse remotamente y desde una consola de administración centralizada.		
8.37	La arquitectura de la solución debe ser cliente-servidor.		
8.38	La solución debe emplear el mínimo de utilización de recursos del CPU.		
8.39	La solución debe tener la capacidad de realizar single Sign-On en sistemas operativos Windows permitiendo el acceso a la maquina mediante las credenciales de Windows y reduciendo los procesos para ingresar.		
8.40	La solución debe soportar la unificación del usuario y contraseña utilizadas por el usuario en el directorio Activo de Microsoft.		
8.41	La solución debe contar con una herramienta externa que utilice las Llaves de Encriptación almacenadas en la consola de administración para ejecutar cualquier actividad de recuperación de discos o archivos.		
8.42	La solución debe soportar Single Sign-On (SSO) en integración con las políticas de grupo (GPO) del Directorio Activo de Microsoft.		
8.43	La solución debe contar con la opción de generar un "código de respuesta" para la recuperación del administrador.		
8.44	El acceso de los usuarios administradores a la consola de administración debe poder hacerse basado en roles.		
8.45	La consola de administración debe permitir la creación de políticas de autenticación que no sean de alcance global.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
8.46	La solución debe proveer reportes del estado de la solución en las maquinas administradas. Todos estos reportes deben ser exportables vía correo o a documentos PDF, XLS y CSV.		
8.47	La solución debe proveer un reporte de los sistemas cifrados, mostrando un estado de Cifrado o Descifrado.		
8.48	La solución debe ser capaz de enviar reportes y notificaciones por email en los siguientes formatos: • CSV • XLS • PDF		
8.49	La solución debe permitir generar reportes basados en eventos históricos.		
8.50	La solución debe contener reportes y consultas (query) que se puedan personalizar.		
8.51	La solución debe contar con la funcionalidad de que gestionar Native Encryption.		
8.52	La solución debe ofrecer beneficios en común para la gestión sobre FileVault y BitLocker: • Posibilidad de actualizar una versión OS X a la siguiente sin tener que descifrar y volver a cifrar el disco. • Compatibilidad de día cero con parches, actualizaciones y actualizaciones de firmware de Apple y Microsoft. • Característica de recuperación que permite a los usuarios restablecer el acceso a sus máquinas. • Fácil administración		
8.53	La solución debe ofrecer beneficios para entornos Mac: • Capacidad de hacer SSO desde el entorno de Pre-Boot de FileVault directamente al inicio del ambiente de OS X. • Administración de File Vault en un HW que puede ejecutar OS X Mountain Lion, Mavericks o Yosemite, desde una consola centralizada. • Generación de reportes de cumplimientos y elaboración de tableros de control. • Apoyo a las herramientas y flujos de trabajo para la recuperación de información proveídas por Apple (FileVault Recovery Key) • Permitir a los administradores la importación manual de FileVault Recovery Keys donde ya manualmente los usuarios han habilitado File Vault.		
8.54	Beneficios para entornos Windows: • Soportar dispositivos certificados Windows To Go • Administrar de BitLocker en hardware Windows 7 u 8, 10 y 11 desde una única consola • Proveer una experiencia transparente al usuario (Trusted Platform Module - TPM) • Soportar los requerimientos FIPS 140-2. • Soportar Microsoft eDrive. • Generación de reportes de cumplimientos y elaboración de tableros de control • Administración de BitLocker sin la necesidad de contar con un servidor Microsoft BitLocker Management and Monitoring (MBAM).		
9. SOLUCIÓN DE SEGURIDAD PERIMETRAL DE CORREO - ANTISPAM			
9.1	Se requiere una solución de tipo "Gateway" que permita la inspección profunda de los correos electrónicos contra las siguientes amenazas: spam, phishing, virus, ataques de directorio, ataques de rebote (bounce attacks) y filtrado de contenidos para 20.000 buzones.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
9.2	El fabricante de la solución deberá ofrecer detectar el 99,9% de Spam con un número de Falsos positivos menor o igual a 1 en un millón.		
9.3	El dispositivo deberá estar soportado para correr tanto en Hardware físico o a través de dispositivos virtualizados en plataformas Hyper-V. La Policía Nacional privilegiará el poder montar la solución en la infraestructura de virtualización existente o en la máquina suministrada por el contratante que cumpla los requerimientos necesarios para soportar la cantidad de usuarios de la Policía Nacional.		
9.4	El número de servidores virtuales de filtrado podrá incrementarse o disminuirse a discreción de la Policía Nacional sin incrementar el costo de la solución.		
9.5	La solución se deberá sincronizar con el Directorio Activo de la Policía Nacional para permitir el acceso a la cuarentena por cada usuario, además de detectar y evitar ataques de directorio.		
9.6	La solución podrá controlar y dilatar las conexiones y el envío de direcciones IP que se hayan detectado envíen Spam principalmente.		
9.7	Además de listas blancas de IP, La solución podrá, sin intervención de administración, tener estadísticas de direcciones IP que envíen correo bueno para privilegiar el envío de correos hacia el interior de la Policía.		
9.8	La Policía Nacional podrá generar direcciones de correo que actualmente no estén uso y sean altamente atacadas para que sean analizados directamente contra problemas de SPAM por parte del fabricante de la Solución.		
9.9	La Policía podrá crear exclusiones de SPAM para buzones dedicados al reporte y análisis de problemas de SPAM y Phishing de los que sufra la ciudadanía.		
9.10	El dispositivo podrá identificar máquinas internas que estén generando ataques al interior de la red de la compañía y rechazar temporalmente dichas conexiones.		
9.11	La solución permitirá la firma de correos electrónicos de salida con el estándar DKIM y así mismo podrá chequear la validez de los correos entrantes para las firmas DKIM.		
9.12	La solución contará con plantillas que permitan examinar los contenidos de los correos y sus adjuntos para evitar fugas de información.		
9.13	La solución incluirá la ejecución de reportes. Dichos reportes podrán dar una idea del estado del servicio y número de correos detenidos, número de correos que presentan malware, correos que no se pudieron escanear, reporte de reputación IP entre otros.		
9.14	La solución tendrá un sitio de cuarentena tipo Web para retener los correos de acuerdo a las Políticas de seguridad de la Policía. Los usuarios podrán acceder a dicha cuarentena bien para eliminar los correos o dejarlos pasar.		
9.15	La solución deberá contar con mecanismos de auditoría detallados para reconocer correos enviados, asunto, disposición de filtrado.		
9.16	La solución tendrá mecanismos de detección antispam basada en firmas, heurísticas que se actualicen frecuentemente de los servicios del fabricante.		
9.17	El dispositivo a través del tiempo podrá aprender de los comportamientos de las direcciones IP de los remitentes para rechazar la comunicación de direcciones IP reconocidas como Spammers		
9.18	El dispositivo a través del tiempo tendrá la capacidad de clasificar direcciones IP que envían principalmente correo no spam y privilegiar el paso del correo y haciendo solo la detección antivirus		
9.19	El dispositivo debe permitir la limpieza de amenazas dentro archivos adjuntos (javascript dentro de archivos PDF o Microsoft Word, por ejemplo)		
9.20	El soporte de la solución antispam será 7x24x365 con un tiempo de respuesta de no superior a más de una hora, La solución debe contar con un soporte que permita		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
	accesos directos a los especialistas de producto cuando sea requerido por los diferentes medios de atención por la Policia Nacional.		
9.21	La solución de filtrado de correo electrónico deberá proteger el correo entrante contra amenazas como virus, spyware, malware, spam, phishing y permitirá crear reglas de filtrado dependiendo los destinatarios, remitentes, contenidos.		
9.22	La solución deberá estar en capacidad de cifrar correo electrónico y sus adjuntos para al menos 500 usuarios simultáneos.		
9.23	La solución podrá identificar archivos sin importar su extensión identificando su verdadero contenido.		
9.24	Para archivos cuyo contenido sean ejecutables la solución podrá identificarlos y remover el contenido ejecutable dentro de dichos correos o eliminar el correo.		
9.25	La solución de filtrado de correo electrónico podrá inspeccionar el contenido de los correos para detectar URLs que se consideren maliciosas y actuar de acuerdo a las políticas de la Policía Nacional.		
9.26	La solución podrá ser instalada en al menos un appliance físico o virtual, pero podrá ser distribuida en tantos appliance requiera la Policía, administrados de manera centralizada.		
9.27	La solución contará con consola y/o carpetas de cumplimiento. Una carpeta de cumplimiento es un espacio dentro de la solución en la que se retienen correos electrónicos que caen dentro de la detección de una política (filtran datos sensibles, se requieren para auditoría).		
9.28	La solución no deberá requerir licenciamiento adicional del sistema operativo sobre el que corre.		
9.29	El Software de la solución deberá estar asegurado por el fabricante y el acceso a las cuentas privilegiadas (root) deberá estar deshabilitada como mecanismo de aseguramiento.		
9.30	La solución seguridad perimetral de correo no podrá ser instalada en los servidores de Correo de la Policía Nacional. La idea es disminuir el impacto de este procesamiento y proteger la infraestructura de la Policía.		
9.31	La solución deberá clasificar los mensajes recibidos en categorías dentro de las cuales debe existir una categoría para identificar correos relacionados con marketing (publicidad).		
9.32	La solución tendrá mecanismos de reputación de IP que impedirán o retrasarán la conexión de los atacantes.		
9.33	La solución debe tener listas negras de remitentes tanto locales como globales para ser usadas en las políticas de filtrado.		
9.34	La solución debe ser configurada para tomar acciones diferentes con correos de publicidad y/o boletines de noticias.		
9.35	La solución debe permitir autenticación de remitentes a través de SPF tanto como política general para todos los correos recibidos como para una lista de dominios específicos.		
9.36	El filtrado de correo electrónico deberá permitir enviar muestras de SPAM al fabricante de la solución para obtener reglas personalizadas contra SPAM.		
9.37	La solución debe permitir crear reglas de filtrado de correo de acuerdo con su contenido, tanto para información estructurada como no estructurada, expresiones regulares, diccionarios y palabras clave; y deberá generar un reporte con las posibles violaciones a la política.		
9.38	Debe permitir crear y aplicar políticas de prevención de fuga de información.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
9.39	La solución antispam debe contar con una consola de administración o integrarse con la consola general de administración de la solución, adicionalmente deberá poder integrarse con sistemas de colección de eventos vía syslog o enviadas al SIEM (Enterprise Security manager McAfee) de la Policía Nacional.		
10. DETECCIÓN Y REMEDIACIÓN ANTE AMENAZAS DE SOFTWARE MALICIOSO			
10.1	Combinar la información colectiva sobre amenazas a partir de fuentes de datos globales, con la información sobre amenazas recabada localmente.		
10.2	Obtener visibilidad de la presencia de ataques avanzados en la institución.		
10.3	Compartir en tiempo real la información de seguridad relevante entre los distintos componentes de la solución.		
10.4	Posibilidad de diferentes acciones sobre tipos de archivos nunca vistos anteriormente, en función del contexto de los equipos de punto final (atributos de archivo, proceso o entorno), en base a la información colectiva sobre amenazas.		
10.5	Identificar y supervisar el contexto y estado de los equipos de punto final, para reconocer cambios que puedan estar asociados a indicadores de compromiso.		
10.6	Capacidad de identificar componentes de los ataques que puedan estar en estado latente; y de enviar la información a los componentes de análisis, operaciones o investigación forense.		
10.7	Dar tratamiento a las alertas, para poder realizar ajustes según los cambios en las metodologías de ataque.		
10.8	Automatizar la recopilación de datos, alertas y respuestas; y personalizar sus configuraciones en función de los flujos de trabajo identificados.		
10.9	Capacidad continua para detectar incidentes relacionados con un ataque, y de generar las notificaciones sobre las actividades detectadas.		
10.10	La solución debe utilizar The MITRE Attack Framework para el análisis de posibles incidentes dentro de la organización.		
10.11	En el proceso de análisis de un posible incidente, la herramienta debe permitir asignar distintos estados al proceso de evaluación para determinar la etapa en que se encuentra un incidente.		
10.12	La solución debe permitir el registro, seguimiento y cierre de casos sin que exista límites en la cantidad de los mismos.		
10.13	La solución debe permitir poner en cuarentena a los host comprometidos con el objetivo evitar movimientos laterales de códigos maliciosos.		
10.14	La integración con los otros componentes de la solución ofertada deberá ser a través de un protocolo estándar de comunicación.		
10.15	La solución debe permitir la creación de colectores de información de manera personalizada para realizar búsquedas en tiempo real y en proceso de hunting.		
10.16	La solución debe permitir la creación de reacciones de manera personalizada para contener y aplicar remediaciones que se ajusten a las necesidades de la organización.		
10.17	La solución debe permitir soportar la creación de script de ejecución en Pyhton, Vbscritp y/o la ejecución de comandos de sistemas operativos de manera remota.		
10.18	La solución debe utilizar distintos mecanismos de análisis los cuales deben incluir el uso de playbooks, información de terceros para detectar posibles incidentes dentro del ecosistema.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
11.	**GENERALIDADES**		
SOPORTE Y MANTENIMIENTO			
11.1	El personal que realizará la instalación y configuración de la solución, deberán ostentar el título de Ingeniero de Sistemas, Electrónico y/o a fines, con una experiencia mínima de un (1) año en la configuración e instalación la solución y contar con capacitación certificada por la casa matriz. Para lo cual el oferente deberá presentar con la oferta copia del título de pregrado en ingeniería de sistemas, electrónica y/o a fines, tarjeta profesional vigente, copia de la certificación de la casa matriz sobre la idoneidad en la implementación y administración solución y una certificación de experiencia en la instalación y soporte de la misma de la persona propuesta para la implementación.		
11.2	Los soportes serán generados por los usuarios de la red de la PONAL (Policía Nacional) a través de la herramienta de help desk de la Policía Nacional (SIGMA) para la gestión por parte del ingeniero de soporte asignado por el oferente, el cual deberá proporcionar un soporte 5x8 en sitio durante la misma vigencia de la garantía, derecho a actualizaciones de la licencias de los productos adquiridos, a partir del recibo a satisfacción del contrato, el cual se debe prestar en sitio con tiempos de respuesta no superiores a 30 minutos, y tiempos de solución no mayores a las setenta y dos (72) horas debiéndose dar respuesta oportuna y orientación precisa a los diferentes casos que se reporten. Los soportes e incidentes generados a través de la herramienta SIGMA deberán ser gestionados por el ingeniero de soporte asignado por la empresa contratista desde la red LAN y/o WAN de la Policía Nacional (no se permiten VPN para el soporte), se evaluarán los casos de soporte remoto únicamente para asistencia por parte de la casa matriz.		
11.3	El soporte, mantenimiento y actualizaciones de la solución objeto del contrato será por un término de dieciocho (18) meses a partir del recibo a satisfacción de la solución.		
11.4	El mantenimiento y actualización debe permitir de manera proactiva y centralizada desde la consola de gestión mantener la plataforma tecnológica de la Policía Nacional debidamente asegurada, mediante actividades que permitan validar los niveles de actualización y cobertura de los productos implementados en todas las estaciones y servidores que tengan conectividad con la consola.		
11.5	El servicio de soporte telefónico debe darse directamente por la casa matriz para todos los niveles de prioridad de los incidentes, problemas, inquietudes, dudas que se reporten durante el término de vigencia del contrato.		
11.6	En caso de existir urgencia respecto a incidentes que involucren las soluciones ofertadas el oferente deberá proporcionar en caso de necesitarlo apoyo de casa matriz (remoto o presencial) hasta solucionar el incidente.		
11.7	El soporte de la solución será 8x5 con un tiempo de respuesta no superior a más de una hora por parte del fabricante, La solución debe contar con un soporte que permita accesos directos a los especialistas de producto cuando sea requerido por los diferentes medios de atención por parte la Policía Nacional.		
11.8	El oferente informará periódicamente vía e-mail al correo ponal.csirt@policia.gov.co de la entidad, acerca de los nuevos virus, suministrando los medios para combatirlos y evitar próximos ataques, informando dentro de las dos (02) horas siguientes después de presentarse la alerta mundial.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
12. SERVICIOS DE IMPLEMENTACIÓN			
12.1	La solución ofertada deberá ser instalada y configurada de forma centralizada por el oferente, realizando los despliegues en todos los repositorios a nivel nacional. El oferente en caso de ofrecer un producto diferente al existente en la Policía Nacional deberá realizar la desinstalación del mismo durante el período de implementación.		
12.2	El oferente deberá garantizar total compatibilidad con la infraestructura de red, sin degradar el rendimiento de los equipos bajo las diferentes plataformas tanto de estaciones de trabajo como de servidores e infraestructura de red que se encuentran instalados. Para lo cual deberá soportar técnicamente mediante la realización de pruebas.		
12.3	Se deben incluir Cuarenta y ocho (48) horas de servicios profesionales directamente del fabricante de la solución ofertada, con el fin de realizar actividades que vaya orientadas al mejoramiento continuo de la implementación, despliegue y configuración de la solución adquirida		
13. TRANSFERENCIA DE CONOCIMIENTOS			
13.1	El oferente deberá incluir una capacitación por el oferente o la casa matriz para al menos diez (10) funcionarios de soporte técnico de la solución que incluya el uso y administración del software, antivirus, control de dispositivos, Control de Aplicaciones, Data Lost Prevention - DLP, Cifrado, Antispam, las actualizaciones, funcionalidades de los productos adquiridos en el presente contrato. La intensidad horaria no debe ser inferior a 30 horas.		
14. LICENCIAMIENTO			
14.1	Todo el software que compone la solución debe ser licenciado de manera perpetua a nombre de la Policía Nacional.		
15. ASPECTOS DE CONFIDENCIALIDAD			
15.1	El personal que realice la instalación y configuración de los productos ofertados deberá someterse a un estudio de seguridad realizado por la Dirección de Inteligencia de la Policía Nacional, durante la vigencia del contrato,si se considera pertinente someter a estudio de seguridad al personal que prestará los servicios, el contratista permitirá y facilitará todos los medios que la Entidad le solicite para este fin.		
15.2	En virtud del presente estudio previo, el Oferente se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo. El oferente deberá firmar un acuerdo de confidencialidad y no revelación de la información, para lo cual deberá diligenciar el formulario "ACUERDO DE CONFIDENCIALIDAD".		
16. SERVICIOS PROFESIONALES			
16.1	Se debe presentar junto con el acta de iniciación del contrato, un cronograma de trabajo que relacione la instalación, configuración y las respectivas pruebas de aceptación.		
16.2	El oferente debe garantizar y certificar que el personal que prestará el servicio de soporte y mantenimiento son ingenieros debidamente certificados por la casa matriz del producto solicitado.		
17. DOCUMENTACIÓN TÉCNICA – ENTREGABLES			
17.1	Se debe entregar totalmente documentada la metodología de implementación y configuración de la herramienta ofertada siguiendo las recomendaciones de mejores prácticas de la casa matriz.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
17.2	El oferente deberá disponer de un sitio web de base de conocimiento en el cual se pueda realizar consulta de la documentación de la solución implementada, a su vez la metodología de implementación y configuración de la herramienta ofertada siguiendo las recomendaciones de mejores prácticas de la casa matriz.		
17.3	Toda la documentación debe entregarse en idioma español.		
17.4	Para el acta de inicio del contrato se debe anexar el cronograma detallado de actividades, indicando actividad, tiempo y responsables de la ejecución del contrato		
17.5	Manual de procedimientos de administración y operación de la solución ofrecida.		
18 SEGURIDAD DE INSTALACIONES			
18.1	Durante el tiempo de garantía el contratista deberá cumplir con el protocolo de seguridad de instalaciones y normas internas de seguridad física en cada una de las unidades policiales en todo el territorio colombiano y Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional (Resolución No. 08310 del 28/12/2016), para lo cual deberá diligenciar el formulario "SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO"		
19. SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO			
19.1	El contratista deberá cumplir con la implementación del sistema de Gestión de la Seguridad y Salud en el Trabajo, para lo cual deberán diligenciar el fomulario "SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO"		

