



MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN ADMINISTRATIVA Y FINANCIERA
GRUPO PLANEACIÓN

Consecutivo No: 164 DIRAF- PLANE

CONCEPTO AMBIENTAL

En atención al oficio enviado por la oficina de Ofite de fecha 02/06/2022 en donde se solicita verificar las condiciones ambientales del estudio previo cuya descripción general del objeto es: "SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOSS PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM." de manera atenta informo que se da viabilidad al estudio previo presentado en lo referente al aspecto ambiental, toda vez que no genera aspectos ambientales significativos.

Atentamente,

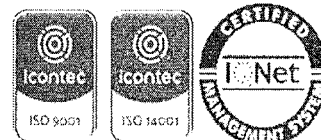

Capitán **YULI GÓMEZ TOVAR**
Responsable Estrategia y de Recursos

Elaborado por: CT. Yuli Gómez Tovar
Fecha elaboración: 02/06/2022
Ubicación: D:\Documentos /Oficios 2022

Carrera 59 No. 26-21, Bogotá
Teléfonos 5159000-9471
diraf.plane@policia.gov.co
www.policia.gov.co



INFORMACIÓN PÚBLICA



SC 0545-1-10 NE SA-CER276652 CO-SC 5545-1-10 NE



MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA DE TELEMÁTICA
GRUPO INVESTIGACION Y PROYECCION TECNOLOGICA



COTEL-GINTE - 15.2

Bogotá, D.C., 07 de junio de 2022

Teniente
ANA CATHERINE MARIÑO RINCON
Jefe Grupo Seguridad De La Informacion
Carrera 59 26-21 CAN PI 1
Bogotá, D.C.

Asunto: respuesta a solicitud comité de requerimientos tecnológicos solución antivirus.

En atención a la solicitud realizada mediante comunicación oficial No. GS-2022-004549-OFITE del 02/06/2022, respetuosamente informo a la señorita Teniente, que el Comité Evaluador de Requerimientos Tecnológicos llevado a cabo el día 07/06/2022 como consta en Acta No. 245 OFITE (adjunta al presente), emitió concepto de viabilidad técnica para continuar con el proyecto cuyo objeto es la "ADQUISICIÓN SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM PARA LA POLICÍA NACIONAL".

Atentamente,



Firmado digitalmente por:
Nombre: Jansen Jair Gonzalez Aragon
Grado: Mayor
Cargo: Jefe Grupo Investigacion Y Proyeccion Tecnologica
Cédula: 80220896
Dependencia: Grupo Investigacion Y Proyeccion
Tecnologica
Unidad: Oficina De Telemática
Correo: jansen.gonzalez@correo.policia.gov.co
7/06/2022 6:09:54 p. m.

Anexo: si

Carrera 59 26-21 CAN PI 2
Teléfono: 5159551 - 5159140
ofite.jefat@policia.gov.co
www.policia.gov.co



SC-6545-1-11-NE



SI-CER270009



CO-SC-6545-1-11-NE

INFORMACIÓN PÚBLICA



MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA DE TELEMÁTICA
GRUPO INVESTIGACION Y PROYECCION TECNOLOGICA

Fecha:	Bogotá D.C. 07 de junio de 2022		
Hora de inicio:	14:30 horas	Hora de finalización:	18:00 horas
Lugar:	Oficina de Telemática videoconferencia vía Teams.		

ACTA No. 245 – OFITE – GINTE – 2.25

QUE TRATA DEL CERT No. 045, CUYO OBJETO ES LA ADQUISICIÓN SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM PARA LA POLICÍA NACIONAL, POR PARTE DEL GRUPO SEGURIDAD DE LA INFORMACIÓN – OFITE.

ORDEN DEL DÍA

1. Verificación de asistentes
2. Lectura del acta anterior
3. Verificación de los compromisos
4. Temas a tratar

DESARROLLO

1. Verificación de asistentes

Conforme a lo dispuesto en el procedimiento 1DT-PR-0019 del 23/08/2019, denominado "REQUERIMIENTOS TECNOLÓGICOS", cuyo objeto es analizar, estudiar y evaluar las necesidades de tecnología de la Policía Nacional"; el día 07/06/2022 se reúnen a través de videoconferencia por la plataforma Teams, los funcionarios que hacen parte del Comité Evaluador de Requerimientos Tecnológicos CERT - OFITE, con la señorita Teniente. ANA CATHERINE MARIÑO RINCON – Jefe Grupo Seguridad de la Información.

Mediante acta No. 008- OFITE- GINTE del 14 de enero de 2022 y orden del día No. 3 del 3 de enero de 2022, se realiza el nombramiento de los integrantes del Comité Evaluador de Requerimientos Tecnológicos CERT.

- MY. JANSEN JAIR GONZALEZ ARAGON, JEFE GINTE OFITE
- MY. CESAR ALFONSO GELVES MENDOZA, JEFE GRUDE – OFITE
- CT. JOHN DARIO RESTREPO CORREA, JEFE GACOM – OFITE
- CT. HILDEBRANDO CASTAÑEDA RINCON, JEFE GUCON – OFITE
- TE. ANA CATHERINE MARIÑO RINCON, JEFE GRUSI OFITE
- SI. KAREN VIVIANA HURTADO PINTO, SECRETARIA CERT– OFITE
- SI. YESICA ALEJANDRA CONEJO SEGURA, ANALISTA RIESGOS – OFITE

Nota: teniendo en cuenta que mediante orden del día No. 091 del 01/04/2022, se nombró al señor CT. Ronal Alexander Franco Aguilera- Asesor Jurídico OFITE, para que actúe como invitado al CERT por su idoneidad en materia jurídica, se deja constancia que no asistió.

2. Lectura del acta anterior

No aplica

3. Verificación de los compromisos

No aplica

4. Temas a tratar

4.1 Antecedentes

Mediante Resolución No. 05884 del 27 de diciembre 2019 hoja No. 351 "CONTINUACIÓN DE LA RESOLUCIÓN POR LA CUAL SE EXPIDE EL MANUAL PARA LA ADMINISTRACIÓN DE LOS RECURSOS LOGÍSTICOS DE LA POLICÍA NACIONAL DE COLOMBIA", se indica en la (...) *nota 6. "Para los proyectos de los entes territoriales gestiones a través de otras fuentes de financiamiento y/o se generen a partir de recursos propios del ente territorial, el Grupo de Telemática de la unidad será el enlace ante el ente territorial a fin de garantizar que estos posean la viabilidad funcional y operativa (a cargo del Comandante del Departamento) y viabilidad técnica (a cargo de la Oficina de Telemática), permitiendo la integración con otros sistemas a nivel nacional; igualmente, los grupos de telemática de las unidades deberán validar funcionalmente el sistema, una vez culminada su etapa de implementación.*

CAPITULO 8. SUBCOMPONENTE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

8.4 lineamientos para el desarrollo, adquisición de sistemas de información de la Policía Nacional Grupo de Investigación y Proyección Tecnológica de la Oficina de Telemática de la Policía Nacional: son funcionarios Policiales, Analistas de Proyectos y Tecnologías de la información, quienes analizan, evalúan la necesidad y convocan el Comité de Evaluación de Requerimientos Tecnológicos, con el fin de emitir conceptos, viabilidades técnicas, pruebas de concepto y especificaciones técnicas para proyectos, desarrollos tecnológicos y/o la adquisición de tecnologías de información y las comunicaciones.

Viabilidad técnica: será emitida por la Oficina de Telemática a través de los grupos de telemática desconcentrados, los cuales deben verificar que el sistema cumpla con las condiciones y especificaciones técnicas mínimas requeridas de los equipos e instalación, a fin de garantizar el correcto funcionamiento (...)

Con base en lo anterior, la señorita Teniente. ANA CATHERINE MARIÑO RINCON – Jefe Grupo Seguridad de la Información, mediante comunicación oficial No. GS-2022-004549-OFITE del 02/06/2022, solicita concepto de viabilidad al siguiente proyecto:

4.2 PROYECTO

- GRUPO OFITE

ADQUISICIÓN SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM PARA LA POLICÍA NACIONAL.

