## ESTUDIO DE CONVENIENCIA Y OPORTUNIDAD

| | |
|---|---|
| **Dependencia solicitante:** | Oficina de Tecnología y Sistemas de Información (OTSI) |
| **PABS:** | 110407626 - 110409126 |

## 1. DESCRIPCIÓN DE LA NECESIDAD:

El Departamento Nacional de Planeación (DNP), de conformidad con el literal d) del numeral 1 del artículo 38 de la Ley 489 de 1998[1], es un departamento administrativo del sector central de la administración pública, perteneciente a la Rama Ejecutiva del poder público en el orden nacional. Su carácter técnico le ha asignado el objetivo de impulsar una visión estratégica del país en los campos social, económico y ambiental, a través del diseño, la orientación y evaluación de las políticas públicas, el manejo y asignación de la inversión pública y la concreción de estas en planes, programas y proyectos del Gobierno.

Mediante artículo 1.1.1.1 del Decreto 1082 de 2015 modificado por el artículo 2 del Decreto 1893 de 2021, "*Por el cual se modifica la estructura del Departamento Nacional de Planeación"*, se establece como objetivo: *"El Departamento Nacional de Planeación tiene como objetivos fundamentales la coordinación y diseño de políticas públicas y del presupuesto de los recursos de inversión; la articulación entre la planeación de las entidades del Gobierno Nacional y los demás niveles del gobierno; la preparación, el seguimiento de la ejecución y la evaluación de resultados de las políticas, planes, programas y proyectos del sector público; así como realizar en forma permanente el seguimiento de la economía nacional e internacional, proponer los estudios, planes, programas y proyectos para avanzar en el desarrollo económico, social, institucional y ambiental, y promover la convergencia regional del país (…)*".

El Plan Nacional de Desarrollo - PND 2022 – 2026 denominado "*Colombia Potencia Mundial de la Vida*", expedido mediante la Ley 2294 de 2023, establece 372 artículos orientados a impulsar transformaciones en diferentes ámbitos del desarrollo nacional, incluyendo aspectos relacionados con la transformación digital, la seguridad digital y el fortalecimiento institucional del Estado. Es así como, la línea de acción "*7. la Defensa integral del territorio para la protección de la soberanía, independencia, integridad territorial y del orden constitucional*", la seguridad incluye la protección del ciberespacio y esto cubre las infraestructuras tecnológicas que soportan las infraestructuras críticas de las Entidades de Gobierno. Así mismo, en el catalizador *"Habilitadores que potencian la seguridad humana y las oportunidades de bienestar"* y en la línea de acción *"8. Seguridad digital confiable para la garantía de las libertades, la protección de la dignidad y el desarrollo integral de las personas"* describe la actividad relacionada con la seguridad digital en las Entidades del Estado *"Protección de las personas, de las infraestructuras digitales, fortalecimiento de las entidades del Estado y garantía en la prestación de sus servicios en el entorno digital Se diseñará e implementará una estrategia para adelantar las medidas enfocadas a salvaguardar la infraestructura crítica cibernética del país. Se protegerá la información de las entidades gubernamentales y de las personas de posibles ataques cibernéticos y delitos informáticos, bajo principios de resiliencia y rápida recuperación (…)".*

En este contexto, uno de los ejes de transformación corresponde a la seguridad humana y justicia social, la cual consiste en una política social para la adaptación y mitigación del riesgo que integra la protección de la vida con la

[1] Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones.

seguridad jurídica e institucional, así como la seguridad económica y social, partiendo de un conjunto de habilitadores estructurales como un sistema de protección social universal y adaptativo; una infraestructura física y digital para la vida y el buen vivir. En ese sentido, es vital que como entidad se continúe propendiendo por mantener una infraestructura tecnológica que permita el buen funcionamiento y servicio que se presta a todos los ciudadanos contando con sistemas, software y aplicativos debidamente protegidos y garantizando la confidencialidad de la información.

La Ley 2294 de 2023[2] en el artículo 143 establece: *"TRANSFORMACIÓN DIGITAL COMO MOTOR DE OPORTUNIDADES E IGUALDAD. El Ministerio de Tecnologías de la Información y las Comunicaciones diseñará e implementará una estrategia integral para democratizar las TIC y desarrollar la sociedad del conocimiento y la tecnología en el país, mediante las siguientes medidas:*

*(…) 7. Promover un entorno digital seguro para generar confianza en el uso y apropiación de las TIC. (…)"*

A su vez, el citado artículo 143 está alineado con la Política Nacional de Confianza y Seguridad Digital (CONPES 3995)[3] cuyo objetivo es *"Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías".*

A nivel institucional la entidad ha definido el Plan Estratégico de Tecnologías de la Información PETI, incluye el servicio tecnológico de protección de virus informáticos y prevención de acceso no autorizado de la información clasificada, como mecanismo para el aseguramiento y mitigación de las amenazas de ataques o intrusión en los sistemas de información institucionales y el cierre de las brechas.

Por lo anterior, para dar cumplimiento al alcance estratégico y a las promesas de valor para los diferentes grupos de interés, se requiere disponer de servicios de tecnologías de la información y las comunicaciones (TIC) que permitan el fortalecimiento y aseguramiento de la Entidad a través de plataformas tecnológicas robustas, con altos niveles de disponibilidad, calidad y cobertura que permitan mejorar la gestión y operación, tanto en el ámbito interno como en su interacción con el ámbito externo.

Así las cosas, conforme con lo señalado anteriormente y al tenor de lo establecido en el artículo 10 del Decreto 1893 de 2021 la Oficina de Tecnología y Sistemas de Información (OTSI) tiene entre sus funciones las contenidas en los siguientes numerales:

*"(…) 3. Desarrollar y actualizar las políticas, lineamientos y estrategias en materia tecnológica, en sistemas de información y en servicios digitales, con el 'fin de habilitar la gestión y gobernabilidad de las Tecnologías de la Información (TI) y la prestación efectiva de los servicios tecnológicos del Departamento Nacional de Planeación.*

*(…) 9. Implementar el Modelo de Seguridad y Privacidad de la información (MSPI) del Departamento Nacional de Planeación, siguiendo los lineamientos del Ministerio de Tecnologías de la Información y las*

[2] *"POR EL CUAL SE EXPIDE EL PLAN NACIONAL DE DESARROLLO 2022- 2026 "COLOMBIA POTENCIA MUNDIAL DE LA VIDA"*

[3] https://www.dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx

*Comunicaciones, alineado al Plan Estratégico de Tecnología y Sistemas de Información (PETI) y las políticas del Gobierno Nacional.*

*10. Gestionar la seguridad y flujo de la información en tecnologías de la información del Departamento Nacional de Planeación a fin de permitir su acceso entre las diferentes dependencias para el cumplimiento de los objetivos institucionales.*
*11. Gestionar los incidentes informáticos en materia de seguridad de la información del Departamento Nacional de Planeación, de acuerdo con los lineamientos y directrices establecidas en la entidad.*

*12. Administrar y soportar la infraestructura tecnológica del Departamento Nacional de Planeación (…)"*

El DNP, en aras de garantizar su funcionamiento como Entidad estatal, atiende sus necesidades en materia de TIC, a través de la OTSI, quien es la encargada de proveer a la Entidad estos servicios TI, los cuales se encuentran soportados sobre una infraestructura tecnológica robusta, funcional, estable y confiable, que, dados los avances tecnológicos que se presentan constantemente, requiere estar alineada en la medida de lo posible con la evolución tecnológica para atender de manera satisfactoria sus necesidades.