21. EXPERIENCIA MÍNIMA DEL PROPONENTE

PROPONENTE NACIONAL

El Registro Único de Proponentes es el instrumento a través del cual los proponentes deberán acreditar el requisito de experiencia, para tal efecto las Personas Naturales, las Personas Jurídicas, las Uniones Temporales, los Consorcios, que participen en este proceso, para efectos de verificación de este requisito, deberán acreditar experiencia como se menciona a continuación:

El oferente deberá demostrar su experiencia específica hasta la fecha de cierre de la presente contratación, mediante la celebración de máximo tres (3) contratos identificados con el códigos del clasificador de bienes y servicios de Naciones Unidas descrito en el numeral 1.1 DESCRIPCIÓN GENERAL DEL OBJETO del presente estudio previo, cuyo objeto sea igual o similar al objeto del presente proceso y se relacione con LA SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM, celebrados con Entidades públicas y/o privadas, ejecutados y/o liquidados, para tal efecto se verificará en el Registro Único de Proponentes donde se acredite que dichas operaciones comerciales fueron realizadas antes del cierre de la presente contratación y que su valor sumado sea igual o superior al item a ofertar conforme al cuadro que se relaciona a continuación

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE	VALOR EXPRESADO EN SMMLV
43233200	Difusión de Tecnologías de información y telecomunicaciones	Software	Software de seguridad y protección	700

Nota 1: el Certificado de Registro Único de Proponentes constituye plena prueba respecto de la información verificada documentalmente y cuyo registro se encuentra vigente y en firme.

Nota 2: en la presentación de la oferta el oferente deberá diligenciar y entregar los formularios, donde relacionará los contratos que considere para la evaluación de la experiencia mínima requerida.

Cuando los documentos no indiquen su valor en SMMLV, o si estos son de años anteriores a 2022, se hará la respectiva conversión de acuerdo al año en que término el contrato. La verificación será realizada por el comité evaluador técnico.

Nota 3: si los contratos acreditados fueron realizados bajo la modalidad de Consorcio o de Unión Temporal, La Dirección Administrativa y Financiera tomará para la verificación, el porcentaje (%) de participación en la ejecución del contrato del oferente que haga parte del Consorcio o de la Unión Temporal, y luego sumará el valor obtenido para así establecer el total acreditado. Para lo anterior, deberá presentar el documento que acreditó la conformación del Consorcio o de la Unión Temporal, donde deberá constar el porcentaje de participación de cada uno de los integrantes para la ejecución del contrato.

Nota 4: en el caso que el proponente haya participado en procesos de fusión o escisión empresarial, debe tomar para estos efectos, exclusivamente los contratos que le hayan asignado en el respectivo proceso de fusión o escisión, para ello debe aportar el certificado del contador público o del revisor fiscal (si la persona jurídica tiene revisor fiscal) que así lo acredite.

Nota 5: si en la Información relacionada en el RUP para acreditar la experiencia mínima, se requiere verificar, la entidad se reserva el derecho de solicitar documentación adicional para verificar la información de la documentación entregada.

Nota 6: circular Externa No. 12 del 5 de mayo 2014 Colombia Compra Eficiente "La experiencia es un requisito habilitante. Los proponentes deben inscribir en el RUP su experiencia usando los códigos del Clasificador de Bienes y Servicios. Por su parte, las Entidades Estatales al establecer el requisito habilitante de experiencia deben incluir los códigos específicos del objeto a contratar o el de bienes, obras o servicios afines al Proceso de Contratación respecto de los cuales los proponentes deben acreditar su experiencia".

Nota 7: la Entidad podrá solicitar información adicional (que no conste en el RUP) para verificar la experiencia mínima requerida.

Nota 8: cuando el adjudicatario sea una persona natural, dentro de los tres días siguientes a la suscripción del acta de inicio, debe informar mediante documento a quien otorga facultades legales de representación en eventos de fuerza mayor a ocaso fortuito.

EXPERIENCIA PARA PERSONAS NATURALES O JURÍDICAS, EXTRANJERAS SIN DOMICILIO O SIN SUCURSAL EN COLOMBIA

Las personas naturales o jurídicas, extranjeras sin domicilio o sin sucursal en Colombia, que aspiren a celebrar contratos con las entidades estatales no requieren estar inscritos en el Registro Único de Proponentes, por ello se verificará la experiencia mediante la certificación de máximo tres (3) contratos celebrados y ejecutados con entidades públicas y/o privadas, que deban contener como mínimo la siguiente información:

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE	VALOR EXPRESADO EN SMMLV
43233200	Difusión de Tecnologías de información y telecomunicaciones	Software	Software de seguridad y protección	700

- Identificación de cada uno de los contratos.
- Nombre o razón social del contratante.
- Nombre o razón social del contratista.
- Objeto del Contrato
- Cuantía o valor del contrato.
- La certificación debe venir debidamente suscrita por la persona facultada para expedir dicho documento.
- Si la certificación incluye varios contratos, se deberán indicar los requisitos aquí exigidos para cada uno de ellos y se ponderará por contrato suscrito relacionado.
- Si la certificación incluye el contrato principal con sus adiciones se entenderá como un solo contrato certificado.
- Porcentaje del valor del contrato que ejecutó como miembro de un Consorcio, Unión Temporal, Sociedad de Objeto único, Empresa Unipersonal o Sociedades en general (Si es el caso).

- Porcentaje del valor del contrato que ejecutó como miembro de un Consorcio, Unión Temporal, Sociedad de Objeto único, Empresa Unipersonal o Sociedades en general (Si es el caso).

Nota 1: si son contratos realizados bajo la modalidad de Consorcio o de Unión Temporal, la DIRECCIÓN ADMINISTRATIVA Y FINANCIERA tomará para la verificación, el porcentaje (%) de participación en la ejecución del contrato del oferente que haga parte del Consorcio o de la Unión Temporal, y luego sumará el valor obtenido para así establecer el total acreditado. Para lo anterior, deberá presentar el documento que acreditó la conformación del Consorcio o de la Unión Temporal, donde deberá constar el porcentaje de participación de cada uno de los integrantes para la ejecución del contrato.

Nota 2: no podrá acumularse a la vez, la experiencia de los socios y la de la persona jurídica cuando estos se asocien entre sí para presentar propuesta

Nota 3: no se aceptarán auto certificaciones.

Nota 4: no se tendrán en cuenta las certificaciones de contratos en ejecución.

Nota 5: no se aceptan certificaciones con enmendaduras o que presenten inconsistencias no subsanadas de acuerdo con este pliego de condiciones.

Nota 6: en el caso que el proponente haya participado en procesos de fusión o escisión empresarial, debe tomar para estos efectos, exclusivamente los contratos que le hayan asignado en el respectivo proceso de fusión o escisión, para ello debe aportar el certificado del contador público o del revisor fiscal (si la persona jurídica tiene revisor fiscal) que así lo acredite

Nota 7: en el caso de sociedades que se escindan, la experiencia de la misma se podrá trasladar a cada uno de los socios escindidos, y se contabilizará según se disponga en los respectivos pliegos de condiciones del proceso

Nota 8: los proponentes extranjeros deben diligenciar el Formulario "CERTIFICACIÓN DE CONTRATOS PARA ACREDITACIÓN DE EXPERIENCIA PROPONENTE EXTRANJERO SIN SUCURSAL O DOMICILIO EN COLOMBIA" y/o "CLASIFICACIÓN PROPONENTE EXTRANJERO."