Alcance- Justificación: La Policía Nacional requiere una solución que permita controlar el software malicioso que se mueve a través del internet, evitando afectación al componente tecnológico e información institucional, así:

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

ACTA No. 245 – OFITE – GINTE – 2.25 QUE TRATA DEL CERT No. 045, CUYO OBJETO ES LA ADQUISICIÓN SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM PARA LA POLICÍA NACIONAL, POR PARTE DEL GRUPO SEGURIDAD DE LA INFORMACIÓN – OFITE.

plataforma institucional, con esto cumpliendo uno de los requisitos de la norma ISO 27001 13 para lo cual la Policía Nacional ya cuenta con la implementación del SGSI a nivel nacional y siete 7 procesos certificados (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 contarán 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.

Adicionalmente, el licenciamiento para quince mil 15 000 nodos que serán cifrados para prevenir la fuga de información.

Finalmente, 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.

Adquisición solución software Antivirus, Data Lost Prevención, Control de Aplicaciones, Cifrado y Antispam para la Policía Nacional



Presupuesto - costo

El valor estimado para el presente proceso de contratación es de MIL CUATROCIENTOS MILLONES DE PESOS (\$1,400.000.000,00) EXENTO DE IVA, discriminado de la siguiente manera:

ITEM Y/O LOTE	RUBRO Y DESAGREGACIÓN PRESUPUESTAL	UNIDAD	DESCRIPCIÓN	RECURSO	CANTIDAD	VALOR UNITARIO ESTIMADO, INCLUIDO IVA, EXENTO DE IVA O EXCLUIDO DE IVA SEGÚN CORRESPONDA	VALOR TOTAL ESTIMADO INCLUIDO IVA, EXENTO DE IVA O EXCLUIDO DE IVA SEGÚN CORRESPONDA
1	1501-0100-22-0-1501037-02	OFITE	Adquisición solución software Antivirus, Data Lost Prevención (DLP), Control de Aplicaciones, Cifrado y Antispam para la Policía Nacional	11	1	\$ 1.400.000.000,00	\$ 1.400.000.000,00
VALOR TOTAL ESTIMADO							\$1.400.000.000,00

Tiempo estimado de implementación: El plazo de ejecución del contrato será de ciento veinte 120 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.

Beneficios: La solución minimizará el riesgo de fuga, pérdida 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.

Además, 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.

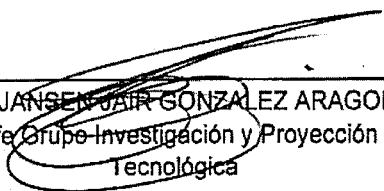
Estos aspectos hacen que día a día se busquen nuevos mecanismos para proteger la información de los procesos, logrando así reducir las brechas de seguridad, que puedan facilitar el acceso de personal no autorizado a los sistemas de la institución y la violación al manual de seguridad de la información realizando la instalación de software no licenciado ni autorizado por la Policía Nacional.

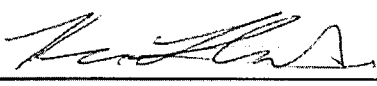
Concepto: el Comité Evaluador de Requerimientos Tecnológicos emite concepto de viabilidad técnica para adelantar el proyecto.

5. COMPROMISOS:

Relación de los compromisos adquiridos por los participantes

Actividad	Responsable	Fecha de entrega
Emitir respuesta a la solicitud presentada	SI. Karen Hurtado	Inmediato


MY. JANSEN GONZALEZ ARAGON
Jefe Grupo Investigación y Proyección
Tecnológica


SI. KAREN VIVIANA HURTADO PINTO
Analista Proyectos y Tecnologías de la
Información

Anexo: uno (pantallazos asistencia vía Teams)

Elaborado por: SI. Karen Hurtado / OFITE - GINTE
Revisado por: MY. Jansen González / OFITE - GINTE
Fecha de elaboración: 07/06/2022
Ubicación: D.1022/CERTACTAS

Carrera 59 26-21 CAN, Bogotá
Teléfonos 515 9551
ofite.jefat@policia.gov.co
www.policia.gov.co



SC-6545-1-11-NE SI-CER278869 CO SC-6545-1-11-NE

INFORMACIÓN PÚBLICA CLASIFICADA

Asistencia vía Teams videoconferencia

Nombre completo	Marca de tiempo
ALEJANDRO BERNAL SALAMANCA	7/6/2022, 2:22:21 p. m.
DIPRO TELEM	7/6/2022, 2:22:21 p. m.
YESICA ALEJANDRA CONEJO SEGURA	7/6/2022, 2:22:21 p. m.
ANA CATHERINE MARIÑO RINCON	7/6/2022, 2:22:21 p. m.
MECAL TELEM-RED1	7/6/2022, 2:22:21 p. m.
DEGUA ALTEC	7/6/2022, 2:22:21 p. m.
DEGUA ALTEC	7/6/2022, 2:22:38 p. m.
JOHN DARIO RESTREPO CORREA	7/6/2022, 2:22:21 p. m.
KAREN VIVIANA HURTADO PINTO	7/6/2022, 2:22:21 p. m.
JAIR DAVID RODRIGUEZ ORTEGA	7/6/2022, 2:26:17 p. m.
HILDEBRANDO CASTAÑEDA RINCON	7/6/2022, 2:26:58 p. m.
CESAR ALFONSO GELVES MENDOZA	7/6/2022, 2:27:24 p. m.
JANSEN JAIR GONZALEZ ARAGON	7/6/2022, 2:29:52 p. m.

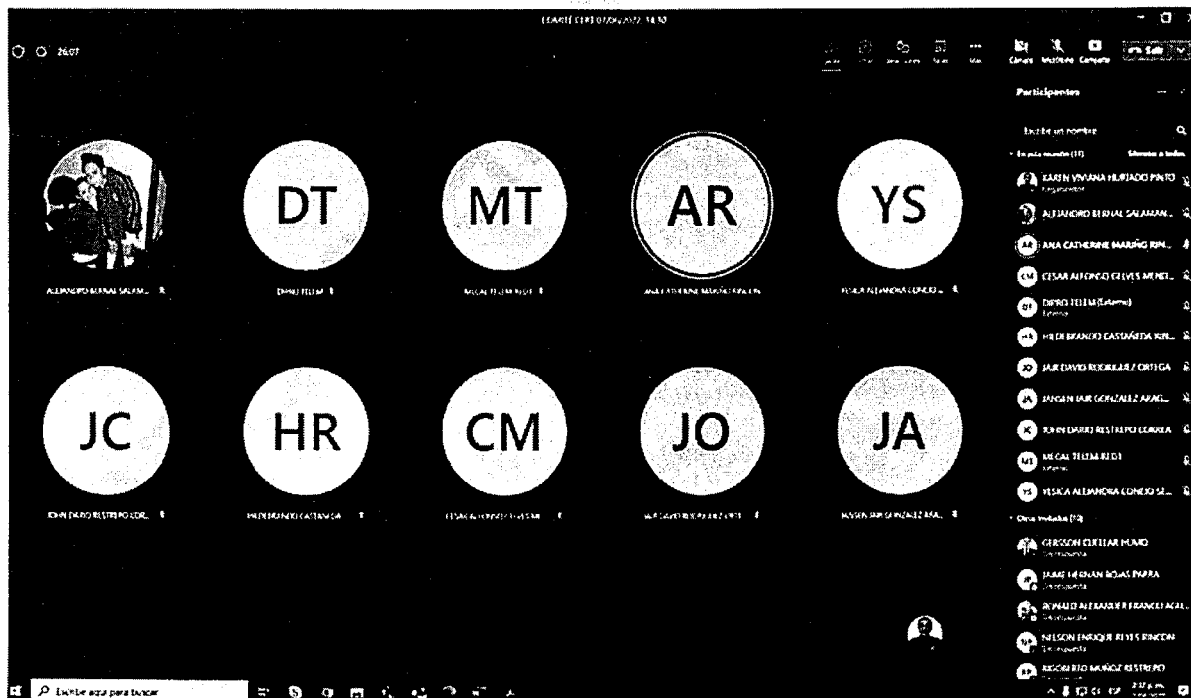


**Imagen captada de Teams por el organizador de la reunión*.*



MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCION ADMINISTRATIVA Y FINANCIERA
ÁREA DE CONTRATACIÓN

Bogotá D. C., 06 de junio de 2022

CERTIFICACIÓN

En cumplimiento al numeral 8 del Artículo 2.2.1.1.2.1.1 del Decreto 1082 del 26 de mayo de 2015, se 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 LOSS PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM.”**, por un valor de **\$1.400'000.000,00.**, **SI** está cubierto bajo las obligaciones de carácter internacional derivadas de los Acuerdos: ALIANZA DEL PACIFICO (CHILE, MEXICO Y PERÚ), CANADÁ, CHILE, COREA, ESTADOS UNIDOS, COSTA RICA, MEXICO, TRIANGULO NORTE, ESTADOS AELC, UNION EUROPEA, CAN; toda vez que:

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

De acuerdo a lo anterior, se debe 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.