Es así como en el año 2009 el DNP implementó el Sistema de Gestión de Seguridad de la información (SGSI) que tiene como alcance: i. la identificación de los activos de información, ii. la aplicación de la metodología de gestión de riesgos sobre los procesos, activos de la información y iii. la implementación de los controles aplicables para proteger la confidencialidad, integridad y disponibilidad de los activos de información.

Ahora bien, es importante indicar que un activo de información es cualquier elemento relacionado con el tratamiento de la información que tiene valor para la organización, en el DNP los activos de información están clasificados en seis (6) tipos:

i. Servicios de información o sistemas de información;
ii. Servicios tecnológicos;
iii. Software;
iv. Hardware;
v. Recurso humano; y
vi. Edificios (las instalaciones).

Adicionalmente, los activos de información poseen tres (3) propiedades que deben ser protegidas desde el SGSI: 1) confidencialidad, 2) integridad y 3) disponibilidad.

- **Confidencialidad:** la información debe estar debidamente protegida para que sólo sea accedida por el usuario autorizado.
- **Integridad:** la información debe estar adecuadamente protegida para asegurar que no sea alterada.
- **Disponibilidad:** la información debe estar disponible en cualquier momento.

A su vez, los activos de información relacionados con productos de tecnologías (servicios de información o sistemas de información, servicios tecnológicos, software, hardware) se encuentran expuestos con la identificación de nuevos virus informáticos (Troyanos, Gusanos, Ransomware, Spyware, Rootkits, Keyloggers, entre otros), donde un virus informático puede afectar las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.

Los virus informáticos pueden hacer lo siguiente:

a) Permitir que un atacante ejecute comandos como otro usuario.
b) Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos.
c) Permitir a un atacante eliminar información sensible.
d) Permitir a un atacante realizar una negación de servicio.

En cumplimiento de los objetivos misionales y el desarrollo tecnológico, la Entidad cuenta con una infraestructura que soporta la operación diaria de las diferentes áreas y que comprende entre otros, equipos de cómputo y servidores, y con el fin de proteger la infraestructura del DNP, en el año 2007 se adquirió una solución de Antivirus del Fabricante Trellix a través del contrato DNP-302-07 suscrito con la empresa PC Micros LTDA, cuyo objeto era: "*El DEPARTAMENTO NACIONAL DE PLANEACIÓN está interesado en recibir propuestas para adquirir el servicio de actualización de 800 licencias de Antivirus McAfee modalidad AVD a la modalidad TEA para 800 licencias con 2 años de mantenimiento, modalidad perpetuo, incluidos los servicios de implementación, configuración, capacitación y soporte técnico correspondiente*"[4].

Actualmente la Entidad cuenta con un parque computacional compuesto por equipos de cómputo distribuidos a nivel nacional, servidores virtuales bajo plataforma HYPER-V, servidores físicos, y servidores virtuales en la nube de Microsoft Azure, dicha plataforma se encuentra protegida por el producto del fabricante Trellix, por lo cual se hace necesario renovar la suite para mantener actualizada su postura de seguridad acorde con los lineamientos del Gobierno Nacional.

El grant[5] del DNP con número 17931022-NAI incluye los siguientes productos y fechas de expiración:

| Nodos | SKU | Producto | Inicio | Expiración |
|---|---|---|---|---|
| 2,655 | MV6ECE-AA | Trellix EDR & EPP 1:1TE | 11/19/2024 | 30/09/2026 |
| 127 | CWEYFM-AB | Cloud Workload Sec Essl 1YrTE[P+] | 11/19/2024 | 30/09/2026 |
| 55 | MV3ECE-AA | Trellix Mobile Advanced 1:1TE | 11/19/2024 | 30/09/2026 |

[4] https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=07-2-89084&g-recaptcha-response=0cAFcWeA6WaPYDBZ1dI51dsRO-kl6vOSmey2MlprcMC037b1XDXaikspUWY_t0rVjejRKCIbLfTYnlxu8erzFd9mfKJO-XI_KU7CK_0ciVzDiyBfrXCu_k1edwcxOHgHXqrURUwcM3rtcERP4PE_s56zkhqMC-9lFNPcHq8y1eUMo1oraXNbkRr_L_xlJAZHh-uD7Fkcn8R-dRv23BTyByrM7_SlAnBgwjsrLQkzVlN_tile-08vnDsl-wnFZq5sMEdvFprT7OuOY0lWcg0gZ2L6sNMIHtNKjg_M6d-Rv5B167XHbanZr6lZb4pX_e1pBwEWcfy3RKQ7X0YgdGIoclyurFFyaOECyReUUs7v0hSGlchVGnCXxMs60KbWT9W0DqQATL2kUGN8Wz_ZRB7GTbnkhyr6M7wUed3LvMSr6i77ZlfjNcQip7aTOW-cxBd-clsrKuw53jc00DBjXImwk8MamWGQEh8rPnuUyixZ2lbkoD3g7h1rnQ7XUpFlbZBlWFvDFs78yFgXvqSLKlz31xu-yvU_j7liDpkyS3EFDuWiVmMPQ9PT0DphR4sU3kt2tCjKGxpS0_8nyOe-n7PjPAfoYpX4k-AV4Gf98dwpBVwOi40yXXvxCyFPzlpezOf0qK1idEqBolrJIB9iwueiGHCslcqdfFCr3WVY0XJit8SMca9Bmrm-PoKqIGMfwgbPjgP4AMiGzDDUZQDn86k3KebnG24xI7q9PjCFPMgRYNmN9882feBZzlUDOeDSSj2GN3BY4pWZDXqnZm6qAdIRnSZS63zgBQyG-mOKh0gFHmSAvqZBR3SK92jzrDoAZk-pFDjXJb9ny-VkkuzCabKCvJiPScejqYSAZ_QZI5eMq07pHRoA2SZMt6WJeYgj3IXMgiRCLLhSJFfDL8IsEBou4lt7HzYFHMxxTs73OGXlQT2xqCNt9yFEu2ybahcMkBqn1bDRYr9KFv_eq3fYtorwcKQHFeFkHWonbE2PG_d2wdLBTFsHTTy6fHx4mb4Gt9aCOqJD1Lmcb235rtUMTmK53_hSQiuVCZwcACoTMQqiflvR6U_2olK3yJ8S_EgST-lLVFBILrlrc76VZJ5WRToD7n-DOEHUjboelPgPlpjW-9jntOOSSz3AuAJaQ