Nota 9: la entidad podrá solicitar información adicional para verificar la experiencia mínima requerida

Nota 10: cuando el adjudicatario sea una persona natural, dentro de los tres días siguientes a la suscripción del acta de inicio, debe informar mediante documento a quien otorga facultades legales de representación en eventos de fuerza mayor a ocaso fortuito.

La Policía Nacional **se reserva el derecho** de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin constatar el contenido de la misma.

Patrullero **JOJAN DANIEL PRADO FULA**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Patrullero **WILMER ALEXANDER BARACALDO CIFUENTES**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Intendente **ALEXANDER DIAZ CASTILLO**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Teniente **ANA CATHERINE MARIÑO RINCÓN**
Jefe Grupo Seguridad de la Información
Estructurador Estudio Previo

ANÁLISIS DEL RIESGO Y LA FORMA DE MITIGARLO

	Clase	Fuente	Etapa	Tipo	Descripción	Consecuencia de la Ocurrencia del Evento	Probabilidad	Impacto	Calificación Total	Prioridad	¿A quién se le asigna el riesgo?	Tratamiento controles a ser implementados	Impacto después del tratamiento				Afecta la ejecución del contrato	¿Afecta el equilibrio económico del contrato?	Persona responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se complementa el tratamiento	Monitoreo y Revisión	
													Probabilidad	Impacto	Calificación	Calificación total						¿Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?
1	GENERAL	EXTERNO	CONTRATACIÓN	ECONÓMICO	FLUCTUACIÓN EN EL PRECIO DEL DÓLAR SOBRE LA TASA REPRESENTATIVA DEL MERCADO	SOBRECOSTO EN LA ADQUISICIÓN, CON OCASIÓN DE LA IMPORTACIÓN DE BIENES	2	3	5	MEDIO	CONTRATISTA	EL CONTRATISTA EN SU OFERTA ECONÓMICA DEBERÁ CONTEMPLAR LAS VARIACIONES DE LA TASA REPRESENTATIVA DEL MERCADO, POR CUANTO EL PRESUPUESTO OFICIAL ASIGNADO, ES EN PESOS COLOMBIANOS	1	1	2	BAJO	SI	SI	CONTRATISTA	A PARTIR DE LA PRESENTACIÓN DE LA OFERTA	FINALIZACIÓN DEL CONTRATO	RECIBIDO A SATISFACCIÓN	ACTA DE RECIBO A SATISFACCIÓN
2	ESPECIFICO	EXTERNO	SELECCIÓN	OPERACIONAL	FALSEDAD EN LOS DOCUMENTOS QUE CONFORMAN LA OFERTA	DECLARATORIA DESIERTO DEL PROCESO DE CONTRATACIÓN	1	4	5	MEDIO	ENTIDAD	EVITAR EL RIESGO/VERIFICACIÓN ESTRICTA DE LOS DOCUMENTOS QUE CONFORMA LA OFERTA, POR PARTE DEL COMITÉ EVALUADOR	1	1	2	BAJO		NO	INTEGRANTES DE LOS COMITES EVALUADORES (JURÍDICO, ECONÓMICO Y TÉCNICO)	DE ACUERDO A LA CRONOLOGÍA DEL PROCESO	DE ACUERDO A LA CRONOLOGÍA DEL PROCESO	EVALUACIONES	DE ACUERDO A LA CRONOLOGÍA DEL PROCESO
3	ESPECIFICO	EXTERNO	SELECCIÓN	OPERACIONAL	NO CUMPLIMIENTO DE LOS REQUISITOS HABILITANTES POR NINGÚN OFERENTE	DECLARATORIA DESIERTO DEL PROCESO DE CONTRATACIÓN	2	3	5	MEDIO	ENTIDAD	ESTABLECER ADECUADAMENTE LAS ESPECIFICACIONES TÉCNICAS EN EL ESTUDIO PREVIO	1	2	3	BAJO		NO	ESTRUCTURADOR DEL ESTUDIO PREVIO	ELABORACIÓN DEL ESTUDIO PREVIO	ELABORACIÓN DEL ESTUDIO PREVIO	ESTUDIO PREVIO	EN LA APROBACIÓN DEL ESTUDIO PREVIO
4	GENERAL	EXTERNO	EJECUCIÓN	JURÍDICO	QUE EL PERSONAL QUE REALICE EL PROCEDIMIENTO DE INSTALACIÓN NO SEA IDÓNEO PARA LA EJECUCIÓN DEL PROCESO	INSTALACIÓN Y/O FUNCIONAMIENTO NO ADECUADO DE LOS EQUIPOS	2	3	5	MEDIO	ENTIDAD	EL CONTRATISTA DEBERÁ GARANTIZAR DESDE LA PRESENTACIÓN DE LA OFERTA QUE CUENTA CON PERSONAL EXPERTO E IDÓNEO PARA EJECUTAR EL CONTRATO	1	1	2	BAJO		SI	SUPERVISOR DEL CONTRATO	A PARTIR DE LA APROBACIÓN DE LA GARANTÍA ÚNICA	TERMINACIÓN DEL CONTRATO	INFORME AL ORDENADOR DEL GASTO	PERMANENTE
5	ESPECIFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	QUE SE REALICE LA INSTALACIÓN DE LOS EQUIPOS Y NO SE DE CUMPLIMIENTO AL PROCEDIMIENTO TÉCNICO ESTABLECIDO POR CADA FABRICANTE	FALLA EN EL SISTEMA DE ALMACENAMIENTO	4	3	7	MODERADO	CONTRATISTA	REDUCIR LA PROBABILIDAD DE OCURRENCIA, EL CONTRATISTA DURANTE LA EJECUCIÓN DEL CONTRATO DEBERÁ GARANTIZAR EL CUMPLIMIENTO AL PROCEDIMIENTO TÉCNICO ESTABLECIDO POR CADA FABRICANTE.	1	1	2	BAJO		SI	SUPERVISOR DEL CONTRATO Y CONTRATISTA	INICIO DEL CONTRATO	TERMINACIÓN DEL CONTRATO	INFORME AL ORDENADOR DEL GASTO	PERMANENTE

6	ESPECIFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	QUE EL PERSONAL REALICE TRABAJOS DE INSTALACIÓN, MANTENIMIENTO Y/O REPARACIÓN SIN EL DEBIDO CRONOGRAMA	NO SE REALICE LA INSTALACIÓN Y/O CONFIGURACIÓN A TODOS LOS EQUIPOS CONTEMPLADOS EN EL PRESENTE PROCESO	3	2	5	MEDIO	CONTRATISTA	REDUCIR LA PROBABILIDAD DE OCURRENCIA, EL SUPERVISOR DEL CONTRATO SOLICITARA AL CONTRATISTA UN CRONOGRAMA DE ACTIVIDADES	1	1	2	BAJO		NO	SUPERVISOR DEL CONTRATO	INICIO DEL CONTRATO	TERMINACIÓN DEL CONTRATO	CUMPLIMIENTO ESPECIFICACIONES TÉCNICAS DEL ESTUDIO PREVIO	CRONOGRAMA DE TRABAJO
7	ESPECIFICO	INTERNO	EJECUCIÓN	OPERACIONAL	QUE EL PERSONAL DE LA INSTITUCIÓN NO CUENTE CON EL CONOCIMIENTO NECESARIO PARA LA OPERACIÓN DE LOS SISTEMAS DE ALMACENAMIENTO OFERTADOS	FALLAS EN LA OPERACIÓN DE LOS SISTEMAS DE ALMACENAMIENTO.	4	3	7	MODERADO	ENTIDAD	EL CONTRATISTA DEBERÁ GARANTIZAR LA TRANSFERENCIA DE CONOCIMIENTO CERTIFICADO DE CADA UNO DE LOS SISTEMAS DE ALMACENAMIENTOS OFERTADOS	1	1	2	BAJO		SI	SUPERVISOR DEL CONTRATO	A PARTIR DE LA APROBACIÓN DE LA GARANTÍA ÚNICA	TERMINACIÓN DEL CONTRATO	INFORMES DE SUPERVISIÓN	DURANTE LA VIGENCIA DEL CONTRATO.
8	ESPECIFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	QUE SE PRESENTEN PROBLEMAS EN LA ATENCIÓN OPORTUNA DE LOS CASOS REPORTADOS POR EL SUPERVISOR DE CONTRATO	QUE SE PRESENTEN DAÑOS Y/O FALLAS EN LA SOLUCIÓN OFERTADA	4	3	7	MODERADO	CONTRATISTA	EL CONTRATISTA DEBERÁ GARANTIZAR QUE EN EL CASO DE PRESENTARSE DAÑOS Y/O FALLAS SE ATENDERÁ EN UN HORARIO DE ATENCIÓN 8X5 DÍAS A LA SEMANA	1	1	2	BAJO		SI	SUPERVISOR DEL CONTRATO	A PARTIR DE LA APROBACIÓN DE LA GARANTÍA ÚNICA	TERMINACIÓN DEL CONTRATO	INFORMES DE SUPERVISIÓN	DURANTE LA VIGENCIA DEL CONTRATO.
9	ESPECIFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	DURANTE LA EJECUCIÓN DEL CONTRATO NO SE COORDINE EL ACCESO AL SITIO, LO CUAL NO PERMITIRÍA CUMPLIR CON EL OBJETO CONTRACTUAL EN EL PLAZO ESTABLECIDO.	NO CUMPLA CON EL PLAZO DE EJECUCIÓN ESTABLECIDO EN EL CONTRATO.	3	3	6	ALTO	ENTIDAD	REDUCIR LA PROBABILIDAD DE OCURRENCIA BASADO EN LOS CRONOGRAMAS DE TRABAJO, LA SUPERVISIÓN DEL CONTRATO COORDINARA LA AUTORIZACIÓN DE ACCESO AL SITIO DE INSTALACIÓN CON EL FIN DE NO TENER INCONVENIENTES EN LA EJECUCIÓN DE CONTRATO.	1	2	3	BAJO	NO	SUPERVISOR DEL CONTRATO	A PARTIR DE LA APROBACIÓN DE LA GARANTÍA ÚNICA	TERMINACIÓN DEL CONTRATO	CORREO ELECTRÓNICO	DURANTE LA VIGENCIA DEL CONTRATO	A PARTIR DE LA APROBACIÓN DE LA GARANTÍA ÚNICA

NOTA: Con la presentación de la oferta, el oferente acepta y aprueba los riesgos propuestos por la Policía Nacional, así como el análisis realizado por la Entidad para su mitigación y gestión, de igual forma corresponde al estructurador del estudio previo, analizar los riesgos a los cuales se expone la entidad y el oferente frente a la ejecución del contrato, por cuanto cada proyecto es único en los factores ambientales, económicos, políticos, sociales y tecnológicos.

Jojan Daniel Prado.

Patrullero **JOJAN DANIEL PRADO FULA**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Patrullero **WILMER ALEXANDER BARACALDO CIFUENTES**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Intendente **ALEXANDER DIAZ CASTILLO**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Teniente **ANA CATHERINE MARIÑO RINCÓN**
Jefe Grupo Seguridad de la Información
Estructurador Estudio Previo

GARANTÍAS DEL PROCESO

ETAPA PRECONTRACTUAL

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACIÓN DE LOS RIESGOS	ESTIMACIÓN DEL RIESGO	ASIGNACIÓN DEL RIESGO	VIGENCIA	JUSTIFICACIÓN COBERTURA / VIGENCIA
Garantía de Seriedad	Riesgo Jurídico	La no suscripción del contrato sin justa causa	Diez por ciento (10%) del monto del contrato	Oferentes	Desde la presentación de la oferta y por tres (03) meses más.	Ampara la no suscripción del contrato sin justa causa, por el diez (10%) del monto del presupuesto oficial, desde la presentación de la oferta hasta la aprobación de la garantía que cubre los riesgos propios de la etapa contractual.
	Riesgo jurídico	La no ampliación de la vigencia de la garantía de seriedad de oferta cuando el término previsto en los pliegos para la adjudicación del contrato se prorrogue o cuando el término previsto para la suscripción del contrato se prorrogue, siempre y cuando esas prórrogas no excedan un término de tres (3) meses.				
	Riesgo jurídico	La falta de otorgamiento por parte del proponente seleccionado, de la garantía de cumplimiento exigida por la entidad para amparar el incumplimiento de las obligaciones del contrato.				
	Riesgo jurídico	El retiro de la oferta después de vencido el término fijado para la presentación de las propuestas				

ETAPA CONTRACTUAL

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACIÓN DE LOS RIESGOS	ESTIMACIÓN DEL RIESGO	ASIGNACIÓN DEL RIESGO	VIGENCIA	JUSTIFICACIÓN COBERTURA / VIGENCIA
Garantía única	RIESGO JURÍDICO	Incumplimiento del contrato	Veinte por ciento (20%) del valor del contrato	Contratista	Vigente por un término igual a la vigencia del contrato y sesenta (60) días calendario más	Ampara el riesgo de incumplimiento durante la vigencia del contrato y 60 días calendario más. La estimación del riesgo cubre el veinte por ciento (20%) del valor del contrato como quiera que se pretenda el pago parcial o definitivo de los perjuicios que cause a la entidad, en los mismos términos de la Cláusula Penal pecuniaria.
Garantía única	RIESGO OPERATIVO	Calidad de los bienes	Cincuenta por ciento (50%) del valor del contrato	Contratista	Vigente por un término igual a la vigencia del contrato y dieciocho (18) meses más para garantizar la calidad de los elementos y del servicio de instalación de los equipos	Ampara el riesgo de mala calidad de los bienes, vigente por un término igual a la vigencia del contrato y dieciocho (18) meses más para garantizar la calidad de los elementos y del servicio de instalación del presente proceso, La estimación cubre el cincuenta por ciento (50%) del valor del contrato lo que cubriría el perjuicio administrativo por la posible pérdida de los recursos, los gastos ocasionados por el proceso y la no entrega o de mala calidad del hardware y/o software, componentes y/o accesorios, buscando resarcir el detrimento

						causado a la entidad durante la vigencia del contrato.
Garantía única	Riesgo jurídico	No pago de salarios, prestaciones e indemnizaciones laborales	Cinco por ciento (5%) del valor total del contrato	Contratista	Vigente por un término igual a la vigencia del contrato y dieciocho (18) meses más.	Ampara a la Entidad de los perjuicios que se le ocasione como consecuencia del incumplimiento de las obligaciones laborales a que esté obligado el contratista derivadas de la contratación del personal utilizados para la ejecución del contrato.