Atentamente,

PRO03 JOHN ALEXANDER MANTILLA
Analista Contractual DIRAF

** Excepción: Las convocatorias limitadas a Mipyme: Esta excepción sólo es aplicable en los casos en que la Entidad Estatal verifica las condiciones previstas en el artículo 2.2.1.2.4.2.2. del Decreto 1082 de 2015 para que una convocatoria sea limitada a Mipyme. Así, esta excepción no puede ser utilizada para excluir la cobertura del Acuerdo Comercial en el aviso de Convocatoria; los estudios y documentos previos; o, el borrador del pliego de condiciones. (Colombia Compra Eficiente M-MACPC-14).*

ELABORADO POR: PRO03 JOHN MANTILLA
REVISADO POR: PRO03 JOHN MANTILLA
FECHA ELABORACIÓN: 06062022
UBICACIÓN: ESCRITORIO/CERTINT 2022

Carrera 59 26-21 CAN, Bogotá
Teléfonos 315 9550 – 315 9827
arcon.diraf@policia.gov.co
www.policia.gov.co



SC-6545-1-G-NE



SI-CER431788



CO-SC-6545-1-G-NE

INFORMACIÓN PÚBLICA



Procesos | Contratos | Proveedores | Menú | Ir a

Buscar...

Escritorio → Menú → Procesos de la Entidad Estatal → Expediente

Id de página: 10005226 Ayuda ?

Volver

Opciones

Proceso : SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, ...

Solicitud de información a los Proveedores

PN DIRAF 009-2022 (En análisis) [Pliegos](#)

PROVEEDORES

Unidad de contratación DIRECCION ADMINISTRATIVA Y FINANCIERA

[Ver Enlace](#)

Interesados

4

795

Competidores

Comedidamente me permito solicitar su colaboración en el sentido de realizar la cotización para la contratación de objeto
SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM.

(Zona horaria (UTC-05:00) Bogotá, Lima, Quito)

Fecha de presentación de ofertas 2/06/2022 2:00 PM - Fecha de publicación 27/05/2022 3:39 PM

LÍNEA DE TIEMPO

Fecha de publicación de concurso	Presentación de ofertas	Plazo para solicitar aclaraciones
27/05/2022	02/06/2022	02/06/2022

LISTA DE OFERTAS

Opciones

OBSERVACIONES
AL PLIEGO DE
CONDICIONES[Contestar](#)No tiene ninguna observación a
los documentos del proceso

Referencia de oferta	Entidad	Presentada	Oferta
Estudio de Mercado - Solución de Seguridad	M.S.L. DISTRIBUCIONES Y CIA S.A.S	2/06/2022 1:40 PM	4.203.080.000
oferta economica Diraf 009 2022	Némesis	2/06/2022 12:29 PM	1.478.935.200
Cotización - Ona Systems S.A.S	Ona Systems	2/06/2022 11:49 AM	1.400.000.000

MENSAJES

[Crear](#)

Sin mensajes

EVALUACIÓN ECONÓMICA

Nuevo

Opciones

TAREAS

[Crear](#)

Sin tareas

EVALUACIÓN

Opciones

MODIFICACIONES /
ADENDAS[Crear](#)

CO1.AMD.1406650
Razón: actualización
ficha técnica
1/06/2022 3:03 PM
CO1.AMD.1405200
Razón: actualización
especificaciones y
ampliación plazo de
cotización
31/05/2022 5:19 PM

Modificación
al proceso
publicadaModificación
al proceso
publicada[Ver más »](#)

PROVEEDORES SUSCRITOS

Némesis Asociados s.a.
1/06/2022 10:49 AM
M.S.L. DISTRIBUCIONES Y CIA S.A.S
31/05/2022 10:39 PM
Ona Systems S.A.S.
31/05/2022 8:11 AM
ESOFT COLOMBIA SAS
27/05/2022 4:51 PM

[Ver más »](#)

Las modificaciones serán
aplicadas sólo en este proceso

Equipo: ESTRUCTURADOR / 21/0
4/2022 8:28 AM (UTC -5 horas) ((UT
C-05:00) Bogotá, Lima, Quito) / 27/0
5/2022 3:31 PM (UTC -5 horas) ((UT
C-05:00) Bogotá, Lima, Quito)

EVENTOS DEL PROCESO

**El proceso CO1.BDOS.2952178
ha cambiado de Solicitud
información publicada a En
análisis.**

Sistema
2/06/2022 2:00 PM

**El proceso
CO1.REQ.3033183 cambiado de
estado Solicitud información
publicada a En análisis.**

Sistema
2/06/2022 2:00 PM

**Oportunidad
CO1.OPDOS.13280735 fue
consultado por el Proveedor
Némesis Asociados s.a..**
Némesis Asociados s.a.
2/06/2022 1:50 PM

**Oportunidad
CO1.OPDOS.13295015 fue
consultado por el Proveedor
M.S.L. DISTRIBUCIONES Y CIA
S.A.S.**
M.S.L. DISTRIBUCIONES Y CIA
S.A.S
2/06/2022 1:40 PM

**La información
CO1.RPL.2785025 fue
presentada**
M.S.L. DISTRIBUCIONES Y CIA
S.A.S
2/06/2022 1:40 PM

Ver más »



MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA DE TELEMÁTICA

No. GS-2022-

/ OFITE – GRUSI– 29.25

Bogotá, 27 de mayo de 2022

Señores
Oferentes
Ciudad.

Asunto: solicitud cotización

Comendidamente me permito solicitar su colaboración en el sentido de realizar la cotización para la contratación de objeto "SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM." de acuerdo con las condiciones que a continuación se relacionan, así:

ADVERTENCIA	La cotización solicitada servirá únicamente de base para la elaboración de un estudio de mercado y, por tanto, <u>no constituye en sí misma una oferta</u> y consecuentemente NO obliga a las partes.	
OBJETO	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM.	
VALIDEZ DE LA COTIZACIÓN	(Por favor aclarar la validez de la cotización, se solicita que no sea inferior a 90 días calendario a partir de la fecha.)	
ESPECIFICACIONES TÉCNICAS	Ver anexo No. 1 adjunto	
CONDICIONES DE CONTRATACIÓN	PLAZO DE EJECUCIÓN	A partir de la aprobación de la garantía única, 90 días calendario.
	FORMA DE PAGO	Se realizará un (01) pago total después del cumplimiento de la totalidad de la condiciones técnicas mínimas, 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). Nota: 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, reprogramará el valor a cancelar una vez se hubieran 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).
	OBLIGACIONES DEL CONTRATISTA	Ver anexo No. 2 adjunto
	RIESGOS DE LA CONTRATACIÓN	Ver anexo N° 3 adjunto

	MECANISMO DE COBERTURA DE LOS RIESGOS	Ver anexo N° 4 adjunto
VALOR OFRECIDO	<i>El cotizante deberá tener en cuenta todos los gastos en los que incurra para la suscripción, legalización y ejecución del contrato, como impuestos, publicaciones, constitución de garantía única, transportes, operarios, etc.</i>	
PLAZO PARA PRESENTAR COTIZACIÓN	<p>El plazo será de hasta cinco (05) días calendario contados a partir del recibo del presente documento.</p> <p>La cotización debe ser enviada a la Oficina de Telemática, Cra 59 # 26 21 CAN Teléfono 5159586 y/o al correo electrónico, alexander.diazc@correo.policia.gov.co</p>	

Nota: Con la presentación de la cotización la firma acepta las condiciones jurídicas, técnicas y económicas establecidas por la Policía Nacional; adicionalmente la cotización debe estar identificada cada hoja con el logo de la compañía, diligenciado las casillas de cumple y/o no cumple.