[5] Número de concesión e identificación de código único, emitido por el fabricante Trellix cuando se adquieren sus productos.

| | | | | |
|---|---|---|---|---|
| 2112 | DLPECE-AT | Data Loss Prvtn Endpt Comp 1:1TE | 11/19/2024 | 30/09/2026 |

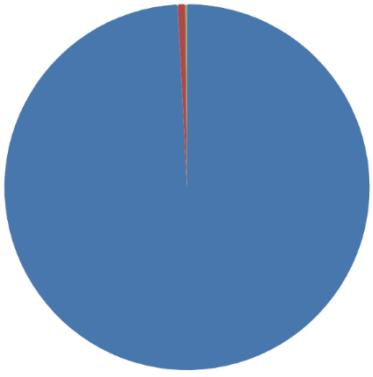
El contar con soporte técnico activo provee al DNP el derecho a acceder a ampliaciones, mejoras, actualizaciones y soporte, esto aplica tanto para software licenciado por suscripción como a perpetuidad, dichas mejoras y actualizaciones están sujetas a los términos de la licencia otorgada por Trellix al cliente a través de la Carta de Concesión, el Acuerdo de Licencia de Usuario Final (EULA por sus siglas en Ingles), y los Términos y Condiciones de Soporte.

El antivirus ofrece una gama completa de productos de seguridad, como cortafuegos y programas antispyware. El Antivirus viene con un conjunto de características que van a mantener a los servidores y estaciones cliente del DNP libre de virus, gusanos informáticos, troyanos y otros programas maliciosos. Con el antivirus se obtienen los siguientes beneficios:

1. Detectar, prevenir y corregir amenazas rápidas y avanzadas tanto en estaciones cliente como en servidores de la entidad.
2. Manejar aprendizaje automático y la tecnología de detección y respuesta a amenazas para Endpoint, ya que encuentra y neutraliza rápidamente amenazas sin archivos, amenazas zero-day, ransomware y otros tipos de ataques avanzados.
3. Consta de una plataforma de protección de Endpoint, consolidada, administrada y centralizada.
4. Se tiene protección continua y adaptable, ante ataques potenciales.
5. Con la consola de antivirus se reduce el tiempo dedicado a detectar y responder a las amenazas, ayudando al grupo de seguridad de la OTSI a priorizar las amenazas rápidamente y a disminuir posibles interrupciones de servicio ya que la misma permite supervisar la actividad de los Endpoint, detectando comportamientos sospechosos.
6. Automatiza y elimina las tareas manuales para recopilar y analizar pruebas.

En el siguiente gráfico se refleja la estadística de amenazas registrados y tipificadas. La consola registró las amenazas, que fueron a su vez bloqueadas o eliminadas según el caso.

**Gráfica 1. Eventos amenazas durante el 2025 y 2026 en los servidores**

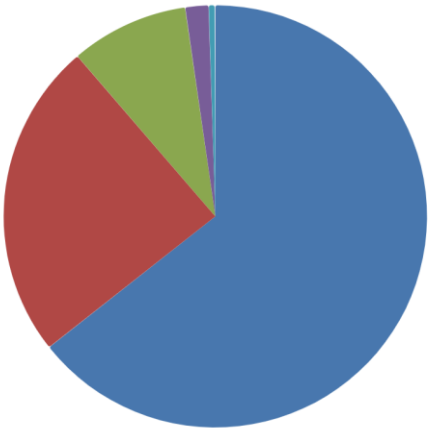


Fuente. Herramienta de monitoreo Consola EPO Trellix

| Event Category | Number of Threat Events |
|---|---|
| Host intrusion buffer overflow | 19,551,989 |
| 'Process' class or access | 131,359 |
| Host intrusion (hip.nips) | 27,837 |
| Reputation | 785 |
| 'File' class or access | 180 |
| 'Registry' class or access | 26 |
| Malware detected | 20 |
| (Task started) | 4 |
| (Task ended) | 2 |
| **Total** | **19,712,202** |

Fuente. Herramienta de monitoreo Consola EPO Trellix

**Gráfica 2. Eventos amenazas durante el 2025 y 2026 en los equipos de cómputo**



Fuente. Herramienta de monitoreo Consola EPO Trellix

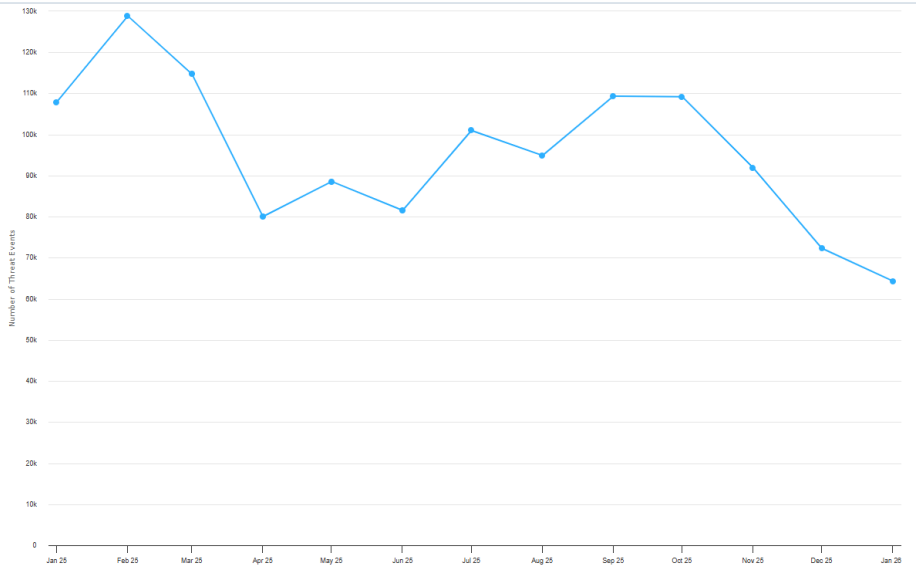
| Event Category | Number of Threat Events |
|---|---|
| 'Registry' class or access | 775,431 |
| Host intrusion buffer overflow | 293,233 |
| 'File' class or access | 108,507 |
| 'Process' class or access | 21,361 |
| Policy | 5,674 |
| Malware detected | 213 |
| Reputation | 87 |
| Host intrusion (hip.nips) | 68 |
| Malicious site navigation | 26 |
| Malicious file download | 16 |
| Malware detected using heuristics | 14 |
| (Task started) | 1 |
| **Total** | **1,204,631** |

Fuente. Herramienta de monitoreo Consola EPO Trellix

Siendo los malware y software malicioso, una de las principales y más recurrentes amenazas existentes a nivel de seguridad, la consola registra de forma diaria los ataques perpetrados por agentes externos, identificando parámetros como máquina atacada, usuario propietario, origen del ataque, firmas digitales asociadas, entre otros importantes atributos que permiten realizar un seguimiento minucioso sobre las vulnerabilidades existentes y en consecuencia impedir que se materialice cualquier riesgo de seguridad que comprometa el normal funcionamiento de las estaciones cliente y servidores con los que dispone la entidad.