CLÁUSULAS SANCIONATORIAS

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACIÓN DE LOS RIESGOS	ESTIMACIÓN DEL RIESGO	ASIGNACIÓN DEL RIESGO	VIGENCIA	JUSTIFICACIÓN COBERTURA / VIGENCIA
Multa	Riesgo jurídico	La no constitución dentro del término y en la forma prevista en el contrato o en alguno de sus modificatorios la póliza de garantía única	Multa cuyo valor se liquidará con base en un cero punto dos (0.2%) del valor del contrato	Contratista	La multa se aplicará por cada día de retardo y hasta por diez (10) días calendario.	Cuando el contratista no constituya dentro del término y en la forma prevista en el contrato o en alguno de sus modificatorios, a póliza de garantía única.
Multa	Riesgo jurídico	Incumplimiento parcial	Multas cuyo valor se liquidará con base en un cero punto cinco (0.5%) del valor dejado de cumplir o entregar	Contratista	La multa se aplicará por cada día de retardo hasta por un plazo de quince (15) días calendario que se descontará del saldo que le adeude la entidad. Esta sanción se impondrá mediante acto administrativo motivado en el que se expresará las causas que dieron lugar a ella	Ampara la mora o incumplimiento parcial de alguna obligación derivada del contrato por causas imputables al contratista
Clausula penal pecuniario	Riesgo jurídico	Incumplimiento total declaratoria de caducidad	Veinte por ciento (20%) del valor total del contrato	Contratista	El veinte por ciento (20%) del valor total del contrato cuando se trate de incumplimiento total del contrato y proporcional al incumplimiento parcial del contrato,	Ampara el incumplimiento parcial o definitivo del contrato por parte del contratista, se busca el pago parcial y definitivo de los perjuicios que se causen a la entidad, esta cláusula opera por el simple retardo.

Patrullero **JOJAN DANIEL PRADO FULA**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Patrullero **WILMER ALEXANDER BARACALDO CIFUENTES**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Intendente **ALEXANDER DIAZ CASTILLO**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Teniente **ANA CATHERINE MARIÑO RINCÓN**
Jefe Grupo Seguridad de la Información
Estructurador Estudio Previo

PÁGINA EN BLANCO

FICHA TÉCNICA DE PRODUCTO

DENOMINACIÓN DE BIEN O SERVICIO
SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM..

DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO
SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM..

UNIDAD DE MEDIDA
UNIDAD

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
1.1	El contratista deberá suministrar una (1) solución con soporte para cuarenta y cinco mil (45.000) equipos de cómputo (que soporte Sistema Operativo Windows, Linux y Macintosh) para uso continuo con derecho a actualizaciones y nuevas versiones (upgrade) por un término de dieciocho (18) meses y que cumpla las siguientes características: • Cuarenta y cinco mil (45.000) deben contar con módulo de Antivirus, Control de Dispositivos, Control de Aplicaciones y Data Lost Prevention (DLP) • Quince mil (15.000) debe contar con módulo de y Cifrado de Disco Duro • Veinte mil (20.000) de antispam para buzones de correo on-premise. La funcionalidad de la consola de administración antivirus, funcionalidad modulo antivirus en Windows server y Linux, La solución para estaciones de trabajo deben ser cumplidas por las cuarenta y cinco mil (45.000) licencias, estas deben ser administradas desde ambientes web, la diferencia en módulos se debe a las funcionalidades de cada uno de los equipos de cómputo, sus sistemas operativos y el nivel de riesgo al que se encuentran expuestos.
2.	**MODULO ANTIVIRUS Y CONTROL DE DISPOSITIVOS**
2.1	La solución debe ser desplegada mediante un agente.
2.2	La protección antivirus debe tener compatibilidad con los sistemas operativos Windows, Linux y Macintosh, incluyendo las nuevas versiones y estaciones de trabajo (45.000), incluyendo servidores de archivos Linux y una herramienta de administración y gestión remota, adicionalmente la solución deberá realizar la identificación de equipos no gestionados y la instalación de la solución en los mismos.
2.3	El módulo debe ser instalado en cuarenta y cinco mil (45.000) nodos, configurado y deberá quedar funcionando correctamente en los servidores Windows, Linux, así como en los clientes Windows, Linux en las versiones de 32 y 64 bits y Macintosh en las diferentes versiones con los que cuenta la Policía Nacional.
2.4	La solución de antivirus debe ser además compatible con sistemas Linux CentOS, RedHat, SUSE y Ubuntu.
2.5	Las políticas de antivirus definidas desde la consola deben poder ser aplicables para cualquier sistema operativo soportado. No se aceptará tener que definir políticas diferentes para diferentes sistemas operativos.
2.6	La solución debe contar con un mecanismo de actualización que garantice la integridad y minimice la manipulación o alteración de las definiciones de virus por medio de cifrado y firmas digitales. Esta función deberá ser implementada y estabilizada en la solución para la Policía Nacional.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
2.7	La solución debe contar con tecnología de remoción y detección de virus, macros, troyanos, gusanos, ransomware y en general todo tipo de códigos maliciosos. Esta función deberá ser implementada y estabilizada en la solución para la Policía Nacional.
2.8	El antivirus deberá ser estable, de tal manera que no afecte ni perjudique el rendimiento de las máquinas y/o aplicativos que estén instalados en las mismas, la solución se debe instalar y en máquinas con recursos limitados.
2.9	La solución debe permitir el aseguramiento de archivos, carpetas, elementos compartidos y evitar el desbordamiento de buffer. Esta función deberá ser implementada y estabilizada en la solución para la Policía Nacional.
2.10	La solución debe permitir el acceso en demanda, en segundo plano, proactivo, subsistema de prevención de brotes de virus y filtrado de contenido, protección sobre los protocolos HTTP, HTTPS, FTP y SMTP.
2.11	La solución debe contar y quedar configurado con un módulo de exploración en tiempo real, que ofrezca protección continúa frente a los virus que llegan a través de dispositivos de almacenamiento extraíbles, en la red y de las diversas fuentes en Internet.
2.12	La solución debe tener la capacidad de explorar los procesos que se encuentren corriendo en memoria.
2.13	La solución debe tener el control de la utilización de la CPU para tareas de exploración en demanda.
2.14	La solución debe explorar múltiples formatos de compresión de archivos como: (zip, rar, tar, gzip entre otros).
2.15	La solución debe permitir y quedar configuradas tareas calendarizadas de revisión y limpieza del sistema de archivos.
2.16	La solución debe tener la capacidad de analizar Scripts de Java y VBScript antes de que se ejecuten.
2.17	El antivirus debe contar con un módulo de exploración bajo demanda que permita iniciar una exploración en cualquier momento, especificar los objetivos (discos duros, carpetas, memoria, unidades extraíbles) y las exclusiones de la exploración, así como también determinar cómo debe responder el explorador cuando detecte un virus mostrando el informe detallado.
2.18	El antivirus debe permitirle al administrador las opciones de preguntas en cuanto a limpiar, borrar, denegar acceso, e inclusive debe manejar una carpeta de cuarentena para archivos infectados que se detecten a través de reglas y lista predefinidas y/o personalizadas por el administrador.
2.19	El motor de exploración deberá utilizar distintas tecnologías de detección virus: Exploración de firmas y exploración heurística "busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos".
2.20	La solución debe utilizar detección mediante técnica heurística que permita desenmascarar las amenazas evasivas mediante la combinación de análisis de reputación, con la clasificación dada por el aprendizaje automático y modelos de comportamiento.
2.21	La solución debe permitir la restauración automática de cambios que pudieran ser ejecutados por elementos considerados maliciosos.
2.22	Por cada producto debe entregarse una versión vigente en el mercado y soportada por la casa matriz.
2.23	La solución debe tener soporte para comunicaciones bajo IPv6 y soporte para IPv6 Firewall toda vez que IPv6 es una migración tecnológica que se debe llevar a cabo sobre las arquitecturas actuales.
2.24	La solución debe poder detectar comunicaciones a sitios de comando y control con el fin de evidenciar pérdidas de información en los clientes.
2.25	La solución debe contar con los mecanismos de protección para no poder ser desinstalada o desactivada por el usuario.

ITEM	CONDICIONES TECNICAS MINIMAS
2.26	La solución debe avisar sobre los posibles conflictos que existan de la solución a otras soluciones de antivirus y firewall instalados previamente en la máquina.
2.27	Se deben poder habilitar o deshabilitar los módulos de protección sin ser desinstalados del sistema.
2.28	La solución debe poder desplegar una aplicación cliente STANDALONE que pueda gestionar cambios localmente en caso de que se necesite.
2.29	Se debe poder restringir completamente o parcialmente el acceso a la consola cliente para configurar parámetros individuales sobre el host.
2.30	La desinstalación de la aplicación puede ser protegida mediante contraseñas desplegadas por políticas configuradas por el administrador.
2.31	Puede existir más de una configuración de idioma para la aplicación cliente.
2.32	La solución debe permitir a los administradores configurar escaneos bajo demanda en modo "escanear en reposo", para que se ejecuten sólo cuando el sistema esté inactivo.
2.33	El fabricante debe contar con centros de investigación globales con el objetivo de detectar incidentes en diferentes países/regiones y compartir inteligencia de amenazas con la organización.
2.34	La solución debe basarse en una plataforma común sobre la cual se incorporan módulos de Prevención de Amenazas, y Firewall de escritorio, y que permita el intercambio de información entre cada uno de los módulos.
2.35	La solución debe poder configurarse para realizar escaneos por demanda o programados, desde la consola de administración o desde la consola cliente. Dichos análisis pueden ser ejecutados en diferentes niveles de agresividad y umbral de consumos de recursos máximo sobre el sistema.
2.36	Se debe poder configurar acciones sobre infecciones identificadas: Denegar acceso / limpiar / Eliminar / Ninguna.
2.37	Se deben reportar eventos de amenazas directamente sobre la consola cliente y visibles desde la consola de administración de la solución.
2.38	La solución debe poder habilitar la opción de escaneo de clic-derecho sobre archivos y carpetas específicas.
2.39	Debe contar con mecanismos de protección de Exploits Generic Buffer Overflow Protección (GBOP) o integración con Microsoft DEP (Data Execution Prevention).
2.40	La solución debe contar con características de protección para navegadores web (Active X).
2.41	La solución debe contar con mecanismos de protección a ejecución de scripts maliciosos de Internet Explorer, sean JavaScript o VBScript.
2.42	La solución debe poder configurar mediante reglas o políticas de protección de: • Entradas y llaves de registro de Windows. • Prevención de creación de ejecutables portables (.INI, .PIF) • Creación de archivos autorun • Prevención de uso de archivos TFTP (Trivial File Transfer Protocol) • Contra lectura de archivos en cache de navegadores de internet • Creación y modificación remota de archivos o carpetas • Acceso remoto de archivos o carpetas. .EXE, .BAT y otros ejecutables bajo la llave de registro HKEY_CLASSES_ROOT • Modificación de procesos Core de Windows • Modificación de configuraciones de exploradores y navegadores web • Proteger procesos con subreglas personalizadas Asignar las reglas por nombre de usuario.
2.43	Utilizar modelos locales de aprendizaje en combinación con la clasificación de aprendizaje dada desde la nube, para identificar rápidamente el malware de día cero y comenzar la remediación.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
2.44	El sistema debe permitir la detección basada en el comportamiento anómalo en el punto final.
2.45	Contener aplicaciones desconocidas impidiéndoles realizar cambios a nivel del sistema, mediante reglas de Protección de acceso a aplicaciones y monitoreo de procesos en ejecución desconocidos.
2.46	La solución debe emplear una arquitectura multicapa, para defenderse de ataques basados en comportamientos, evitando cambios a nivel de sistema, restringiendo el acceso a procesos, archivos, recursos compartidos, valores y claves de registro específicos.
2.47	La solución debe poder identificar patrones similares de comportamiento dentro de diferentes variantes, usando reglas que pueden configurarse para evitar la instalación y / o la carga de nuevas variantes históricas, actuales y en evolución de amenazas de día cero.
2.48	La solución debe ser compatible con versiones soportadas de los navegadores Internet Explorer, Google Chrome, Mozilla Firefox.
2.49	Disponer de un motor antimalware que detecte infecciones y analice virus, gusanos, spyware, malware, ransomware y otras amenazas ubicadas en las estaciones de trabajo.
2.50	Debe estar diseñado para optimizar el rendimiento de los equipos y el consumo de ancho de banda.
2.51	Proteger las estaciones de trabajo contra infecciones a través descargas de internet, archivos adjuntos de e-mail, redes, archivos compartidos, CD-ROM, USB, dispositivos extraíbles, carpetas públicas y carpetas personales de todo tipo de correo, almacenadas localmente, mensajes de correo electrónico entrante y saliente, servicios en línea, entre otros tipos de almacenamiento.
2.52	La solución debe ser instalada, configurado y gestionado en cada estación de forma centralizada desde los servidores, sin tener que hacer un despliegue uno a uno.
2.53	La solución debe tener la capacidad de generar exclusiones por nombre de archivos, carpetas y tipos de archivos.
2.54	Debe contar con medidas de seguridad para que el usuario o cliente no pueda modificar políticas corporativas efectuadas desde la consola de administración.
2.55	La solución debe ser capaz de detectar el 100% de los virus conocidos (reportados en listas), contra programas malignos especificados.
2.56	Debe anticiparse a los virus desconocidos e intrusos mediante herramientas que supervisen los procesos en ejecución en busca de comportamientos maliciosos.
2.57	La solución de protección de endpoint debe tener la capacidad de detectar, detener y eliminar códigos o aplicaciones maliciosas como: gusanos, troyanos, spyware, ad-ware, keyloggers, ramsonware y cualquier otro programa potencialmente peligroso.
2.58	Debe permitir generar informes detallados con los datos referentes a la detección de virus tanto en tiempo real, como del análisis bajo demanda y programado.
2.59	Análisis en tiempo real de amenazas sobre los dispositivos extraíbles antes de tener acceso a los archivos en ellos almacenados.
2.60	La solución debe contar con mecanismos de protección de amenazas avanzadas tipo ransomware.
2.61	La solución debe contar con mecanismos de borrado seguro de malware residente en memoria que sean difíciles de erradicar, evitando el reinicio de servidores críticos.
2.62	La solución debe contar con tecnología de prevención/mitigación de EXPLOITS, que ataquen soluciones comúnmente usadas y que pueden no estar actualizadas, como acrobat, flash player, entre otras.
2.63	La solución debe mitigar la explotación de vulnerabilidades sobre sistemas operativos cliente y servidor.