Atentamente,

Intendente **ALEXANDER DÍAZ CASTILLO**
Estructurador estudio previo

Anexos: (12) Folios

Elaborado por: PT. Wilmer Alexander Baracaldo Cifuentes
Revisado por: IT. Alexander Díaz castillo
Fecha elaboración: 21/04/2022
Archivo: Z:\2022\CARPETAS PERSONALES\1.IT.ALEXANDER DIAZ CASTILLO

Carrera 59 26-21 CAN, Bogotá
Teléfonos 515 9090 – 515 9586
ponal.csirt@policia.gov.co
www.policia.gov.co



SC-6545-1-11-NE SI-CER279069 CO-SC-6545-1-11-NE

INFORMACIÓN PÚBLICA

ANEXO No 1
CONDICIONES TÉCNICAS MÍNIMAS

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
1. LA SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM			
1.1	<p>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:</p> <ul style="list-style-type: none"> • Cuarenta y cinco mil (45.000) deben contar con módulo de Antivirus, Control de Dispositivos, Control de Aplicaciones y Data Loss 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. <p>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.</p>		
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.		
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.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
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 continua 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.		
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.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
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	<p>La solución debe poder configurar mediante reglas o políticas de protección de:</p> <ul style="list-style-type: none"> • 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 <p>Asignar las reglas por nombre de usuario.</p>		
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.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
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, adware, keyloggers, ransomware 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		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
	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 específico.		
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.		
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.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
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: <ul style="list-style-type: none"> • Estado del cliente • Últimas 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.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
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 trabajo: 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.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
5.18	La función de protección de escritura y cambios a los sistemas deberá proteger de: <ul style="list-style-type: none"> • 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 LOSS PREVENTION - DLP			
6.1	El módulo Data Loss 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.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
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 mínimo 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: <ul style="list-style-type: none"> • 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 encriptación 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 TECNICAS MINIMAS	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	<p>La solución debe contar con una lista de reglas de acción para realizar como mínimo lo siguiente:</p> <ul style="list-style-type: none"> • 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	<p>La solución debe integrarse con soluciones de Rights Management (IRM) como:</p> <ul style="list-style-type: none"> • Microsoft Windows Rights Management Services • Seclore FileSecure information Rights Management <p>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.</p>		
7.6	<p>Debe de permitir la integración con etiquetado de terceros como:</p> <ul style="list-style-type: none"> • 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	CUMPLE	NO CUMPLE
7.11	<p>Los revisores o administradores de la consola deberán poder auditar las siguientes acciones:</p> <ul style="list-style-type: none"> • Entrada al servidor de administración • Cambio de perfiles o roles • Cambio de contraseñas • Cambios de políticas <p>Esta característica es importante cuando se desea descubrir cambios ocurridos en el servidor de administración.</p>		
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.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
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.		
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: <ul style="list-style-type: none"> • Windows 7 and SP1 (32- and 64-bit), (Not XP Mode) • Windows 8 • windows 10 • Windows 11 y posteriores 		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
8.28	La solución debe poseer al menos las siguientes certificaciones: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
8.51	La solución debe contar con la funcionalidad de que gestionar Native Encryption.		
8.52	<p>La solución debe ofrecer beneficios en común para la gestión sobre FileVault y BitLocker:</p> <ul style="list-style-type: none"> • 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	<p>La solución debe ofrecer beneficios para entornos Mac:</p> <ul style="list-style-type: none"> • 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	<p>Beneficios para entornos Windows:</p> <ul style="list-style-type: none"> • 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	CUMPLE	NO CUMPLE
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 Policía 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).		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
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.		
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.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
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.		
10.12	La solución debe permitir poner en cuarentena a los host comprometidos con el objetivo evitar movimientos laterales de códigos maliciosos.		
10.13	La integración con los otros componentes de la solución ofertada deberá ser a través de un protocolo estándar de comunicación.		
10.14	La solución debe permitir la creación de colectores de información de manera personalizada para realizar búsquedas en tiempo real y en proceso de hunting.		
10.15	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.		
10.15	La solución debe permitir soportar la creación de script de ejecución en Python, Vbscript y/o la ejecución de comandos de sistemas operativos de manera remota.		
10.26	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	<p>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.</p> <p>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.</p>		
11.2	<p>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.</p> <p>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.</p>		
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.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
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 ponac.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 Loss 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		
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 diligenciar el Formulario No. 1 "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.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
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.		
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.		

ANEXO No. 2

OBLIGACIONES DEL CONTRATISTA

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. 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.
6. 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 Policía Nacional y a las autoridades competentes para que se adopte las medidas necesarias.
7. 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.
8. 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 que se hayan suministrado.
9. Cumplir con la implementación del Sistema de Gestión de Seguridad y Salud en el Trabajo, de acuerdo a lo establecido en el Decreto 1072 de 2015, Decreto Único Reglamentario del Sector Trabajo y demás normas que lo complementen, razón por la cual deberán diligenciar el formulario No. 2 del presente estudio previo.
10. Guardar la confidencialidad de 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, diligenciar el formulario No. 1 ACUERDO DE CONFIDENCIALIDAD, del presente estudio previo.
11. Cumplir con la normatividad ambiental vigente nacional para reducir los aspectos e impactos ambientales asociados a su actividad productiva. El oferente deberá tener los permisos, licencias que dieran lugar dentro del desarrollo de su actividad productiva. Cualquier infracción ambiental por omisión de permisos, concesiones o licencias ambientales que hubiese sido necesario tramitar antes del inicio del contrato, en el transcurso y después de la actividad del presente proceso, serán asumidas como responsabilidad del CONTRATISTA.
12. Las actividades que se desarrollan en el complejo DIPON, como; servicios de mantenimiento entre otras, deberán planificarse y controlarse para el cumplimiento de la política ambiental y sus objetivos ambientales a través de los programas y controles operacionales.
13. Los productos y servicios que se adquieran por alguna gestión administrativa deberán establecer los lineamientos para la planeación, operación, control y mejoramiento de la gestión ambiental en la Policía Nacional, a partir del cumplimiento de los requisitos legales ambiental y las condiciones mínimas ambientales; con el objetivo de contribuir a la sostenibilidad ambiental de los procesos,

productos y servicios de la Institución. Así como, el cumplimiento de la Política Ambiental de la Policía Nacional:

"En la Policía Nacional nos comprometemos a contribuir con la protección del ambiente a través de la prevención de la contaminación, el cumplimiento de la legislación y las diferentes regulaciones ambientales y el control de los impactos ambientales adversos asociados a nuestras instalaciones, procesos y servicios; así como al mejoramiento continuo del desempeño ambiental de la Institución".

14. El contratista deberá dar cumplimiento a la Política Ambiental del Sistema de Gestión Ambiental, cada vez que se realice actividades dentro las instalaciones policiales e involucre el alcance del Sistema de Gestión Ambiental o alguno de los procesos: (Convivencia y Seguridad Ciudadana, Prevención, Logística y Abastecimiento, Administración de Recursos Financieros, Direccionamiento del Talento Humano, Direccionamiento Estratégico, Direccionamiento del SGI, Mejora Continua e Innovación, Direccionamiento Tecnológico, Integridad Policial, Comunicación Pública, Control Interno, Actuación Jurídica y Gestión Documental y Relaciones Internacionales), así como las actividades y servicios generados de otros procesos para la Selección e Incorporación.
15. El contratista deberá garantizar que los resultados que se entregarán a la Policía Nacional de forma digital lo realicen en un medio reutilizable, los escritos deberán estar ajustado de acuerdo con la Directiva Presidencial 04 de 2012 *"Parámetros sobre la eficiencia administrativa y lineamientos de política cero papel en la Policía Nacional"* (Aplica a los contratos que deben presentar informes, manuales y/o información).
16. 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.
17. El contratista deberá desarrollar acciones de prevención para disminuir el riesgo de contagio y sus eventuales complicaciones.