En lo corrido del 2025 y 2026 se han registrado un total de 1.244,440 eventos bloqueados de amenaza por malware en servidores y 19.866.637 en estaciones cliente, como se observa a continuación.

**Gráfica 3. Eventos amenazas durante el 2025 y 2026 en los servidores**

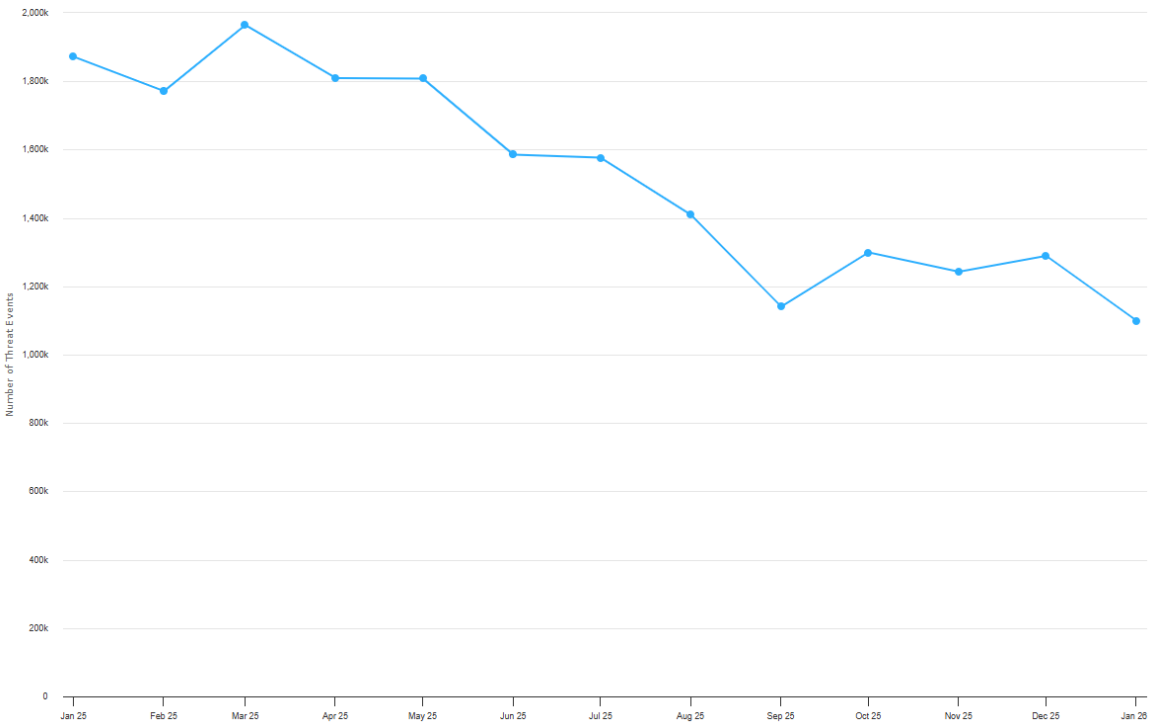



Fuente. Herramienta de monitoreo Consola EPO Trellix

| Event Generated Time | Number of Threat Events |
|---|---|
| January 2025 | 107,898 |
| February 2025 | 128,849 |
| March 2025 | 114,710 |
| April 2025 | 80,029 |
| May 2025 | 88,541 |
| June 2025 | 81,540 |
| July 2025 | 100,979 |
| August 2025 | 94,892 |
| September 2025 | 109,326 |
| October 2025 | 109,206 |
| November 2025 | 91,866 |
| December 2025 | 72,276 |
| January 2026 | 64,328 |
| **Total** | **1,244,440** |

Fuente. Herramienta de monitoreo Consola EPO Trellix

**Gráfica 4. Eventos amenazas durante el 2025 y 2026 en los equipos de cómputo**




Fuente. Herramienta de monitoreo Consola EPO Trellix

| Event Generated Time | Number of Threat Events |
|---|---|
| January 2025 | 1,871,628 |
| February 2025 | 1,771,367 |
| March 2025 | 1,964,324 |
| April 2025 | 1,809,340 |
| May 2025 | 1,808,007 |
| June 2025 | 1,585,332 |
| July 2025 | 1,576,361 |
| August 2025 | 1,409,281 |
| September 2025 | 1,140,558 |
| October 2025 | 1,299,080 |
| November 2025 | 1,242,755 |
| December 2025 | 1,288,977 |
| January 2026 | 1,099,627 |
| **Total** | **19,866,637** |

Fuente. Herramienta de monitoreo Consola EPO Trellix

A continuación, se presenta el resumen de las contrataciones realizadas hasta la fecha, donde se evidencia que la contratación se ha realizado bianualmente, y periódicamente el producto ha sido migrado a las versiones vigentes por el fabricante:

| Año | Contrato | Valor | Vigencia | Variación valor por Año | Total Licencias | Suite | Justificación Valores |
|---|---|---|---|---|---|---|---|
| 2007 | DNP-302-07 | $ 114.492.000 | 2 años | | 800 | TEA | |
| | TOTAL | $ 114.492.000 | | $ 114.492.000 | 800 | | |
| 2009 | DNP-489-09 | $ 84.970.116 | 2 años | | 906 | TEA | La variación del valor es porque se incluyen nuevas licencias |
| | DNP 526-09 | $ 263.970.000 | 2 años | | 63 | TEA | |
| | Contrato de adquisición de bienes y servicios No.2092731 | $ 18.691.080 | 2 años | | 5 | TEA | |
| | TOTAL | $ 367.631.196 | | $ 253.139.196 | 974 | | |
| 2010 | contrato de adquisición de bienes N02092885 y 2092795 | $ 45.636.720 | 2 años | | 11 | TEA | La variación del valor es porque cambia la modalidad de licenciamiento |
| | DNP 500-2010 | $ 57.400.000 | | | 13 | EPA | |
| | CONTRATO No. 2101003 | $ 180.137.500 | 2 años | | 11 | EPA | |
| | TOTAL | $ 283.174.220 | | -$ 84.456.976 | | | |
| 2011 | DNP 549-2011 | $ 177.114.500 | 2 años | | 1385 | EPA | La variación del valor es porque se incluyen nuevas licencias |
| | TOTAL | $ 117.114.500 | | -$ 166.059.720 | 1385 | | |
| 2014 | DNP-388-14 | $ 184.039.858 | 2 años | | 1697 | EPA | La variación del valor es porque se incluyen nuevas licencias |
| | TOTAL | $ 184.039.858 | | $ 66.925.358 | 1697 | | |
| 2016 | DNP-529-16 SGR-037-16 | $ 297.041.200 | 2 años | | 1926 | EPA | La variación del valor es |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | TOTAL | $ 297.041.200 | | $ 113.001.342 | 1926 | | porque se incluyen nuevas licencias |
| 2018 | DNP-551-18 SGR-077-18 PC MICROS S.A.S | $164.000.000 | 2 años | | 1851 | CEB | La variación del valor es porque cambia la modalidad de licenciamiento |
| | | | | | 75 | CWS | |
| | TOTAL | $ 164.000.000 | | -$ 133.041.200 | | | |
| 2020 | DNP-759-20-SGR-158 | $377.672.000 | 2 años | | 2284 | EDR | La variación del valor es porque se incluyen nuevas licencias |
| | PC MICROS SAS | | | | 54 | CWS | |
| | | | | | 21 | CEB | |
| | TOTAL | $ 377.672.000 | | $ 213.672.000 | | | |
| 2022 | DNP-929-2022 / SGR-073-2022 | $485.234.500 | 2 años | | 2252 | EDR | La variación del valor es porque se incluyen nuevas licencias |
| | PC MICROS S.A.S. | | (Vigente hasta el 7 de noviembre de 2024) | | 54 | CWS | |
| | TOTAL | $ 485.234.500 | | $ 107.562.500 | | | |
| 2024 | DNP-1167-2024 SGR-058-2024 | $ 1.083.817.728 | 2 años | | 2284 | EDR | La variación del valor es porque se incluyen nuevas licencias y se adiciona licencias para módulo de DLP |
| | | | (Vigente hasta el 30 de septiembre de 2026 | | 2112 | DLP | |
| | TOTAL | $ 1.083.817.728 | | $ 598.583.228 | | | |

La detección y respuesta de Endpoint (EDR por sus siglas en ingles Endpoint Threat Detection and Response) es una tecnología que monitorea y protege los dispositivos (como computadoras y servidores) dentro de una red, la cual detecta comportamientos sospechosos o maliciosos, como intentos de acceso no autorizado o actividad anómala, y responde tomando medidas para bloquear o mitigar las amenazas. Algunas de sus características principales incluyen:

- Protección proactiva utilizando inteligencia artificial y aprendizaje automático para identificar y bloquear amenazas conocidas y desconocidas en tiempo real.

- Monitoreo continuo de la actividad de los Endpoint para detectar comportamientos sospechosos y responder rápidamente a incidentes de seguridad.
- Análisis detallados de las amenazas detectadas, ayudando a entender su origen, impacto y cómo mitigar futuros ataques.
- Remediación automática de amenazas para minimizar el impacto en la organización y reducir el tiempo de respuesta.
- Visibilidad integral de la actividad de los Endpoint en toda la red, facilitando la gestión y el monitoreo de la seguridad.
- Integración con otras herramientas de seguridad de Trellix y de terceros para proporcionar una defensa en profundidad y mejorar la coordinación en la respuesta a incidentes.

Por su parte Trellix CWS (por sus siglas en ingles Cloud Workload Security) es una solución de seguridad relevante en varios escenarios, especialmente cuando se trata de proteger cargas de trabajo en entornos de nube, la cual cubre los servidores Linux, servidores físicos y servidores virtuales de Azure. Algunas de sus características principales incluyen:

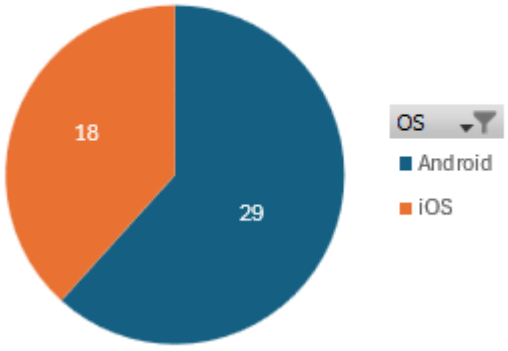
- Utiliza **inteligencia artificial** y aprendizaje automático para identificar y mitigar amenazas avanzadas en tiempo real.
- Protección de las aplicaciones basadas en la nube contra vulnerabilidades y ataques, asegurando que las aplicaciones críticas funcionen de manera segura.
- Visibilidad completa de las cargas de trabajo en la nube, permitiendo a las organizaciones monitorear y gestionar la seguridad de sus entornos en la nube de manera efectiva.
- Implementación de políticas de seguridad consistentes en todos los entornos de nube.
- Integración con otras herramientas de seguridad de Trellix y de terceros para ofrecer una protección unificada y coordinada en todos los entornos de nube.

Trellix Mobile Advanced es un software que detecta las amenazas y brinda protección y seguridad en dispositivos móviles iOS y Android, esta solución de seguridad protege los dispositivos móviles de los usuarios de amenazas y ataques cibernéticos, utilizando tecnología de detección en el dispositivo para proporcionar protección en tiempo real, incluso cuando el dispositivo no está conectado a internet, incluye características como: protección contra malware y amenazas móviles, seguridad de aplicaciones, seguridad de red.

1. La protección contra malware y amenazas móviles protege contra virus, spyware, troyanos y otras amenazas maliciosas.
2. La seguridad de aplicaciones analiza las aplicaciones instaladas para detectar comportamientos sospechosos o maliciosos.
3. La seguridad de red protege contra ataques de red y asegura las conexiones WI-FI.
4. Protege dispositivos Android e iOS, incluidos iPhone y iPads.
5. Se instala directamente en los dispositivos móviles para brindar protección permanente sin importar cómo esté conectado el dispositivo: a través de una red corporativa, un punto de acceso público o un operador celular, e incluso sin conexión.
6. Cuenta con los algoritmos de aprendizaje automático analizan las desviaciones del comportamiento del dispositivo para descubrir indicadores de compromiso e identificar con precisión ataques avanzados basados en dispositivos, aplicaciones y redes
7. Protege a los dispositivos contra el phishing detectando enlaces dañinos que se encuentran en mensajes de texto, aplicaciones de redes sociales y correos electrónicos.

8. Permite ampliar la visibilidad y el control de los dispositivos móviles desde la misma consola donde se administran las estaciones cliente y servidores.