ITEM	CONDICIONES TECNICAS MINIMAS
2.64	La solución debe contar con mecanismos que permitan prevenir un evento destinado a aprovechar la ausencia de configuraciones y/o parches específicos de sistema operativo.
2.65	La solución debe contar con funcionalidades de detección de amenazas avanzadas sin necesidad de requerir actualizaciones frecuentes de firmas de virus, de manera que se pueda garantizar la protección en máquinas que se encuentren desconectadas de la red la policía y/o internet por largos periodos de tiempo.
2.66	La solución debe contar con la aplicación de políticas de acuerdo con la identificación de la red a la cual se encuentre conectada la máquina.
2.67	La solución o servicio ofrecido deberá realizar la desinstalación de los productos de protección actualmente instalados sobre los dispositivos de la organización en caso de ofrecer una solución o versión de producto diferente a la utilizada.
2.68	El módulo de Control de Dispositivos debe permitir la creación de excepciones para un usuario, maquina o dispositivo especifico.
2.69	El módulo de Control de Dispositivos debe permitir asignar reglas y políticas para usuarios y grupos de Directorio Activo.
2.70	El módulo de Control de Dispositivos debe tener la capacidad de monitorear las actividades del usuario relacionadas al dispositivo removible de manera silenciosa.
2.71	El módulo de Control de Dispositivos debe tener la capacidad de bloquear los dispositivos de almacenamiento extraíbles, incluyendo CD / DVD y USB entre otras.
2.72	El módulo de Control de Dispositivos debe tener la capacidad de bloquear los dispositivos "Plug and Play".
2.73	El módulo de Control de Dispositivos debe tener la capacidad de poner como de solo lectura a los dispositivos de almacenamiento removible.
2.74	El módulo de control de dispositivos debe tener la capacidad de integrarse con el módulo de cifrado.
2.75	El módulo de Control de Dispositivos debe permitir la creación de categorías de dispositivos a necesidad/personalizados.
2.76	La solución debe permitir compartir de forma instantánea la información sobre amenazas con otras soluciones de seguridad conectadas, incluidas las de terceros.
2.77	La solución de Control de Dispositivos debe permitir la protección de toda la red contra acceso y uso de los dispositivos USB, permitiendo solo los autorizados por la organización.
2.78	El módulo de Control de Dispositivos debe permitir auditar la conectividad de los dispositivos de almacenamiento externo.
2.79	El módulo de Control de Dispositivos debe poder ser desplegado de manera centralizada, a través de la consola de administración o a través de herramientas de distribución de software suministrada.
2.80	El módulo de Control de Dispositivos debe tener la capacidad de inspeccionar en tiempo real, la carga de información hacia un medio removible, con el objetivo de identificar documentos confidenciales y tomar acciones tales como bloqueo, registro, notificación.
2.81	El módulo de Control de Dispositivos debe permitir la creación y manejo de listas blancas y negras de dispositivos tomando en cuenta atributos tales como VID (Vendor ID) y PID (Product ID).
2.82	El módulo de Control de Dispositivos debe tener la capacidad de permitir los dispositivos de almacenamiento removible al menos que se encuentren permitido a través de listas blancas.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
3. FUNCIONALIDAD MODULO ANTIVIRUS EN WINDOWS SERVER Y LINUX	
3.1	Disponer de un motor antimalware o antispyware que detecte infecciones y analice virus, gusanos, y otras amenazas ubicadas en los servidores.
3.2	La remediación o creación de firmas para las amenazas de día cero no deberán superar veinticuatro (24) horas una vez reportada al fabricante.
3.3	Actualización diaria, incremental y automáticamente, así como patrones de comportamiento de los nuevos virus.
3.4	Gestión centralizada y remota de la red con múltiples vistas gráficas de los servidores para un fácil reparto de las tareas entre los administradores.
3.5	Exclusión del análisis en base a extensiones o ficheros que no se desee ser analizados.
3.6	Debe permitir definir el umbral de consumo de recursos del sistema analizado al momento de programación un análisis del sistema.
3.7	Debe realizar el análisis de archivos comprimidos por demanda.
3.8	En los casos que un fichero no se pueda desinfectar, en análisis de tiempo real o bajo demanda, debe permitir borrar y/o enviar a cuarentena dicho fichero.
3.9	Debe disponer de un producto especializado para ser implementado en los servidores virtuales existentes en infraestructura tecnológica de la Policía Nacional (Oracle, Hyperv). que suman 200 servidores virtuales y 200 físicos.
3.10	Debe quedar instalado en los servidores de archivos y sharepoint.
4. FUNCIONALIDAD DE LA CONSOLA DE ADMINISTRACIÓN ANTIVIRUS	
4.1	Despliegue, actualización, administración y soporte a toda la solución de seguridad ofertada; funcionalidades que deben efectuarse a través de una consola de gestión de políticas de seguridad y tareas.
4.2	Debe interactuar con las consolas de administración que tiene actualmente la Policía Nacional (Directorio Activo – Microsoft), a fin de poder forzar el despliegue de políticas de seguridad e instalación hacia los dispositivos a ser protegidos.
4.3	Debe disponer de un filtrado de vistas de las estaciones de trabajo y servidores instalados como mínimo con las siguientes características: • Estado del cliente • Ultimas Conexiones • Dirección IPv4/IPv6
4.4	Debe permitir la detección y bloqueo remoto de equipos infectados, evitando, de esta manera, la propagación de amenazas a través de la red.
4.5	Permitir la ejecución de tareas de instalación, despliegue o desinstalación de forma remota, reconociendo a los equipos por su dirección o rango de direcciones IP, nombre, pertenencia a dominio, lista plana.
4.6	La solución debe poder ser administrada de forma segura vía web utilizando el protocolo HTTPS
4.7	Capacidad de detectar equipos no gestionados en la red y sobre los cuales no se ha desplegado las técnicas de protección requeridas.
4.8	Capacidad para descargar las actualizaciones desde Internet a través de las versiones seguras de los protocolos FTP y/o HTTP, colocándolas en múltiples repositorios distribuidos donde los clientes puedan buscar las definiciones de manera local, lo cual permite un ahorro en el ancho de banda.
4.9	Capacidad de programar las actualizaciones para que sean realizadas en diferentes momentos y horas específicas (diaria, semanal, mensual, cuando la máquina este inactiva, inmediatamente, entre otras).
4.10	Capacidad de actualizar automáticamente los archivos de definiciones de virus, motor antivirus, ficheros de firmas y actualizaciones del producto antivirus de forma: automática, centralizada e incremental.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
4.11	Capacidad de generar reportes ilimitados, detallados y personalizados por fecha, tipo de amenaza, amenazas detectadas y/o eliminadas, equipos infectados y/o desinfectados.
4.12	La solución debe quedar instalada en modo alta disponibilidad y balanceo de cargas, con el fin de garantizar un plan de recuperación y continuidad en caso de desastre. El oferente deberá garantizar todos los requerimientos para esta instalación.
4.13	La solución deberá permitir manejar una estructura distribuida donde los sistemas en diferentes locaciones puedan replicar políticas y eventos desde un punto hacia la consola de gestión. La solución deberá permitir la instalación de múltiples consolas para mantener un esquema de gestión independiente en caso sea requerido.
4.14	Disponer de información que permita ver el estado de seguridad y mantenimiento de los productos de toda la solución.
5. MÓDULO CONTROL DE APLICACIONES	
5.1	El módulo de control de aplicaciones debe ser instalado para Dieciocho mil (18.000) nodos.
5.2	El módulo de control de aplicaciones debe proporcionar un módulo de descubrimiento de aplicaciones instaladas en cada uno de los hosts, este reporte debe ser entregado al momento de la instalación, por demanda y/o definido a criterio del administrador, adicionalmente debe permitir la desinstalación remota desde la consola de administración del software que el administrador defina.
5.3	La solución debe estar en la capacidad de generar lista blanca de aplicaciones, ejecutables y librerías independientemente si se encuentran instaladas y/o en uso.
5.4	El módulo de control de aplicaciones debe permitir definir listas blancas de aplicaciones que pueden ser ejecutadas en los equipos de cómputo protegidos, esta lista podrá ser modificada en cualquier momento sin restricción.
5.5	Las listas deben ser creadas de forma independiente por cada uno de los equipos protegidos, deben ser usadas para la realización de inventario de software y para el control de la ejecución de las mismas.
5.6	El módulo de control de aplicaciones debe permitir definir listas negras de aplicaciones que no pueden ser ejecutadas, ni instaladas en los equipos de cómputo protegidos (de forma global para toda la plataforma), esta lista podrá ser modificada en cualquier momento sin restricción.
5.7	La solución debe poder realizar inventario de las estaciones de trabajo el cual permitirá conocer las aplicaciones instaladas en estos.
5.8	La solución permitirá proteger estaciones de trabajo mediante el control de la ejecución de aplicaciones, realizado a través de listas blancas y negras, por medio de la prevención de modificaciones hacia los archivos del punto final.
5.9	La solución debe emplear un modelo de confianza y/o monitoreo de comportamiento para bloquear las aplicaciones no autorizadas o maliciosas.
5.10	Debe contar con mecanismos de protección de memoria para contrarrestar los ataques de buffer overflow sobre las aplicaciones en lista blanca.
5.11	Debe proteger contra las amenazas persistentes avanzadas y de tipo zero-day sin actualizaciones de firmas.
5.12	La solución deberá permitir a los usuarios ser notificados sobre la razón por la cual la aplicación ha sido bloqueada.
5.13	La solución deberá permitir a usuarios específicos que puedan instalar nuevo software en caso de que sea necesario, sin necesidad de autorización adicional.
5.14	La solución deberá tener protección contra lectura y escritura de archivos.
5.15	La solución deberá soportar los siguientes sistemas operativos Microsoft Windows server: 2008, 2008 R2, 2012, 2012 R2, y posteriores Además de los siguientes para estación de trábajo: 7, 8, 8.1, 10, 11 y posteriores.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
5.16	La solución deberá soportar los siguientes Sistemas Operativos de Microsoft los cuales ya no cuentan con soporte del fabricante: 2003, 2003 R2, Windows XP.
5.17	La solución deberá soportar los siguientes sistemas operativos de Microsoft Windows Embedded: XPE, 7E, WEPOS, POS Ready 2009, WES 2009, 8 Industry, 8.1.
5.18	La función de protección de escritura y cambios a los sistemas deberá proteger de: • Eliminar • Modificar Contenido • Cambiar Propietario • Truncar
5.19	La solución debe proveer un panel de monitoreo para poder visualizar los cambios y violaciones en los equipos finales.
5.20	El control de aplicaciones debe permitir realizar la desinstalación de software de forma remota.
5.21	Reconocimiento de anomalías, detección y bloqueo de ataques de tipo Host Sweep, TCP or UDP port Scan, CGI Holes, entre otros.
5.22	Detección de ataques de tipo Exploits hacia vulnerabilidades de sistema operativo como también de aplicaciones diferentes de Microsoft.
5.23	El módulo de control de aplicaciones debe incluir un sistema de detección y prevención de intrusos basados en host que proteja los recursos del sistema y las aplicaciones de ataques internos y externos.
5.24	El módulo de control de aplicaciones debe contar con una consola de administración o integrarse con la consola general de administración de la solución, adicionalmente deberá poder integrarse con sistemas de colección de eventos vía syslog o enviadas al SIEM (Enterprise Security manager McAfee) de la Policía Nacional.
5.25	El módulo de control de aplicaciones debe contar con un Firewall personal para los equipos Windows.
5.26	El módulo de control de aplicaciones debe permitir obtener estadísticas del software instalado en los equipos de cómputo, intentos de instalación de aplicativos que se encuentren en listas negras, entregando hora, máquina y usuario que intenta realizar la instalación.
5.27	El módulo de control de aplicaciones debe contar con la opción de bloquear todas las aplicaciones por defecto y generar listas blancas creadas por la casa matriz de acuerdo a reputación del sitio de descarga, hash, checksum, nombre, lista blanca, definición del administrador, entre otros. Adicionalmente La solución deberá permitir a los usuarios ser notificados sobre la razón por la cual la aplicación ha sido bloqueada.
5.28	Capacidad de generar reportes ilimitados, detallados y personalizados por fecha, tipo de amenaza, amenazas detectadas y/o eliminadas, equipos infectados y/o desinfectados.
6. DATA LOST PREVENTION - DLP	
6.1	El módulo Data Lost Prevention - DLP debe ser instalado para Cuarenta y Cinco Mil (45.000) nodos.
6.2	La solución debe basarse en un agente que se instala en cada computadora y servidor que servirá como medio de comunicación entre las estaciones de trabajo y la consola de administración.
6.3	La solución debe tener una base de datos de Microsoft SQL u Oracle en la cual deberá guardar todos los informes sobre la detección de violaciones de políticas.
6.4	La solución deberá permitir crear diferentes sets de permisos para asignar diferentes tipos de administración a usuarios y grupos.
6.5	La solución deberá contar con un tablero de Analíticos, este tablero podrá mostrar los incidentes basados en la clasificación.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
6.6	La solución de protección de fuga de información del endpoint deberá contar con un agente para sistemas operativos MAC donde los usuarios de dicha plataforma puedan aplicar: Reglas de acceso por medio de aplicaciones, reglas de protección Cloud, reglas para protección de compartir en red y dispositivos removibles.
6.7	La solución deberá integrarse con Active Directory y permitir hacer inicio de sesión a la consola de administración utilizando las credenciales de red con sus respectivos permisos.
6.8	La solución debe tener la capacidad de administrar, configurar, instalar, desinstalar, actualizar, asignar políticas para el software de Control de dispositivos y Prevención de Fuga de Información (DLP).
6.9	La solución debe llevar como minimo 6 años consecutivos como líder en el cuadrante de Gartner de prevención de fuga de datos.
6.10	La solución debe identificar contenidos basados en tipo de contenido/documento.
6.11	La solución debe monitorear el contenido que viaje a través del ENDPOINT, por dirección IP y protocolo.
6.12	La solución debe monitorear el contenido que viaje a través el ENDPOINT, debido al acceso de aplicaciones.
6.13	La solución debe permitir crear políticas para dispositivos extraíbles de almacenamiento, por fabricante.
6.14	La solución debe poder identificar contenido usando expresiones regulares, palabras clave, las funciones hash, y la coincidencia de patrones.
6.15	La solución debe poder identificar el contenido basado en localización.
6.16	La solución debe poder identificar el contenido usando FINGERPRINT.
6.17	La solución debe cumplir las políticas aplicadas de protección de fuga de información, sin importar que el equipo final se encuentre fuera de la red corporativa.
6.18	La solución debe contar con una funcionalidad de Soporte de virtualización mejorada. Es decir que cada política por usuario debe ofrecer flexibilidad y un mejor control de los datos que fluyen a las terminales compartidas e infraestructuras de escritorio virtual (VDI). Así, las políticas por usuario deben aplicar a múltiples sesiones.
6.19	La solución debe brindar protección a nivel de portapapeles para ambos: "copia de" y "pegar", además de protección de captura de pantalla para proteger el diseño de productos y códigos fuente contra la pérdida de datos intencional y no intencional. Garantizando esta protección incluso si se utilizan métodos alternativos como aplicaciones de recortes de office, one note, navegadores, entre otros.
6.20	La solución debe permitir la configuración de incidentes de acuerdo con sus propiedades para una revisión posterior. Las propiedades deben ser como mínimo: • Severidad • Estatus • Resolución • Revisor
6.21	La solución debe contar con mecanismos que prevengan la vista no autorizada de información confidencial, a través del módulo de manejo de incidentes, limitando la vista de incidentes sólo a revisores o administradores con un rol cuyos privilegios se lo permitan.
6.22	La solución de contar con reglas de protección que estén basadas en: tipo de archivo, extensiones de archivo, propiedades de documento, tipos de encripción y asignación de usuarios o grupos.
6.23	La solución debe permitir usar repositorios para evidencia.
6.24	La solución deberá replicar de forma manual o automática a través de tareas el software para las actualizaciones e instalaciones.
6.25	La solución deberá permitir crear políticas para clasificar el contenido sensible por medio de categorización de aplicaciones como; editores, exploradores, confiables y archivadores.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
6.26	La solución debe tener la capacidad de obtener información completa sobre las propiedades del documento sensible como; quien lo grabo de último, el título, autor, comentarios, etc.
6.27	La solución debe permitir crear configuraciones por grupo, dominio o maquina sin afectar la estructura del árbol de administración.
6.28	La solución debe controlar la impresión usando impresoras locales, en red, print screen e impresión en PDF.
6.29	La solución no debe de requerir el reinicio de la computadora al instalar o hacer actualización.
6.30	La solución debe controlar la carga de información sensible hacia aplicaciones de la nube como Box.inc, Dropbox, Google Drive, iCloud, OneDrive (personal) OneDrive for Business (groove.exe) y Simplicity.
6.31	La solución debe contar con una lista de reglas de acción para realizar como mínimo lo siguiente: • Sólo lectura • Reportar a la consola central • Poner en cuarentena • Cifrar • Guardar la evidencia • Solicitar justificación • Notificar al usuario • Monitorear • Bloquear
7. ARQUITECTURA	
7.1	La solución debe contar con una arquitectura distribuida para optimización de funcionalidades.
7.2	Deberá contar con la creación de patrones avanzados para reducir los falsos positivos.
7.3	La solución deberá tener mecanismos de control de incidentes para su revisión y operaciones como; Manejo de caso, comentarios, envió por correo, etc.
7.4	La solución debe presentar un flujo de trabajo que debe contar con una fase de clasificación o definición, una fase de identificación y registro, una fase de protección y una fase de monitoreo.
7.5	La solución debe integrarse con soluciones de Rights Management (IRM) como: • Microsoft Windows Rights Management Services • Seclore FileSecure information Rights Management Con el objetivo de aplicar políticas de RM a archivos detectados en escaneos de descubrimiento y poder incluir o excluir archivos protegidos por RM, de las reglas de protección de correo, almacenamiento removible, sistemas de archivos y web posting.
7.6	Debe de permitir la integración con etiquetado de terceros como: • TITUS • Boldon James
7.7	La solución debe contar con una consola de gestión centralizada, desde la cual sea posible gestionar políticas, reglas de protección de información.
7.8	La interfaz de monitoreo de la solución debe proveer un panel para el manejo de incidentes, separado de un panel para eventos operacionales, donde se muestren eventos administrativos.
7.9	La solución debe contar con la posibilidad de hacer control de acceso basado en roles.
7.10	Se requiere que la solución posea una consola de administración vía web.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
7.11	Los revisores o administradores de la consola deberán poder auditar las siguientes acciones: • Entrada al servidor de administración • Cambio de perfiles o roles • Cambio de contraseñas • Cambios de políticas Esta característica es importante cuando se desea descubrir cambios ocurridos en el servidor de administración.
7.12	El agente debe registrar todas las violaciones e informes en la base de datos central de la consola, cuando se establece una conexión a la red corporativa.
7.13	La solución deberá contar con reportes predefinidos y la posibilidad de crear nuevos a partir de queries personalizados.
7.14	La solución debe soportar reglas y exclusiones basadas en directorio de datos para reforzar las políticas basándose en cualquier atributo del documento y/o receptor.
7.15	La solución debe incluir una biblioteca de plantillas predefinidas de detección orientadas al cumplimiento con regulaciones locales y globales como la Ley de protección de datos (Ley 1581, SOX, PCI y HIPAA.), Si la solución no incluye la plantilla el proveedor deberá crear dicha plantilla y dejarla en operación.
7.16	La solución debe permitir detectar y analizar archivos y anexos de correo de tamaños mayores a 20 MB sin verse afectado el rendimiento de los equipos.
7.17	La solución debe permitir especificar el grado de proximidad como una condición de una coincidencia para un incidente.
7.18	La solución debe detectar la información sin importar que el orden de los datos haya sido alterado.
7.19	La solución deberá estar en la capacidad de detectar contenido confidencial incluso si el nombre o tipo de archivo es modificado.
7.20	La solución debe soportar la detección de coincidencias en un contenido con exactitud del 100% para documentos específicos tales como código fuente, documentos financieros, etc.
7.21	Debe ser posible definir un umbral o porcentaje mínimo requerido de coincidencia de un documento para considerar que existe una violación a la política configurada.
7.22	La solución debe permitir la detección basada en expresiones regulares.
7.23	La solución debe permitir la detección o presencia de archivos cifrados.
7.24	La herramienta podrá ser integrada con herramientas de cifrado de datos, para que en el caso de detectar contenido sensible tenga como respuesta el cifrado de la información.
7.25	La solución debe permitir notificar automáticamente a remitentes administradores y jefes inmediatos de un usuario cuando este ha violado una política.
8. CIFRADO	
8.1	El módulo de cifrado debe ser licenciado y configurado para quince mil (15.000) nodos.
8.2	La solución de cifrado de discos debe permitir el cifrado en los sistemas operativos Microsoft, Linux y MAC.
8.3	La solución debe permitir la integración con el directorio activo.
8.4	La solución de cifrado debe permitir la creación de políticas a través de grupos del directorio activo.
8.5	La solución de cifrado debe contar con una consola de administración centralizada.
8.6	La solución debe permitir el envío de tareas remotas tales como cifrar y descifrar desde la consola de administración.
8.7	La solución de cifrado debe permitir tener una recuperación centralizada a través de la consola de administración.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
8.8	La solución de cifrado debe permitir tener SSO (Single Sign-On) con el directorio activo para el acceso a las maquinas cifradas.
8.9	La solución de cifrado de discos deberá integrar en el mismo licenciamiento la funcionalidad de cifrado de archivos que se copian a medios removibles.
8.10	La solución de cifrado de discos debe tener una funcionalidad que se copie en los medios extraíbles para ver la información cifrada en equipos que no tengan ninguna solución de cifrado. Esta funcionalidad debe poder abrirse en Windows y MacOSX.
8.11	La solución de cifrado debe permitir crear una contraseña para el cifrado de todos los archivos que se copian a los medios extraíbles o tener una contraseña según las preferencias del usuario.
8.12	Las contraseñas que se crean para la copia de archivos a medios extraíbles deben permitir configurar complejidad.
8.13	La solución de cifrado debe permitir generar informes del estado de los discos administrados y cifrados.
8.14	La solución de cifrado debe permitir la configuración de un método de seguridad cuando se ingrese la contraseña incorrectamente un determinado número de veces. Ejemplo evitar la autenticación durante determinado tiempo.
8.15	La solución de cifrado debe permitir configurar un tiempo de expiración de las contraseñas.
8.16	La solución debe permitir la configuración del periodo de conexión entre los agentes de cifrado y la consola centralizada.
8.17	La solución de cifrado debe permitir la autenticación en las maquinas cifradas con password, token o token y password.
8.18	La solución de cifrado debe tener métodos de recuperación ante desastres, en caso de que exista daño en el sistema operativo, el usuario olvide su contraseña y/o los métodos de recuperación no funcionen.
8.19	La solución de cifrado debe soportar cifrado AES 256 Bits.
8.20	La ventana de Preboot debe permitir la personalización de logo y mensaje de bienvenida.
8.21	La solución de cifrado de discos debe permitir el cifrado de solo el Boot de inicio o de todos los discos según se requiera.
8.22	La consola de administración de cifrado de discos duros debe permitir visualizar las particiones cifradas y las no cifradas.
8.23	El agente de cifrado de discos debe permitir visualizar las unidades que están cifradas y descifradas en la máquina.
8.24	El agente de cifrado de discos debe permitir ver un porcentaje del proceso de cifrado de discos.
8.25	La solución de cifrado de medios removibles debe permitir crear exclusiones para evitar que determinadas extensiones de archivos se cifren automáticamente.
8.26	La solución de cifrado de medios extraíbles debe permitir crear exclusiones de dispositivos que no se cifraran.
8.27	El producto debe soportar las siguientes maquinas clientes: • Windows 7 and SP1 (32- and 64-bit), (Not XP Mode) • Windows 8 • windows 10 • Windows 11 y posteriores
8.28	La solución debe poseer al menos las siguientes certificaciones: • Common Criteria EAL2 +, FIPS 140-1, FIPS 140-2 • AES CBC (e/d; 256).