ANEXO No. 3 ANÁLISIS DEL RIESGO Y FORMA DE MITIGARLO

Clase	Fuente	Etapas	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 completa 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	SORRECOSTO EN LA OPORTUNIDAD DE LA OCASIÓN DE LA IMPORTACIÓN DE BIENES	2	3	5	MEDIO	CONTRATISTA	EL CONTRATISTA EN SU OFERTA ECONÓMICA DEBERÁ CONTEMPLAR LAS VARIACIONES DE LOS PRECIOS DEL MERCADO, POR CUANTO EL PRESUPUESTO, 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	ESPECÍFICO	EXTERNO	SELECCIÓN	OPERACIONAL	FALSIDAD EN LOS DOCUMENTOS QUE CONFORMAN LA OFERTA	DECLARATORIA DESIERTO DEL PROCESO DE CONTRATACION	1	4	5	MEDIO	ENTIDAD	EVITAR EL RIESGOVERIFICACIÓN ESCRITA DE LOS DOCUMENTOS QUE CONFORMA LA OFERTA, POR PARTE DEL COMITE EVALUADOR	1	1	2	BAJO	NO	NO	INTEGRANTES DE LOS COMITÉS EVALUADORES (JURIDICO, ECONOMICO Y TECNICO)	DE ACUERDO A LA CRONOLOGIA DEL PROCESO	DE ACUERDO A LA CRONOLOGIA DEL PROCESO	EVALUACIONES	DE ACUERDO A LA CRONOLOGIA DEL PROCESO
3	ESPECÍFICO	EXTERNO	SELECCIÓN	OPERACIONAL	NO CUMPLIMIENTO DE OBLIGACIONES POR HABITANTES 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	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 MANTENIMIENTO DE LOS EQUIPOS Y NO SE 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 ADECUADO PARA EJECUTAR EL CONTRATO	1	1	2	BAJO	SI	SI	SUPERVISOR DEL CONTRATO	A PARTIR DE LA APROBACIÓN DE LA GARANTÍA LA ÚNICA	TERMINACIÓN DEL CONTRATO	INFORME AL ORDENADOR DEL GASTO	PERMANENTE
5	ESPECÍFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	QUE SE REALICE LA INSTALACIÓN DE LOS EQUIPOS Y NO SE DE CUMPLIMIENTO AL MANTENIMIENTO 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 TÉCNICO ESTABLECIDO POR CADA FABRICANTE.	1	1	2	BAJO	SI	SI	SUPERVISOR DEL CONTRATO Y COMITÉ EVALUADOR	INICIO DEL CONTRATO	TERMINACIÓN DEL CONTRATO	INFORME AL ORDENADOR DEL GASTO	PERMANENTE

6	ESPECÍFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	QUE EL PERSONAL REALICE TRABAJOS DE INSTALACIÓN, MANTENIMIENTO Y/O REPARACIÓN DE LOS EQUIPOS DEBIDO CRONOGRAMA	NO SE REALICE LA INSTALACIÓN A TODOS LOS EQUIPOS EN EL PRESENTE PROCESO	3	2	5	MEDIO	CONTRATISTA	REDUCIR LA PROBABILIDAD DE QUE EL PERSONAL DEL CONTRATO SOLICITE AL CONTRATISTA UN CRONOGRAMA DE ACTIVIDADES	1	1	1	2	BAJO		NO	SUPERVISOR DEL CONTRATO	INICIO DEL CONTRATO	TERMINACIÓN DEL CONTRATO	CUMPLIMIENTO DE ESPECIFICACIONES DE LOS EQUIPOS DEL ESTUDIO PREVIO	CRONOGRAMA DE TRABAJO
7	ESPECÍFICO	INTERNO	EJECUCIÓN	OPERACIONAL	QUE EL PERSONAL DE LA INSTITUCIÓN NO CUENTE CON EL CONOCIMIENTO NECESARIO PARA LA OPERACIÓN DE LOS EQUIPOS DE ALMACENAMIENTO OFERTADOS	FALLAS EN LA OPERACIÓN DE LOS SISTEMAS DE ALMACENAMIENTO	4	3	7	MODERADO	ENTIDAD	EL CONTRATISTA DEBERÁ GARANTIZAR LA TRANSCENCIA DE LOS EQUIPOS DE ALMACENAMIENTO OFERTADOS	1	1	1	2	BAJO		SI	SUPERVISOR DEL CONTRATO	A PARTIR DE LA APROBACIÓN DE LA GARANTÍA ÚNICA	TERMINACIÓN DEL CONTRATO	INFORMES DE SUPERVISIÓN	DE LA VIGENCIA DEL CONTRATO
8	ESPECÍFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	QUE SE PRESENTEN PROBLEMAS EN LA ATENCIÓN OPORTUNA DE LOS EQUIPOS REPORTADOS POR EL SUPERVISOR DE CONTRATO	QUE SE PRESENTEN DAÑOS EN LA SOLUCIÓN OFERTADA	4	3	7	MODERADO	CONTRATISTA	EL CONTRATISTA DEBERÁ GARANTIZAR QUE EN EL CASO DE FALLAS SE ATENDERÁ EN UN PLAZO DE 8 HORAS A LA SEMANA	1	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	ESPECÍFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	DURANTE LA EJECUCIÓN DEL CONTRATO SE COORDINE EL ACCESO AL SITIO, LO CUAL NO PERMITIRÁ CUMPLIR CON EL CRONOGRAMA DE TRABAJO ESTABLECIDO EN EL PLAZO ESTABLECIDO.	NO CUMPLA CON EL PLAZO DE EJECUCIÓN ESTABLECIDO EN EL CONTRATO	3	3	6	ALTO	ENTIDAD	REDUCIR LA PROBABILIDAD DE QUE EL PERSONAL DEL CONTRATO COORDINE EL ACCESO AL SITIO, LO CUAL NO PERMITIRÁ CUMPLIR CON EL CRONOGRAMA DE TRABAJO ESTABLECIDO EN LA EJECUCIÓN DE CONTRATO.	1	2	3	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

ANEXO No. 4
MECANISMO DE COBERTURA DE LOS RIESGOS
ESTIMACIÓN, TIPIFICACIÓN Y ASIGNACIÓN DE RIESGOS Y DETERMINACIÓN DE
GARANTÍAS

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	Ofertantes	Desde la presentación de la oferta y por cuatro (04) 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 cinco (5) años 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 cinco (5) años 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 cinco (5) años 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.

1 Sobre único

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, por lo cual son bienes que están exentos del impuesto sobre las ventas.

Incluya el precio como lo indique la Entidad Estatal

							Incluya el precio como lo indique la Entidad Estatal
							1.478.935.200,00
Ref. Artículo	Código UNSPSC	Descripción	Cantidad	Unidad	Precio unitario estimado	Precio unitario	Incluya el precio como lo indique la Entidad Estatal
1	43233200	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM	1,00	UN		1.478.935.200,00	1.478.935.200,00

Bogotá, 02 de junio de 2022

Señores

Policía Nacional

Oficina Telemática

Ciudad.

Asunto: solicitud cotización

Realizamos la cotización para la contratación de objeto "SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM." de acuerdo con las condiciones que a continuación se relacionan, así:

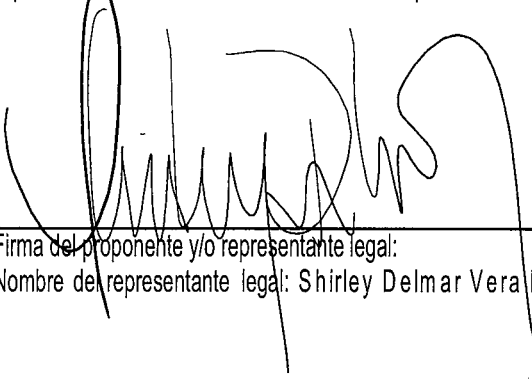
ADVERTENCIA	La cotización solicitada servirá únicamente de base para la elaboración de un estudio de mercado y, por tanto, <u>no constituye en sí misma una oferta</u> y consecuentemente NO obliga a las partes.	
OBJETO	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM.	
VALIDEZ DE LA COTIZACIÓN	90 días calendario a partir de la fecha de presentación ✓	
ESPECIFICACIONES TÉCNICAS	Ver anexo No. 1 adjunto	
CONDICIONES DE CONTRATACIÓN	PLAZO DE EJECUCIÓN	A partir de la aprobación de la garantía única, 90 días calendario.
	FORMA DE PAGO	Se realizará un (01) pago total después del cumplimiento de la totalidad de la condiciones técnicas mínimas, 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). Nota: 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, reprogramará el valor a cancelar una vez se hubieran 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).
	OBLIGACIONES DEL CONTRATISTA	Ver anexo No. 2 adjunto
	RIESGOS DE LA CONTRATACIÓN	Ver anexo N° 3 adjunto
	MECANISMO DE COBERTURA DE LOS RIESGOS	Ver anexo N° 4 adjunto
VALOR OFRECIDO	<i>El cotizante deberá tener en cuenta todos los gastos en los que incurra para la suscripción, legalización y ejecución del contrato, como impuestos, publicaciones, constitución de garantía única, transportes, operarios, etc.</i>	
PLAZO PARA PRESENTAR COTIZACIÓN	<p>El plazo será de hasta cinco (05) días calendario contados a partir del recibo del presente documento.</p> <p>La cotización debe ser enviada a la Oficina de Telemática, Cra 59 # 26 21 CAN Teléfono 5159586 y/o al correo electrónico, alexander.diazc@correo.policia.gov.co</p>	