**Gráfica 5. Número de dispositivos móviles a proteger**




Fuente. Herramienta de monitoreo Consola EPO Trellix

Además, el DNP ha identificado 6 riesgos de seguridad de la información, incluyendo la fuga de información, que se refiere a la divulgación no autorizada o accidental de información confidencial, sensible, clasificada y/o reservada, afectando la confidencialidad de la información, ya sea intencional o accidental. La materialización de este riesgo puede ocasionar un impacto significativo y negativo, provocando posibles multas por incumplimiento de normativas de protección de datos, afectando gravemente la reputación de la entidad, erosionando la confianza de los grupos de valor y ciudadanía, enfrentando a la Entidad a litigios y reclamaciones legales por parte de afectados, por ello en la gestión integral de riesgos el DNP identificó la necesidad de fortalecer las opciones de manejo del riesgo de seguridad de la información denominado fuga de información (197) el cual se registra en la Matriz Integral de Riesgos del DNP conforme se observa en la imagen.

**Gráfica 6. Opciones de manejo riesgo fuga de información**

OTSI

| | IDENTIFICACIÓN DEL RIESGO | | ANÁLISIS DEL RIESGO | OPCIÓN DE MANEJO | | | | |
|---|---|---|---|---|---|---|---|---|
| No. Riesgo | Descripción del riesgo/ Impacto ambiental | Tipo de riesgo | Riesgo residual (valoración después de controles) | Opción de manejo | Objetivo de manejo | Descripción de las actividades para implementar la opción de manejo | Dependencia responsable | Fecha de ejecución de opción de manejo (DD/MM/AAAA) |
| 197 | Fuga de información (Afecta la confidencialidad) | Seguridad de la información | IMPORTANTE | Reducir-Controles Administrativos | Disminuir el impacto de la materialización del riesgo | a) Sensibilización sobre el uso de la informacion, clasificada, reservada y datos personales<br>b) Investigar herramientas en el mercado para la prevencion de la fuga de información, para gestionar su adquisión e implementación<br>c) Revisar y referenciar las politicas y/o controles de los componentes de Seguridad de la información, Gestión Documental y de Gestión del Conocimiento en relación con la protección de la información | a-b. OTSI<br>c. OTSI- GGDB- OAP | a-b. 31/12/2024<br>c. 31/012/2024 |

Fuente. Matriz Integral de Riesgos del DNP

En las opciones de manejo se incluyó la renovación del módulo DLP de la solución implementada de Trellix dado que permite la integración nativa con la necesidad de DNP a través del licenciamiento Trellix Data Loss Prevention (DLP).

El componente Trellix Data Loss Prevention (DLP) tiene como objetivo la prevención de pérdida de datos, es una solución de seguridad que identifica y ayuda a prevenir el intercambio, la transferencia o el uso inseguro o inapropiado de datos que desean ser protegidos por la Entidad. El componente de DLP cuenta con las siguientes características:

1. Prevención de exfiltración de datos sin afectar las operaciones de los usuarios mediante la personalización de notificaciones para los usuarios que intenten violar las políticas de uso compartido de datos y soliciten justificación.
2. Orientación a los usuarios finales que intentan infringir las políticas de seguridad establecidas.
3. Capacitación y notificaciones instantáneas para el usuario final
4. Creación de reportes para evidenciar el cumplimiento de la protección de la información.
5. Ajuste de reglas y reportes predefinidos para usar alineados con los marcos regulatorios clave.
6. Identificar, clasificar y proteger la información institucional en más de 400 tipos de archivos
7. Monitoreo centralizado y seguimiento de eventos
8. Inventariar datos confidenciales en redes, ubicaciones de almacenamiento y bases de datos.
9. Protección y monitoreo de estaciones de trabajo y servidores para prevención de pérdida de datos

Trellix DLP ofrece una consola única y conveniente para gestionar la implementación, administrar políticas, monitorear eventos en tiempo real y obtener informes listos para garantizar el cumplimiento.

La renovación de la solución DLP refuerza la mejora continua del componente de seguridad de la información al implementar la Resolución 500 de 2021, que establece los lineamientos y estándares para la estrategia de seguridad digital, adoptando el Modelo de Seguridad y Privacidad basado en la norma internacional ISO 27001:2013. Este componente de DLP contribuye al cumplimiento del artículo 10 de dicha resolución, que exige a las entidades del Gobierno Nacional definir una estrategia para proteger la privacidad de la información de la entidad y de los ciudadanos, en concordancia con la Ley 1581 de 2012 y sus decretos reglamentarios, así como al artículo 17, que requieren adoptar políticas y mecanismos para evitar la fuga de datos e información.

La renovación del componente de DLP apoya el cumplimiento de la norma ISO 27001:2022 de la siguiente manera:

1. Establecer que la información debe etiquetarse de acuerdo con el esquema de clasificación aplicable adoptado por el DNP. Esto ayuda a garantizar que la información sea adecuadamente protegida en función de su nivel de sensibilidad y criticidad. El control del anexo A de la norma ISO 27001:2022 es A.5.13 - Etiquetado de la información.
2. Establecer que la información debe ser clasificada en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización El control del anexo A de la norma ISO 27001:2022 es A.5.12 - Clasificación de la información. En el DNP la información no pública incluye información pública clasificada y reservada de la Ley 1712 de 2014, los datos personales (semiprivados, privados, reservados, sensibles, menores de edad) de la Ley 1581 de 2012, Ley 1266 de 2008 y el decreto 1377 de 2013 y la información con clasificación interna (Confidencial, Uso interno, Uso privado). La clasificación de la información está incluida en el M-PG-07 Manual Operativo de Seguridad de la información.
3. Asegurar que la información en dispositivos móviles y medios de almacenamiento portátil esté protegida contra accesos no autorizados, pérdidas y fugas de información. El control del anexo A de la norma ISO 27001:2022 es A.7.10 - Medios de almacenamiento (principal):

4. Controlar el acceso a la información según la política de control de acceso de la organización, utilizando medidas como DLP para prevenir la divulgación no autorizada de información sensible. El control del anexo A de la norma ISO 27001:2022 es A.5.15 – Control del acceso a la información:
5. Establecer políticas y procedimientos para asegurar que las transferencias de información sean seguras, empleando DLP para monitorear y controlar el flujo de información sensible El control del anexo A de la norma ISO 27001:2022 es A.5.14 - Transferencia de información.
6. Asegurar que los servicios de red estén protegidos contra accesos no autorizados y fugas de información, utilizando soluciones DLP para monitorear y controlar el tráfico de red. El control del anexo A de la norma ISO 27001:2022 es A.8.21 - Seguridad de los servicios de red:
7. Asegurar que los proveedores cumplan con los requisitos de seguridad de la información de la organización, incluyendo la implementación de DLP para proteger la información compartida con terceros. El control del anexo A de la norma ISO 27001:2022 es A.5.19 - Política de seguridad de la información para relaciones con proveedores:
8. Implementar medidas para proteger los registros de accesos no autorizados y modificaciones, utilizando DLP para monitorear y proteger los datos sensibles. El control del anexo A de la norma ISO 27001:2022 es A.5.33 - Protección de los registros:

Para el 2026 la Entidad renovará el licenciamiento de acuerdo con los siguientes elementos:

| 1- Trellix Protect Plus EDR for Endpoint (MV6) | | |
|---|---|---|
| **Tipo** | **Contrato DNP-1167-2024 SGR-058-2024** | **Renovación 2026** |
| Usuarios Finales | 2116 | 2116 |
| Servidor Windows | 539 | 539 |
| Total | 2655 | 2655 |

| 2- Trellix Cloud Workload Security CWSE-S | | |
|---|---|---|
| **Tipo** | **Contrato DNP-1167-2024 SGR-058-2024** | **Renovación 2026** |
| Servidores Físicos on premise | 45 | 45 |
| Servidores virtuales IAAS Azure | 60 | 60 |
| Linux | 22 | 22 |
| Total | 127 | 127 |

| 3- Trellix Mobile Security Advanced – MV3 | |
|---|---|
| **Tipo** | **Adquisición 2026** |
| Dispositivos móviles personales | 55 |

| 4- Trellix Data Loss Prevention (DLP) | |
|---|---|
| **Tipo** | **Adquisición 2026** |
| Usuarios Finales | 2212 |

Las estaciones de escritorio se encuentran ubicadas en:

| SEDES | CIUDAD | DIRECCIÓN FISICA |
|---|---|---|
| **Edificio FONADE** | Bogotá | Calle 26 N° 13-19 |

| | | |
|---|---|---|
| **Edificio World Service** | Bogotá | Carrera 10 N° 24 - 55 |
| **Edificio Gomez** | Bogotá | Carrera 10 N° 24-39 |
| **Dan Social** | Bogotá | Carrera 10 N° 15 - 2 |
| **Regional centro Oriente** | Bucaramanga | Carrera 26 N° 36-14 edificio Fénix |
| **Regional Caribe 1** | Santa Marta | Calle 15 N° 3 - 25 edificio BCH |
| **Regional Eje Cafetero** | Medellín | Carrera 43ª N° 1 Sur -220 oficina 601 edificio el porvenir |
| **Regional Caribe 2** | Montería | Carrera 5 N° 63-15 oficina 902 edificio Bancolombia |
| **Regional Centro Sur** | Neiva | Carrera 5 No. 13 – 56 Oficina 201 edificio Centro de Negocios León Aguilera |
| **Regional Llanos** | Villavicencio | Calle 15 N° 40 - 10 Centro Comercial Primavera |
| **Regional Pacífico** | Cali | Calle 6n # 1 n – 42 edificio torre centenario |

La nube de Azure tiene tres opciones (IaaS, PaaS y SaaS) para la suscripción de servicios relacionados con plataforma que incluye la implementación de servidores. IaaS que es infraestructura como servicio permite que la Entidad tenga control sobre el sistema operativo de los servidores. En PaaS que es plataforma como servicio permite que la Entidad solo pueda instalar sus portales o sistemas sin tener control sobre el sistema operativo. En SaaS que es software como servicio la Entidad solo puede usar un software que ya está implementado. Por lo anterior, con la solución de antivirus se busca continuar protegiendo los servidores on premise en IaaS de la entidad. Los servidores on premise corresponden a los que se encuentran ubicados en las instalaciones del DNP. Los servidores IAAS azure corresponden a los servidores que se encuentran en la nube de Microsoft.

Entre los servidores mencionados anteriormente se encuentran servidores que componen la granja de SharePoint, Servidores con Sistema Operativo Linux. Los servidores virtuales y los usuarios de las estaciones estarán licenciados bajo MVISION Protect Plus EDR for Endpoint, los demás servidores serán licenciados bajo CWS-E (Cloud Workload Security Essentials).

De conformidad con lo anterior, la entidad requiere renovar y adquirir las siguientes cantidades:

| Descripción | Cantidad Licencias |
|---|---|
| Renovación y actualización (upgrade) del licenciamiento por suscripción de Trellix EDR for Endpoint en su edición Enterprise, con Business Software Support por un (1) año. La suscripción cubre hasta cinco (5) dispositivos asignados por usuario, incluyendo funcionalidades avanzadas de detección, investigación y respuesta extendida ante amenazas | 2655 |
| Renovación de la licencia por suscripción Trellix Cloud Workload Security CWSE-S con Business Software Support por un (1) año en su edición Enterprise. | 127 |
| Renovación de la licencia por suscripción Trellix Mobile Security Advanced con Business Software Support por un (1) año. Cubre hasta 5 dispositivos asignados por usuario en su edición Enterprise. | 55 |
| Renovación de la licencia por suscripción Trellix Data Loss Prevention (DLP) con Business Software Support por un (1) año en su edición Enterprise | 2212 |
| Soporte, transferencia de conocimiento de acuerdo con lo requerido en el anexo técnico y con nivel GOLD | 1 |

Para la Entidad es importante contar con una solución de antivirus robusta dada la cantidad de estaciones cliente, servidores y sistemas de información, para lo cual dispone actualmente de la suite Trellix Cloud Workload Security Essentials (CWS-E) de propósito específico para servidores, adicionalmente la entidad cuenta con las funcionalidades de un antivirus EDR (Endpoint Detection and Response) que por sus características proporcionan monitorización y análisis continuo del Endpoint y la red, el cual está enfocado en amenazas avanzadas, detectando esa actividades peligrosas y conteniendo las amenazas, por ello el DNP requiere renovar y adquirir componentes para la solución de seguridad de estaciones clientes, servidores, dispositivos móviles y DLP. La solución está compuesta por protección, detección y respuesta extendidas (antivirus + EDR) para servidores y estaciones cliente (institucionales y personales) (Trellix Protect Plus EDR for Endpoint MV6), protección de cargas de trabajo en entornos virtuales on-premise y nube (Trellix Cloud Workload Security Essentials (CWS-E), protección avanzada para dispositivos móviles (Trellix Mobile Security Advanced) y Prevención de fuga de información (Trellix Data Loss Prevention (DLP)).

Nota: “El incremento a 2.212 de licencias del módulo DLP se encuentra plenamente justificado en la actualización del inventario de cuentas institucionales activas que hacen uso de los servicios tecnológicos protegidos por la solución DLP. Como resultado del proceso de administración y actualización del directorio institucional, se identificó un total de 2.423 cuentas activas que requieren la aplicación de las políticas de prevención de pérdida de información, cifra que constituye la base para el dimensionamiento del licenciamiento requerido.