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
8.29	La solución debe soportar al menos los siguientes algoritmos de Encriptación: • AES-256.
8.30	La solución de cifrado debe permitir el cifrado de archivos que sean transferidos a dispositivos de almacenamiento extraíble.
8.31	La solución de cifrado debe permitir generar excepciones sobre dispositivos donde no se debe aplicar el cifrado.
8.32	Debe tener la capacidad de cifrar el disco completo, reemplazando el Master Boot Record (MBR).
8.33	La solución debe proveer mecanismos seguros que garanticen la recuperación del acceso en caso de pérdida de la contraseña. Estos mecanismos deben requerir la intervención y el intercambio de información con la consola de administración.
8.34	Debe ser capaz de descifrar el disco en forma automática, desde la consola de administración y mediante mecanismos manuales.
8.35	La solución debe solicitar autenticación al usuario antes de iniciar la carga del sistema operativo (SO). Luego de iniciar el SO, la solución debe poder configurarse de manera que solicite o no, nuevamente, las credenciales de autenticación del usuario.
8.36	Las actualizaciones de la solución deberán realizarse remotamente y desde una consola de administración centralizada.
8.37	La arquitectura de la solución debe ser cliente-servidor.
8.38	La solución debe emplear el mínimo de utilización de recursos del CPU.
8.39	La solución debe tener la capacidad de realizar single Sign-On en sistemas operativos Windows permitiendo el acceso a la maquina mediante las credenciales de Windows y reduciendo los procesos para ingresar.
8.40	La solución debe soportar la unificación del usuario y contraseña utilizadas por el usuario en el directorio Activo de Microsoft.
8.41	La solución debe contar con una herramienta externa que utilice las Llaves de Encriptación almacenadas en la consola de administración para ejecutar cualquier actividad de recuperación de discos o archivos.
8.42	La solución debe soportar Single Sign-On (SSO) en integración con las políticas de grupo (GPO) del Directorio Activo de Microsoft.
8.43	La solución debe contar con la opción de generar un "código de respuesta" para la recuperación del administrador.
8.44	El acceso de los usuarios administradores a la consola de administración debe poder hacerse basado en roles.
8.45	La consola de administración debe permitir la creación de políticas de autenticación que no sean de alcance global.
8.46	La solución debe proveer reportes del estado de la solución en las maquinas administradas. Todos estos reportes deben ser exportables vía correo o a documentos PDF, XLS y CSV.
8.47	La solución debe proveer un reporte de los sistemas cifrados, mostrando un estado de Cifrado o Descifrado.
8.48	La solución debe ser capaz de enviar reportes y notificaciones por email en los siguientes formatos: • CSV • XLS • PDF
8.49	La solución debe permitir generar reportes basados en eventos históricos.
8.50	La solución debe contener reportes y consultas (query) que se puedan personalizar.
8.51	La solución debe contar con la funcionalidad de que gestionar Native Encryption.
8.52	La solución debe ofrecer beneficios en común para la gestión sobre FileVault y BitLocker:

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
	• Posibilidad de actualizar una versión OS X a la siguiente sin tener que descifrar y volver a cifrar el disco. • Compatibilidad de día cero con parches, actualizaciones y actualizaciones de firmware de Apple y Microsoft. • Característica de recuperación que permite a los usuarios restablecer el acceso a sus máquinas. • Fácil administración
8.53	La solución debe ofrecer beneficios para entornos Mac: • Capacidad de hacer SSO desde el entorno de Pre-Boot de FileVault directamente al inicio del ambiente de OS X. • Administración de File Vault en un HW que puede ejecutar OS X Mountain Lion, Mavericks o Yosemite, desde una consola centralizada. • Generación de reportes de cumplimientos y elaboración de tableros de control. • Apoyo a las herramientas y flujos de trabajo para la recuperación de información proveídas por Apple (FileVault Recovery Key) • Permitir a los administradores la importación manual de FileVault Recovery Keys donde ya manualmente los usuarios han habilitado File Vault.
8.54	Beneficios para entornos Windows: • Soportar dispositivos certificados Windows To Go • Administrar de BitLocker en hardware Windows 7 u 8, 10 y 11 desde una única consola • Proveer una experiencia transparente al usuario (Trusted Platform Module - TPM) • Soportar los requerimientos FIPS 140-2. • Soportar Microsoft eDrive. • Generación de reportes de cumplimientos y elaboración de tableros de control • Administración de BitLocker sin la necesidad de contar con un servidor Microsoft BitLocker Management and Monitoring (MBAM).
9. SOLUCIÓN DE SEGURIDAD PERIMETRAL DE CORREO - ANTISPAM	
9.1	Se requiere una solución de tipo "Gateway" que permita la inspección profunda de los correos electrónicos contra las siguientes amenazas: spam, phishing, virus, ataques de directorio, ataques de rebote (bounce attacks) y filtrado de contenidos para 20.000 buzones.
9.2	El fabricante de la solución deberá ofrecer detectar el 99,9% de Spam con un número de Falsos positivos menor o igual a 1 en un millón.
9.3	El dispositivo deberá estar soportado para correr tanto en Hardware físico o a través de dispositivos virtualizados en plataformas Hyper-V. La Policía Nacional privilegiará el poder montar la solución en la infraestructura de virtualización existente o en la máquina suministrada por el contratante que cumpla los requerimientos necesarios para soportar la cantidad de usuarios de la Policía Nacional.
9.4	El número de servidores virtuales de filtrado podrá incrementarse o disminuirse a discreción de la Policía Nacional sin incrementar el costo de la solución.
9.5	La solución se deberá sincronizar con el Directorio Activo de la Policía Nacional para permitir el acceso a la cuarentena por cada usuario, además de detectar y evitar ataques de directorio.
9.6	La solución podrá controlar y dilatar las conexiones y el envío de direcciones IP que se hayan detectado envíen Spam principalmente.
9.7	Además de listas blancas de IP, La solución podrá, sin intervención de administración, tener estadísticas de direcciones IP que envíen correo bueno para privilegiar el envío de correos hacia el interior de la Policía.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
9.8	La Policía Nacional podrá generar direcciones de correo que actualmente no estén uso y sean altamente atacadas para que sean analizados directamente contra problemas de SPAM por parte del fabricante de la Solución.
9.9	La Policía podrá crear exclusiones de SPAM para buzones dedicados al reporte y análisis de problemas de SPAM y Phishing de los que sufra la ciudadanía.
9.10	El dispositivo podrá identificar máquinas internas que estén generando ataques al interior de la red de la compañía y rechazar temporalmente dichas conexiones.
9.11	La solución permitirá la firma de correos electrónicos de salida con el estándar DKIM y así mismo podrá chequear la validez de los correos entrantes para las firmas DKIM.
9.12	La solución contará con plantillas que permitan examinar los contenidos de los correos y sus adjuntos para evitar fugas de información.
9.13	La solución incluirá la ejecución de reportes. Dichos reportes podrán dar una idea del estado del servicio y número de correos detenidos, número de correos que presentan malware, correos que no se pudieron escanear, reporte de reputación IP entre otros.
9.14	La solución tendrá un sitio de cuarentena tipo Web para retener los correos de acuerdo a las Políticas de seguridad de la Policía. Los usuarios podrán acceder a dicha cuarentena bien para eliminar los correos o dejarlos pasar.
9.15	La solución deberá contar con mecanismos de auditoría detallados para reconocer correos enviados, asunto, disposición de filtrado.
9.16	La solución tendrá mecanismos de detección antispam basada en firmas, heurísticas que se actualicen frecuentemente de los servicios del fabricante.
9.17	El dispositivo a través del tiempo podrá aprender de los comportamientos de las direcciones IP de los remitentes para rechazar la comunicación de direcciones IP reconocidas como Spammers
9.18	El dispositivo a través del tiempo tendrá la capacidad de clasificar direcciones IP que envían principalmente correo no spam y privilegiar el paso del correo y haciendo solo la detección antivirus
9.19	El dispositivo debe permitir la limpieza de amenazas dentro archivos adjuntos (javascript dentro de archivos PDF o Microsoft Word, por ejemplo)
9.20	El soporte de la solución antispam será 7x24x365 con un tiempo de respuesta de no superior a más de una hora, La solución debe contar con un soporte que permita accesos directos a los especialistas de producto cuando sea requerido por los diferentes medios de atención por la Policia Nacional.
9.21	La solución de filtrado de correo electrónico deberá proteger el correo entrante contra amenazas como virus, spyware, malware, spam, phishing y permitirá crear reglas de filtrado dependiendo los destinatarios, remitentes, contenidos.
9.22	La solución deberá estar en capacidad de cifrar correo electrónico y sus adjuntos para al menos 500 usuarios simultáneos.
9.23	La solución podrá identificar archivos sin importar su extensión identificando su verdadero contenido.
9.24	Para archivos cuyo contenido sean ejecutables la solución podrá identificarlos y remover el contenido ejecutable dentro de dichos correos o eliminar el correo.
9.25	La solución de filtrado de correo electrónico podrá inspeccionar el contenido de los correos para detectar URLs que se consideren maliciosas y actuar de acuerdo a las políticas de la Policía Nacional.
9.26	La solución podrá ser instalada en al menos un appliance físico o virtual, pero podrá ser distribuida en tantos appliance requiera la Policía, administrados de manera centralizada.
9.27	La solución contará con consola y/o carpetas de cumplimiento. Una carpeta de cumplimiento es un espacio dentro de la solución en la que se retienen correos electrónicos que caen dentro de la detección de una política (filtran datos sensibles, se requieren para auditoría).
9.28	La solución no deberá requerir licenciamiento adicional del sistema operativo sobre el que corre.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
9.29	El Software de la solución deberá estar asegurado por el fabricante y el acceso a las cuentas privilegiadas (root) deberá estar deshabilitada como mecanismo de aseguramiento.
9.30	La solución seguridad perimetral de correo no podrá ser instalada en los servidores de Correo de la Policía Nacional. La idea es disminuir el impacto de este procesamiento y proteger la infraestructura de la Policía.
9.31	La solución deberá clasificar los mensajes recibidos en categorías dentro de las cuales debe existir una categoría para identificar correos relacionados con marketing (publicidad).
9.32	La solución tendrá mecanismos de reputación de IP que impedirán o retrasarán la conexión de los atacantes.
9.33	La solución debe tener listas negras de remitentes tanto locales como globales para ser usadas en las políticas de filtrado.
9.34	La solución debe ser configurada para tomar acciones diferentes con correos de publicidad y/o boletines de noticias.
9.35	La solución debe permitir autenticación de remitentes a través de SPF tanto como política general para todos los correos recibidos como para una lista de dominios específicos.
9.36	El filtrado de correo electrónico deberá permitir enviar muestras de SPAM al fabricante de la solución para obtener reglas personalizadas contra SPAM.
9.37	La solución debe permitir crear reglas de filtrado de correo de acuerdo con su contenido, tanto para información estructurada como no estructurada, expresiones regulares, diccionarios y palabras clave; y deberá generar un reporte con las posibles violaciones a la política.
9.38	Debe permitir crear y aplicar políticas de prevención de fuga de información.
9.39	La solución antispam debe contar con una consola de administración o integrarse con la consola general de administración de la solución, adicionalmente deberá poder integrarse con sistemas de colección de eventos vía syslog o enviadas al SIEM (Enterprise Security manager McAfee) de la Policía Nacional.
10. DETECCIÓN Y REMEDIACIÓN ANTE AMENAZAS DE SOFTWARE MALICIOSO	
10.1	Combinar la información colectiva sobre amenazas a partir de fuentes de datos globales, con la información sobre amenazas recabada localmente.
10.2	Obtener visibilidad de la presencia de ataques avanzados en la institución.
10.3	Compartir en tiempo real la información de seguridad relevante entre los distintos componentes de la solución.
10.4	Posibilidad de diferentes acciones sobre tipos de archivos nunca vistos anteriormente, en función del contexto de los equipos de punto final (atributos de archivo, proceso o entorno), en base a la información colectiva sobre amenazas.
10.5	Identificar y supervisar el contexto y estado de los equipos de punto final, para reconocer cambios que puedan estar asociados a indicadores de compromiso.
10.6	Capacidad de identificar componentes de los ataques que puedan estar en estado latente; y de enviar la información a los componentes de análisis, operaciones o investigación forense.
10.7	Dar tratamiento a las alertas, para poder realizar ajustes según los cambios en las metodologías de ataque.
10.8	Automatizar la recopilación de datos, alertas y respuestas; y personalizar sus configuraciones en función de los flujos de trabajo identificados.
10.9	Capacidad continua para detectar incidentes relacionados con un ataque, y de generar las notificaciones sobre las actividades detectadas.
10.10	La solución debe utilizar The MITRE Attack Framework para el análisis de posibles incidentes dentro de la organización.
10.11	En el proceso de análisis de un posible incidente, la herramienta debe permitir asignar distintos estados al proceso de evaluación para determinar la etapa en que se encuentra un incidente.
10.12	La solución debe permitir el registro, seguimiento y cierre de casos sin que exista límites en la cantidad de los mismos.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
10.13	La solución debe permitir poner en cuarentena a los host comprometidos con el objetivo evitar movimientos laterales de códigos maliciosos.
10.14	La integración con los otros componentes de la solución ofertada deberá ser a través de un protocolo estándar de comunicación.
10.15	La solución debe permitir la creación de colectores de información de manera personalizada para realizar búsquedas en tiempo real y en proceso de hunting.
10.16	La solución debe permitir la creación de reacciones de manera personalizada para contener y aplicar remediaciones que se ajusten a las necesidades de la organización.
10.17	La solución debe permitir soportar la creación de script de ejecución en Pyhton, Vbscritp y/o la ejecución de comandos de sistemas operativos de manera remota.
10.18	La solución debe utilizar distintos mecanismos de análisis los cuales deben incluir el uso de playbooks, información de terceros para detectar posibles incidentes dentro del ecosistema.
11.	**GENERALIDADES**
SOPORTE Y MANTENIMIENTO	
11.1	El personal que realizará la instalación y configuración de la solución, deberán ostentar el título de Ingeniero de Sistemas, Electrónico y/o a fines, con una experiencia mínima de un (1) año en la configuración e instalación la solución y contar con capacitación certificada por la casa matriz. Para lo cual el oferente deberá presentar con la oferta copia del título de pregrado en ingeniería de sistemas, electrónica y/o a fines, tarjeta profesional vigente, copia de la certificación de la casa matriz sobre la idoneidad en la implementación y administración solución y una certificación de experiencia en la instalación y soporte de la misma de la persona propuesta para la implementación.
11.2	Los soportes serán generados por los usuarios de la red de la PONAL (Policía Nacional) a través de la herramienta de help desk de la Policía Nacional (SIGMA) para la gestión por parte del ingeniero de soporte asignado por el oferente, el cual deberá proporcionar un soporte 5x8 en sitio durante la misma vigencia de la garantía, derecho a actualizaciones de la licencias de los productos adquiridos, a partir del recibo a satisfacción del contrato, el cual se debe prestar en sitio con tiempos de respuesta no superiores a 30 minutos, y tiempos de solución no mayores a las setenta y dos (72) horas debiéndose dar respuesta oportuna y orientación precisa a los diferentes casos que se reporten. Los soportes e incidentes generados a través de la herramienta SIGMA deberán ser gestionados por el ingeniero de soporte asignado por la empresa contratista desde la red LAN y/o WAN de la Policía Nacional (no se permiten VPN para el soporte), se evaluarán los casos de soporte remoto únicamente para asistencia por parte de la casa matriz.
11.3	El soporte, mantenimiento y actualizaciones de la solución objeto del contrato será por un término de dieciocho (18) meses a partir del recibo a satisfacción de la solución.
11.4	El mantenimiento y actualización debe permitir de manera proactiva y centralizada desde la consola de gestión mantener la plataforma tecnológica de la Policía Nacional debidamente asegurada, mediante actividades que permitan validar los niveles de actualización y cobertura de los productos implementados en todas las estaciones y servidores que tengan conectividad con la consola.
11.5	El servicio de soporte telefónico debe darse directamente por la casa matriz para todos los niveles de prioridad de los incidentes, problemas, inquietudes, dudas que se reporten durante el término de vigencia del contrato.
11.6	En caso de existir urgencia respecto a incidentes que involucren las soluciones ofertadas el oferente deberá proporcionar en caso de necesitarlo apoyo de casa matriz (remoto o presencial) hasta solucionar el incidente.