Nota: Con la presentación de la cotización la firma acepta las condiciones jurídicas, técnicas y económicas establecidas por la Policía Nacional; adicionalmente la cotización debe estar identificada cada hoja con el logo de la compañía, diligenciado las casillas de cumple y/o no cumple.

Atentamente,

Aceptamos las condiciones técnicas dadas en la presente ficha técnica.



Firma del proponente y/o representante legal:
Nombre del representante legal: Shirley Delmar Vera Navas

1 Sobre único

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, por lo cual son bienes que están exentos del impuesto sobre las ventas. Incluya el precio como lo indique la Entidad Estatal

Incluya el precio como lo
Indique la Entidad Estatal
1,400.000.000,00

Ref. Artículo	Código UNSPSC	Descripción	Cantidad	Unidad	Precio unitario estimado	Precio unitario	Incluya el precio como lo Indique la Entidad Estatal
1	43233200	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM	1,00	UN		1.400.000.000,00	1.400.000.000,00

02 de junio de 2022

Señores,
Dirección Administrativa Y Financiera
Policía Nacional
Bogotá,

Asunto: Solicitud Cotización No. GS-2022- / OFITE – GRUSI– 29.25

Propuesta comercial

TECNOLOGÍA			
Referencia	Descripción	Fabricante	Cantidad
MV1ECE-DA-FI	MVISION Protect Standard - Upgrade	Trellix	45000
CWBECE-AB-JI	Trellix Cloud Workload Security Basic Subscription	Trellix	400
CDAECE-DT-FI	DLP - Complete Data Protection Trellix Advanced Upgrade - Subscription	Trellix	45000
ACDYCM-AA-JI	Application Control for PCs	Trellix	18000
BSF800a-h BSFi800a-e	Barracuda Email Security Gateway Appliance 800 Instant Replacement Subscription 1 Month 18 MONTHS SN# 1039340 Barracuda Email Security Gateway Appliance 800 Energize Updates Subscription 1 Month 18 MONTHS SN# 1039340	Barracuda	18 meses
SERV-ONA	SERVICIOS PROFESIONALES Ingeniero en sitio – 18 Meses	Ona Systems	1

TOTAL GENERAL	
VALOR ANTES DE IVA	\$ 1.400.000.000,00

*El bien objeto de adquisición se encuentra catalogado como exento, de acuerdo a lo dispuesto en el artículo 188 del decreto 1819 de 2016, que modifica el artículo 477 del Estatuto Tributario. Bienes que se encuentran exentos del impuesto, literal n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional. Atendiendo su naturaleza y destinación estos bienes se encuentran gravados a la tarifa 0%.

Condiciones generales:

1. Vigencia de la oferta 60 días calendario a partir de la fecha de la presente oferta.
2. Moneda: pesos colombianos.

1

2

[Aumentar el contraste](#)

UTC -5 8:33:16

DIRAF



Procesos

Contratos

Proveedores

Menú

Ir a

Buscar...

Escritorio → Menú → Administración de los procesos → Expediente → **Detalles del mensaje**Id de página: 77000367 [Ayuda ?](#)[Volver](#)[Imprimir](#)

Detalles de mensaje

Referencia interna: PN DIRAF 009-2022**Descripción del proceso** Comedidamente me permito solicitar su colaboración en el sentido de realizar la cotización para la contratación de objeto SOLUC
De: POLICÍA NACIONAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA**Usuario:** jhon alexander mendez mendoza**Fecha:** 5 minutos de tiempo transcurrido (14/06/2022 8:28:01 AM(UTC-05:00)
Bogotá, Lima, Quito)**Para:** Némesis Asociados s.a.; M.S.L. DISTRIBUCIONES Y CIA S.A.S; Ona Systems S.A.S.; ESOFT COLOMBIA SAS;**Referencia del mensaje** CO1.MSG.3768802**Tipo de mensaje:** General**Asunto:** solicitud actualización de la factura

Texto de mensaje

Buenos días

respetuosamente me permito solicitar a Ona Systems S.A.S, actualizar la vigencia de la cotización a un plazo de 90 días calendario.

La actualización de la cotización se deberá enviar anexa a la respuesta de este mensaje



[Aumentar el contraste](#)



UTC -5 9:31:49

DIRAF



Procesos	Contratos	Proveedores	Menú	Ir a
----------	-----------	-------------	------	------

Buscar...

Escritorio → Gestión de mensajes → Gestión de mensajes → **Detalles del mensaje**

Id de página:: 77000367 Ayuda ?

[Volver](#)

[Contestar](#)

[Contestar a todos](#)

[Imprimir](#)

Detalles de mensaje

Referencia interna: PN DIRAF 009-2022

Descripción del proceso Comedidamente me permito solicitar su colaboración en el sentido de realizar la cotización para la contratación de objeto SOLUC

De: Ona Systems S.A.S.

Usuario: Jose Joaquin Rozo Herrera

Fecha: 18 minutos de tiempo transcurrido (14/06/2022 9:11:09 AM(UTC-05:00)
Bogotá, Lima, Quito)

Referencia del mensaje CO1.MSG.3769026

Tipo de mensaje: General

Asunto: RE: solicitud actualización de la factura

	Documento	Nombre del documento	
Anexos	220415_2_Propuesta económica.pdf	220415_2_Propuesta económica.pdf	Detalle
	Agregar documento a la oferta Exportar todos		

Texto de mensaje

Cordial saludo,

Adjunto propuesta comercial con vigencia a 90 días.

Cordialmente,

Equipo Ona Systems S.A.S

6/14/2022 8:28:01 AM POLICÍA NACIONAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA

Buenos días

respetuosamente me permito solicitar a Ona Systems S.A.S, actualizar la vigencia de la cotización a un plazo de 90 días calendario.

La actualización de la cotización se deberá enviar anexa a la respuesta de este mensaje

14 de junio de 2022

Señores,
Dirección Administrativa Y Financiera
Policía Nacional
Bogotá,

Asunto: Solicitud Cotización No. GS-2022- / OFITE – GRUSI– 29.25

Propuesta comercial

TECNOLOGÍA			
Referencia	Descripción	Fabricante	Cantidad
MV1ECE-DA-FI	MVISION Protect Standard - Upgrade	Trellix	45000
CWBECE-AB-JI	Trellix Cloud Workload Security Basic Subscription	Trellix	400
CDAECE-DT-FI	DLP - Complete Data Protection Trellix Advanced Upgrade - Subscription	Trellix	45000
ACDYCM-AA-JI	Application Control for PCs	Trellix	18000
BSF800a-h BSFi800a-e	Barracuda Email Security Gateway Appliance 800 Instant Replacement Subscription 1 Month 18 MONTHS SN# 1039340 Barracuda Email Security Gateway Appliance 800 Energize Updates Subscription 1 Month 18 MONTHS SN# 1039340	Barracuda	18 meses
SERV-ONA	SERVICIOS PROFESIONALES Ingeniero en sitio – 18 Meses	Ona Systems	1

TOTAL GENERAL	
VALOR ANTES DE IVA	\$ 1.400.000.000,00

*El bien objeto de adquisición se encuentra catalogado como exento, de acuerdo a lo dispuesto en el artículo 188 del decreto 1819 de 2016, que modifica el artículo 477 del Estatuto Tributario. Bienes que se encuentran exentos del impuesto, literal n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional. Atendiendo su naturaleza y destinación estos bienes se encuentran gravados a la tarifa 0%.

Condiciones generales:

1. Vigencia de la oferta 90 días calendario a partir de la fecha de la presente oferta.
2. Moneda: pesos colombianos.

1 Sobre único

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, por lo cual son bienes que están exentos del impuesto sobre las ventas. Incluya el precio como lo indique la Entidad Estatal

Incluya el precio como lo
Indique la Entidad Estatal
4,203,080,000.00

Ref. Artículo	Código UNSPSC	Descripción	Cantidad	Unidad	Precio unitario estimado	Precio unitario	Incluya el precio como lo Indique la Entidad Estatal
1	43233200	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM	1.00	UN		4,203,080,000.00	4,203,080,000.00

Propuesta Comercial

Junio 02 de 2022

Contenido de la propuesta

Introducción.....	1
MSL Distribuciones\CA Technologies.....	1
Problemática a resolver ..	2
Información de las Soluciones.....	2
Propuesta Económica	3
Condiciones Comerciales.	5

Introducción

M.S.L. DISTRIBUCIONES & CIA S.A.S, se permite someter a su consideración, la propuesta para la adquisición de la solución DLP.

Agradecemos su interés y confianza en nuestras soluciones y quedamos a la espera de cualquier comentario al respecto.

Reciba un cordial saludo,

Andrea Talero Molano

Gerente de cuenta

atalero@msl.com.co

Cel: 320 9627274

MSL Distribuciones\CA Technologies

"Somos una organización que brinda soluciones integrales de informática en las áreas de Gestión, Seguridad y Optimización de TI"

CA Technologies/Broadcom es uno de los proveedores de software de administración de TI más grande del mundo. Su software y experiencia permiten unificar y simplificar entornos de TI complejos de forma segura en toda la empresa, para obtener mejores resultados de negocio. De la mano de **M.S.L Distribuciones y Cia S.A.S** como **Tier 1** se han implementado y desarrollado diferentes soluciones para todo tipo de negocios tanto en el sector publico como privado.

El software y las soluciones de CA ayudan a nuestros clientes a impulsar la productividad de toda la empresa, ofrecer experiencias de usuarios diferenciadas y abrir nuevas oportunidades de crecimiento. Y podemos ofrecer este valor en varios entornos: ya sea móvil, en la nube privada o pública, distribuido y en el gran sistema. Nuestro objetivo es que nuestros clientes nos reconozcan como un Partner crítico en la nueva economía de las aplicaciones.

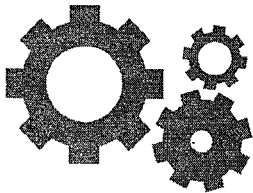
Explore las soluciones de CA Technologies / Broadcom y los servicios profesionales de M.S.L Distribuciones que pueden ayudar a potenciar su futuro:

<http://www.broadcom.com>

<http://www.msl.com.co>

Problemática a resolver

Se presenta oferta comercial según solicitud para la adquisición de 17 licencias de Symantec DLP para la Jurisdicción Especial para la Paz JEP como cliente final. Se proyectan 17 licencias de cada modulo que compone la solución como esta implementada en la JEP con el fin de dar cubrimiento a las necesidades en modalidad de Bundle completo.



*"Proteger lo realmente útil
y necesario"*

Información de las Soluciones

Symantec Data Loss Prevention

Symantec Data Loss Prevention le permite:

- Descubra y ubique información confidencial en repositorios de almacenamiento en la nube, en servidores de archivos y web, en bases de datos y en terminales (sistemas de escritorio y portátiles)
- Proteja la información confidencial mediante cuarentena
- Monitorear el tráfico de la red para la transmisión de datos confidenciales
- Supervisar el uso de datos confidenciales en terminales
- Evite la transmisión de datos confidenciales a ubicaciones externas
- Aplique automáticamente las políticas de cifrado y seguridad de los datos

Los módulos Descubrir, Proteger, Monitorear y Prevenir se pueden implementar como productos independientes o en combinación. Independientemente de los productos independientes que implemente, Enforce Server siempre se proporciona para la administración central. Tenga en cuenta que el módulo Network Protect requiere el módulo Network Discover / Cloud Storage Discover.

Propuesta Económica

Licencias en suscripción de Symantec DLP

Descripción	Unidades	Valor Total
Servicio en suscripción durante 18 meses, de la solución Data Loss Prevention Endpoint Prevent, Subscription License with Support, Managed Devices.	45.000	\$ 2.788.000.000
Servicio en suscripción durante 18 meses, de la solución Data Loss Prevention Endpoint Discover, Subscription License with Support, Managed Devices.	45.000	
Servicio en suscripción durante 18 meses, de la solución Endpoint Encryption, Subscription License with Support, Devices.	15.000	
Servicio en suscripción durante 18 meses, de la solución Secure Email Gateway Safeguard, Hybrid Subscription License with Support, Users.	20.000	
Servicios profesionales de Implementación DLP Endpoint Prevent DLP Endpoint Discover Endpoint Encryption Capacitación equipo Policía Nacional Servicios de desinstalación soluciones anteriores de McFee. Servicio profesional de soporte en sitio 5*8, durante 18 meses.	1	\$ 744.000.000
Total		\$ 3.532.000.000
IVA 19%		\$ 671.080.000
TOTAL		\$ 4.203.080.000

Handwritten signature

Nota 1. Los valores ofertados en la presente propuesta se encuentran discriminados en pesos colombianos e incluyen el impuesto del IVA.

Nota 2. El valor ofertado incluye todas las licencias contenidas en el apartado **descripción de la oferta**.

Nota 3. El licenciamiento es en modalidad de suscripción por 18 meses.

Nota 4. El costo del agente en sitio es por 18 meses.

FC 006	Revisión: 3	4 de junio de 2019
--------	-------------	--------------------

Carrera 7d No. 108ª-59 P.B.X.: 7429730
Bogotá, D.C. – Colombia
msl@msl.com.co

Descripción de la oferta

Respecto al ítem que describe los servicios profesionales van incluidos:

Servicios profesionales de Implementación

- DLP Endpoint Prevent
- DLP Prevention Endpoint Discover
- Endpoint Encryption
- Capacitación equipo Policía Nacional
- Servicios de desinstalación soluciones anteriores de McFee.

Agente en sitio

- Ingeniero por 18 meses en sitio.

Condiciones Comerciales

FC 006	Revisión: 3	4 de junio de 2019
--------	-------------	--------------------

Carrera 7d No. 108ª-59 P.B.X.: 7429730
Bogotá, D.C. – Colombia
msl@msl.com.co

FORMA DE PAGO:

Un único pago contra entrega del licenciamiento a la Policía Nacional.

IMPUESTOS:

Esta propuesta comercial incluye el impuesto del IVA

VALIDEZ DE LA PROPUESTA:

La presente propuesta comercial es válida hasta el 30 de Junio de 2022

PROPIEDAD Y CONFIDENCIALIDAD:

Este documento contiene información comercial y técnica de carácter confidencial, de propiedad de M.S.L. Distribuciones & S.A.S. Ltda. En virtud de esto, no se permite la copia, reproducción o cualquier tipo de duplicación del total o de partes de este documento sin la expresa autorización por escrito de M.S.L. Distribuciones & S.A.S, así como la divulgación de la información aquí contenida a terceros.