ITEM	CONDICIONES TÉCNICAS MÍNIMAS
11.7	El soporte de la solución será 8x5 con un tiempo de respuesta no superior a más de una hora por parte del fabricante, La solución debe contar con un soporte que permita accesos directos a los especialistas de producto cuando sea requerido por los diferentes medios de atención por parte la Policía Nacional.
11.8	El oferente informará periódicamente vía e-mail al correo ponal.csirt@policia.gov.co de la entidad, acerca de los nuevos virus, suministrando los medios para combatirlos y evitar próximos ataques, informando dentro de las dos (02) horas siguientes después de presentarse la alerta mundial.
12. SERVICIOS DE IMPLEMENTACIÓN	
12.1	La solución ofertada deberá ser instalada y configurada de forma centralizada por el oferente, realizando los despliegues en todos los repositorios a nivel nacional. El oferente en caso de ofrecer un producto diferente al existente en la Policía Nacional deberá realizar la desinstalación del mismo durante el período de implementación.
12.2	El oferente deberá garantizar total compatibilidad con la infraestructura de red, sin degradar el rendimiento de los equipos bajo las diferentes plataformas tanto de estaciones de trabajo como de servidores e infraestructura de red que se encuentran instalados. Para lo cual deberá soportar técnicamente mediante la realización de pruebas.
12.3	Se deben incluir Cuarenta y ocho (48) horas de servicios profesionales directamente del fabricante de la solución ofertada, con el fin de realizar actividades que vaya orientadas al mejoramiento continuo de la implementación, despliegue y configuración de la solución adquirida
13. TRANSFERENCIA DE CONOCIMIENTOS	
13.1	El oferente deberá incluir una capacitación por el oferente o la casa matriz para al menos diez (10) funcionarios de soporte técnico de la solución que incluya el uso y administración del software, antivirus, control de dispositivos, Control de Aplicaciones, Data Lost Prevention - DLP, Cifrado, Antispam, las actualizaciones, funcionalidades de los productos adquiridos en el presente contrato. La intensidad horaria no debe ser inferior a 30 horas.
14. LICENCIAMIENTO	
14.1	Todo el software que compone la solución debe ser licenciado de manera perpetua a nombre de la Policía Nacional.
15. DOCUMENTACIÓN TÉCNICA – ENTREGABLES	
15.1	Se debe entregar totalmente documentada la metodología de implementación y configuración de la herramienta ofertada siguiendo las recomendaciones de mejores prácticas de la casa matriz.
15.2	El oferente deberá disponer de un sitio web de base de conocimiento en el cual se pueda realizar consulta de la documentación de la solución implementada, a su vez la metodología de implementación y configuración de la herramienta ofertada siguiendo las recomendaciones de mejores prácticas de la casa matriz.
15.3	Toda la documentación debe entregarse en idioma español.
15.4	Para el acta de inicio del contrato se debe anexar el cronograma detallado de actividades, indicando actividad, tiempo y responsables de la ejecución del contrato
15.5	Manual de procedimientos de administración y operación de la solución ofrecida.

JoJan Daniel Prado

Patrullero **JOJAN DANIEL PRADO FULA**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Patrullero **WILMER ALEXANDER BARACALDO CIFUENTES**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Intendente **ALEXANDER DIAZ CASTILLO**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Teniente **ANA CATHERINE MARIÑO RINCÓN**
Jefe Grupo Seguridad de la Información
Estructurador Estudio Previo

PÁGINA EN BLANCO

1. Poner a disposición del **CONTRATISTA** los bienes y lugares que se requieran para la ejecución y entrega del objeto contratado.

2. Una vez se surta el proceso de contratación estatal, asignar un supervisor, a través de quien la **POLICÍA NACIONAL** mantendrá la interlocución permanente y directa con el **CONTRATISTA**.

3. Ejercer el control sobre el cumplimiento del contrato a través del supervisor designado para el efecto, exigiéndole la ejecución idónea y oportuna del objeto a contratar.

4. Recibir a satisfacción los bienes y/o servicios que sean entregados por el **CONTRATISTA,** cuando estos cumplan con las condiciones establecidas y en especial las especificaciones u obligaciones técnicas contenidas en el anexo técnico.

5. Adelantar las gestiones necesarias para el reconocimiento y cobro de las sanciones pecuniarias y garantías a que hubiere lugar, para lo cual el supervisor dará aviso oportuno a la POLICÍA NACIONAL, sobre la ocurrencia de hechos constitutivos de mora o incumplimiento.

6. Pagar al **CONTRATISTA** en la forma pactada y con sujeción a las disponibilidades presupuestales y de PAC previstas para el efecto.

7. Tramitar diligentemente las apropiaciones presupuestales que requiera para solventar las prestaciones patrimoniales que hayan surgido a su cargo como consecuencia de la suscripción del contrato.

8. Solicitar y recibir información técnica respecto del bien o servicio y demás del **CONTRATISTA** en desarrollo del objeto del contractual.

9. Rechazar los bienes y/o servicios cuando no cumplan con los requerimientos técnicos exigidos.

PÁGINA EN BLANCO

1. Cumplir con el objeto contractual.

2. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y trabas.

3. Responder en los plazos que la **POLICÍA NACIONAL** establezca en cada caso, los requerimientos de aclaración o de información que le formule.

4. Cumplir cabalmente con sus obligaciones, frente al Sistema de Seguridad Social Integral y parafiscales (Cajas de Compensación Familiar, Sena e ICBF), por cuanto el cumplimiento de esta obligación es requisito indispensable para la realización de cualquier pago.

5. Constituir en debida forma y aportar al Grupo Contractual y Seguimiento de la UNIDAD EJECUTORA o quien haga sus veces, dentro de los tres (3) días hábiles siguientes a la suscripción del contrato, la Garantía Única.

6. Guardar la confidencialidad de toda la información que le sea entregada y que se encuentre bajo su custodia o que por cualquier otra circunstancia deba conocer o manipular y responderá civil, penal y disciplinariamente por los perjuicios de su divulgación y/o utilización indebida que por sí o por un tercero se cause a la administración o a terceros.

7. No acceder a peticiones o amenazas, de quienes actuando por fuera de la ley pretendan obligarlo a hacer u omitir algún acto o hecho, el CONTRATISTA deberá Informar de tal evento a la UNIDAD EJECUTORA de la Policía Nacional y a las autoridades competentes para que se adopte las medidas necesarias.

8. Mantener activa la cuenta corriente o de ahorros reportada para los pagos con el fin de evitar traumatismos en el proceso de ejecución del contrato.

9. Restituir a LA POLICÍA NACIONAL los elementos que haya colocado a su disposición para el desarrollo del objeto contractual, cuando se lo requiera o al finalizar el contrato, en caso de que se hayan suministrado.

10. CATALOGACIÓN. - EL CONTRATISTA deberá proporcionar la información necesaria para denominar, clasificar, identificar y numerar los artículos de abastecimiento relacionados y/o incluidos en el objeto del contrato, dentro del plazo y en las condiciones señaladas por el Supervisor, quien acreditará el cumplimiento de la presente cláusula, mediante un certificado en que conste la entrega total de la información requerida. La presente certificación será necesaria para la liquidación del contrato. Entendiéndose no finalizada la entrega de los bienes objeto del contrato, en tanto no se cumplan las obligaciones de la cláusula de catalogación.

11. Tener en cuenta lo establecido en la Resolución No. 03049 del 2014, *"Por medio del cual se adopta el Manual de Contratación de la Policía Nacional"*, actualizada, modificada y complementada por las Resoluciones Nos. 00090 del 2018 apéndice 1 y apéndice 2 del 2020.

12. Cumplir con las obligaciones en materia de Seguridad y Salud en el Trabajo y los lineamientos del gobierno nacional en el tema del COVID.

13. Para la facturación de los bienes o servicios contratados, se debe tener en cuenta los lineamientos y parámetros contemplados en la circular externa 016 del 09 de marzo de 2021 establecidos por el Ministerio de Hacienda y Crédito Público, por medio del cual se implementa el modelo de recepción de facturas de venta, notas débito y/o notas crédito, la cual es de obligatorio cumplimiento, de acuerdo con la Directiva Presidencial 09 del 17 de septiembre de 2020 "*Lineamientos para el Pago de Proveedores del Estado*" y la Resolución No. 000042 del 05 de mayo de 2020, "*Por la cual se desarrollan los sistemas de facturación, los proveedores tecnológicos*" y el registro de la factura electrónica de venta.

14. Las demás obligaciones del CONTRATISTA contenidas en el artículo 5º de la Ley 80 de 1993, así mismo, será civil y penalmente responsable por sus acciones u omisiones en la actuación contractual.

NOTA: Las obligaciones de carácter ambiental fueron verificados y aprobados por la señora Capitan Yuli Gomez Tovar Responsable Estrategia y de Recursos mediante certificación No:164/ DIRAF-PLANE del 02/06/2022.

SIIF Nación

Reporte Certificado de Disponibilidad Presupuestal Comprobante

Usuario Solicitante:	MHnjrincon	NILTON JAVIER RINCON AMAYA
Unidad ó Subunidad Ejecutora Solicitante:	16-01-01-000	PONAL GESTION GENERAL
Fecha y Hora Sistema:	2022-06-22-10:04 a. m.	

CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL

El suscrito Jefe de Presupuesto CERTIFICA que existe apropiación presupuestal disponible y libre de afectación en los siguientes "ítems de afectación de gastos"

Numero:	42622	**Fecha Registro:**	2022-06-21	**Unidad / Subunidad ejecutora:**	16-01-01-000 PONAL GESTION GENERAL						
Vigencia Presupuestal	Actual	**Estado:**	Generado		**Tipo:**	Gasto			**Uso Caja Menor**	Ninguno	
Valor Inicial:	1.400.000.000,00	**Valor Total Operaciones:**	0,00		**Valor Actual.:**	1.400.000.000,00	**Saldo x Comprometer:**	1.400.000.000,00	**Vr. Bloqueado**	0,00	

SOLICITUD DE CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL				AUTORIZACION DE ADQUISICION DE BIENES Y SERVICIOS					
Número:	45322	**Fecha Registro:**	2022-06-19	**Número:**		**Modalidad de contratación:**		**Tipo de contrato:**	

ITEM PARA AFECTACION DE GASTO

DEPENDENCIA	POSICION CATALOGO DE GASTO	FUENTE	RECURSO	SITUAC.	FECHA OPERACION	VALOR INICIAL	VALOR OPERACION	VALOR ACTUAL	SALDO X COMPROMETER	VALOR BLOQUEADO
000 PONAL GESTION GENERAL	C-1501-0100-22-0-1501037-02 ADQUISICIÓN DE BIENES Y SERVICIOS - SERVICIO DE CIBERSEGURIDAD - DESARROLLO TECNOLÓGICO POLICIA NACIONAL	Nación	11	CSF						
					Total:	1.400.000.000,00	0,00	1.400.000.000,00	1.400.000.000,00	0,00

Objeto:	PC No. 057INV OBJETO SOLUCIÓN ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM. SEG SOL GS-2022-020801-DIRAF DE 21/06/2022

Capitán CATALINA MÉNDEZ BELTRÁN
Jefe Grupo de Presupuesto General