FC 006	Revisión: 3	4 de junio de 2019
--------	-------------	--------------------

Carrera 7d No. 108ª-59 P.B.X.: 7429730
Bogotá, D.C. – Colombia
msl@msl.com.co

[Aumentar el contraste](#)

UTC -5 8:32:55

DIRAF



Procesos

Contratos

Proveedores

Menú

Ir a

Escritorio → Menú → Administración de los procesos → Expediente → **Detalles del mensaje**[Buscar...](#)Id de página: 77000367 [Ayuda ?](#)[Volver](#)[Imprimir](#)

Detalles de mensaje

Referencia interna: PN DIRAF 009-2022**Descripción del proceso** Comedidamente me permito solicitar su colaboración en el sentido de realizar la cotización para la contratación de objeto SOLUC
De: POLICÍA NACIONAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA**Usuario:** jhon alexander mendez mendoza**Fecha:** 14/06/2022 8:32:20 AM ((UTC-05:00) Bogotá, Lima, Quito)**Para:** Némesis Asociados s.a.; M.S.L. DISTRIBUCIONES Y CIA S.A.S; Ona Systems S.A.S.; ESOFTE COLOMBIA SAS;**Referencia del mensaje** CO1.MSG.3768823**Tipo de mensaje:** General**Asunto:** aclaración cotización

Texto de mensaje

buenos días

de manera atenta y respetuosa me permito solicitar a la empresa **M.S.L. DISTRIBUCIONES Y CIA S.A.S.**, que se actualice el valor de la cotización presentada toda vez que 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.



MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA DE TELEMÁTICA
SOPORTE Y APOYO



OFITE-GUSAP - 3.1

Bogotá, D.C., 15 de junio de 2022

Mayor General
HENRY ARMANDO SANABRIA CELY
 Director Administrativo y Financiero
 Carrera 59 No. 26 – 21 CAN
 Bogotá D.C.

Asunto: informando nombramiento comités de evaluación

De manera atenta y respetuosa me dirijo a mi General, con el propósito de informar la designación del personal que por parte de esta Oficina Asesora realizará el acompañamiento dentro de la evaluación del proceso de contratación cuyo objeto es la *"Solución Software Antivirus Data Lost Prevention, control de aplicaciones, cifrado y Antispam"*, como se relaciona a continuación.

COMITÉ	GRADO Y NOMBRE	CÉDULA	PERFIL
TÉCNICO	IT. LÓPEZ LÓPEZ JUAN MANUEL	3034147	TECNÓLOGO
	SI. VARGAS AMAYA LEYDI JANETH	1013586924	INGENIERA
	SI. ESTUPIÑÁN ALVARADO JAIRO ALEXANDER	1013608221	TECNÓLOGO
ECONÓMICO	TE MARICEL VILLARREAL DIAZ	38643923	CONTADOR
JURÍDICO	CT RONALD ALEXANDER FRANCO AGUILERA	74245716	ABOGADO

Lo anterior, en cumplimiento al comunicado oficial No. GS-2022-006417-DIRAF de fecha 24/02/2022, como apoyo y acompañamiento de los comités económico, y jurídico por parte de esta oficina asesora.

Atentamente,



Firmado digitalmente por:
 Nombre: Carlos Alberto Benitez Rojas
 Grado: Coronel
 Cargo: Jefe Oficina De Telematica
 Cédula: 93391868
 Dependencia: Oficina De Telemática
 Unidad: Oficina De Telemática
 Correo: carlos.benitez@correo.policia.gov.co
 16/06/2022 7:50:44 a. m.

Anexo: no

Carrera 59 No 26-21 CAN Piso 1
 Teléfono: 5159153 - 5159118
 ofite.gusap-jefat@policia.gov.co
 www.policia.gov.co



SC-0545-1-11-NE

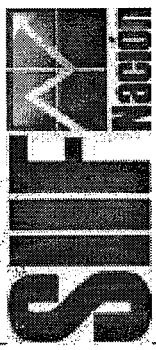
SI-CER27009

CO-SC-0545-1-11-NE

INFORMACIÓN PÚBLICA

42622.60K

65-2022-020001-01RAF



Solicitud de Certificado de Disponibilidad Presupuestal
Comprobante

Usuario Solicitante:
Unidad ó Subunidad
Ejecutora Solicitante:
Fecha y Hora Sistema:

MHajrincon ANGELA JUDITH RINCON MARINO
16-01-01-000 PONAL GESTION GENERAL
19/06/2022 12:00:00 a. m.

SOLICITUD DE CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL					
Numero.:	45322	Fecha Registro:	2022-06-19	Unidad / Subunidad ejecutora:	16-01-01-000 PONAL GESTION GENERAL
Estado.:	Generado	Valor Inicial:	1.400.000.000,00	Valor Total Operaciones:	0,00 Valor Actual: 1.400.000.000,00
ITEM PARA AFECTACION DE GASTO					
DEPENDENCIA		POSICION CATALOGO DE GASTO			
000 PONAL GESTION GENERAL		C-1501-0100-22-0 DESARROLLO TECNOLÓGICO POLICIA NACIONAL		FECHA OPERACION	VALOR INICIAL
				VALOR OPERACION	VALOR ACTUAL
		Total:		1.400.000.000,00	0,00
					1.400.000.000,00

Objeto: SEÚN PC. 057 CUYO OBJETO ES SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM

Capitán INGRID MAYIRE ACOSTA CASTILLO
JEFE AREA DE CONTRATACIÓN

NOTA: Se expide el presente certificado en atención al Comité No. 1 de asignación de recursos y orientación a la contratación presidido por el señor General, Jorge Luis Vargas Valencia, Director General de la Policía Nacional; en el cual aprueba la distribución de los recursos de la

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 ascendente 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 la 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 posteriormente aplicar las medidas estadísticas como lo son el promedio ponderado, la mediana, la desviación estándar, la media podada.

GRÁFICO TALLO Y HOJAS											
Muestra Poblacional	Tallo	Hojas	Bajo, medio y alto nivel de endeudamiento	Mayoría de oferentes están en este rango	Promedio de los 10 muestra poblacional	Mediana	Desviación estándar	Media podada 8 Items de 10	Desviación estándar de la media podada	Razón de endeudamiento por encima o de bajo 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 se evidencian en el pico del gráfico y 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 el doble de la desviación estándar, 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

Rentabilidad del patrimonio	Rentabilidad del activo	Índice liquidez	Razón de endeudamiento	Cobertura de Intereses
$\geq 0,03$	$\geq 0,02$	≥ 1.27	$\leq 0,62$	≥ 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 empresas 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 párrafo transitorio del artículo 2.2.1.1.6.2, 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 párrafo transitorio, agregado al artículo 2.2.1.1.6.2. 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”.

Atentamente,



Firmado digitalmente por:
Nombre: Omar Leonardo Villalobos Rincon
Grado: Teniente Coronel
Cargo: Jefe Contaduría General
Cédula: 79765768
Dependencia: Grupo Contaduría General Diraf
Unidad: Dirección Administrativa Y Financiera
Correo: omar.villalobos@correo.policia.gov.co
6/06/2022 5:14:18 p. m.

Anexo: no

KR 59 26 21
Teléfono: 3159481
diraf.cogen-plane@policia.gov.co
www.policia.gov.co



SC 6545-1.6.21

SC 6545-1.6.21

CO-SC-6545-1.6.21

INFORMACIÓN PÚBLICA



MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCION ADMINISTRATIVA Y FINANCIERA
GRUPO CONTADURIA GENERAL DIRAF



DIRAF-COGEN - 3.1

Bogotá, D.C., 06 de junio de 2022

Capitán
 JHON ALEXANDER MENDEZ MENDOZA
 Analista Continuidad de la Información
 Carrera 59 26-21 CAN PI 1
 Bogotá, D.C.

Asunto: respuesta a la comunicación oficial GS-2022-004564-OFITE del 02/06/2022

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

1.Consideraciones exento

➤ 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 M-DVRHPC-05.
- La información financiera que se tomará para el presente análisis del sector será con cifras 2021 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:

Patrullero LORENA MARCELA BARRETO TOCARRUNCHO, adscrita a la Oficina de Contaduría General de la 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 realizó mediante la aplicación de seis medidas o promedios estadísticos, así:

- Media Aritmética:** para la cual se tuvo en cuenta las diez (10) empresas y se aplicó el promedio ponderado en forma directa.
- 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, tampoco los resultados en cero e indeterminados, 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.
- 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.
- 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.
- Máximo:** promedia el valor del indicador de los diez (10) oferentes asignando el límite superior.
- Promedio Ponderado:** este se aplica ponderando las anteriores medidas estadísticas por cada uno de los indicadores.

"SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENCIÓN, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM"				
Cantidad de Proponentes	Índices Capacidad Organizacional		Índices Capacidad Financiera	
	Rentabilidad del patrimonio	Rentabilidad del activo	Índice liquidez	Cobertura de Intereses
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