La solución DLP protege la información institucional mediante la aplicación de controles sobre las cuentas de usuario autorizadas para acceder, procesar, almacenar o compartir información institucional. En consecuencia, el número de licencias debe corresponder al universo real de cuentas activas, con el fin de garantizar la cobertura integral de los controles de seguridad definidos por la Entidad y evitar que existan usuarios sin protección frente a riesgos de fuga, pérdida, alteración o divulgación no autorizada de la información.

En ese sentido, el incremento de 100 licencias no constituye una ampliación injustificada del alcance del contrato, sino el ajuste necesario derivado del crecimiento y la actualización del número de cuentas institucionales activas, garantizando la continuidad del servicio y la adecuada protección de los activos de información de la Entidad.

De acuerdo con el número de cuentas activas identificadas, la distribución de las licencias entre las fuentes de financiación se realiza de manera proporcional al uso del servicio, así:

PGN: 1.791 cuentas (73,92 %).
SGR: 632 cuentas (26,08 %).

Esta distribución permite que la asignación de los recursos corresponda al número de usuarios beneficiarios de cada fuente de financiación, manteniendo criterios de proporcionalidad, eficiencia y adecuada planeación del proceso contractual”

Establecida la necesidad, y en virtud de lo dispuesto en los artículos 2.2.1.2.1.2.7 y 2.2.1.2.1.2.9 del Decreto 1082 de 2015, la Oficina de Tecnología y Sistemas de Información – OTSI analizó los Acuerdos Marco de Precios relacionados con el sector de las Tecnologías de la Información y las Comunicaciones (TIC) y evidenció que actualmente no existe uno que se enmarque particularmente en el tipo de bien o servicio requerido por la Entidad.

En consecuencia, se prevé el uso de la modalidad de selección abreviada mediante subasta inversa, teniendo en cuenta que los bienes a adquirir corresponden a características técnicas uniformes y son de común utilización.

La presente contratación se encuentra acorde con las medidas de austeridad y eficiencia del gasto público dispuestas en el Decreto 1068 del 26 de mayo de 2015 "*por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público*", Decreto 618 del 17 de junio de 2026 *"Por el cual se establece el Plan de Austeridad del Gasto 2026 para los órganos que hacen parte del Presupuesto General de la Nación*" y demás normas concordantes, toda vez que la herramienta requerida es necesaria y suficiente para el desarrollo de las actividades y funciones de la Oficina de Tecnología y Sistemas de Información, y dentro de la presente justificación se evidencia la necesidad de la contratación para el cumplimiento de las actividades misionales de la Entidad

## 2. OBJETO, ESPECIFICACIONES E IDENTIFICACIÓN DEL CONTRATO:

### 2.1. Objeto:

110407626 110409126 - Adquirir la renovación del licenciamiento por suscripción en su modalidad Enterprise de la Suite de Seguridad Trellix que incluye la actualización (upgrade) y soporte especializado de esta herramienta de gestión, con el propósito de garantizar la continuidad del servicio y fortalecer la seguridad de la infraestructura tecnológica del DNP.

### 2.2. Clasificador de Bienes y Servicios UNSPSC:

Conforme a lo establecido en el Decreto 1082 de 2015, el servicio requerido por el Departamento Nacional de Planeación se enmarca en la siguiente clasificación UNSPSC:

*Tabla Clasificador de Bienes y Servicios UNSPSC*

| CLASIFICACIÓN UNSPSC | SEGMENTO | FAMILIA | CLASE |
|---|---|---|---|
| **43232700** | Difusión de Tecnologías de Información y Telecomunicaciones | Software | Software de aplicaciones de red |
| **43232800** | Difusión de Tecnologías de Información y Telecomunicaciones | Software | Software de administración de redes |
| **43233200** | Difusión de Tecnologías de Información y Telecomunicaciones | Software | Software de seguridad y protección |
| **81111500** | Servicios Basados en Ingeniería, Investigación y Tecnología | Servicios informáticos | Ingeniería de software o hardware |
| **81112200** | Servicios Basados en Ingeniería, Investigación y Tecnología | Servicios informáticos | Mantenimiento y soporte de software |

Fuente: https://www.colombiacompra.gov.co/clasificador-de-bienes-y-Servicios

**Nota**: La presente solicitud hace parte del Plan Anual de Adquisiciones 2026, actualizada en la versión No. 19 bajo los PABS **110407626 110409126** cuyo objeto es *"Adquirir la renovación del licenciamiento por suscripción en su modalidad enterprise de la Suite de Seguridad Trellix que incluye la actualización (upgrade) y soporte especializado de esta herramienta de gestión, con el propósito de garantizar la continuidad del servicio y fortalecer la seguridad de la infraestructura tecnológica del DNP"*. El responsable de la línea es la OTSI - Oficina de Tecnologías y Sistemas de Información, con un valor registrado de $899.429.000 y los códigos UNSPSC 43232700; 43232800; 43233200; 81111500; 81112200

**2.3. Alcance del objeto (SI APLICA):**

El alcance del objeto comprende la renovación, actualización (upgrade) y soporte especializado de la suite de seguridad TRELLIX, incluyendo el licenciamiento bajo modalidad de suscripción, el mantenimiento, el acceso a nuevas versiones y actualizaciones de la solución, así como los servicios asociados requeridos para su correcta operación en la Entidad.

Lo anterior incluye el acceso a la plataforma para la identificación, análisis y gestión de virus informáticos y identificación de acceso de usuarios no autorizados sobre los activos tecnológicos del Departamento Nacional de Planeación, la ejecución de escaneos de seguridad, la generación de reportes, indicadores y tableros de control, así como el soporte técnico y acompañamiento necesario durante la vigencia del contrato, garantizando la continuidad del servicio y el fortalecimiento de la seguridad de la infraestructura tecnológica de la Entidad.

**2.4. Especificaciones Técnicas:**

En desarrollo del objeto del contrato que se suscriba como consecuencia del presente proceso de selección, el oferente seleccionado se compromete con el DNP, a desarrollar las actividades de acuerdo con los requerimientos mínimos exigidos en la FICHA TÉCNICA Y CONDICIONES EXIGIDAS, en las instalaciones del Departamento Nacional de Planeación, ubicadas en la Calle 26 No. 13 – 19, piso 12 de la ciudad de Bogotá, D.C**.**

## 3. MODALIDAD DE SELECCIÓN DEL CONTRATISTA Y FUNDAMENTOS JURÍDICOS QUE LA SOPORTAN:

Teniendo en cuenta que la naturaleza del objeto contractual, se enmarca dentro de los conceptos señalados en el artículo 2 de la Ley 1150 de 2007, el DNP considera pertinente adelantar un proceso de selección a través de la modalidad de Selección Abreviada para la Adquisición de Bienes y Servicios de Características Técnicas Uniformes mediante Subasta Inversa, de acuerdo con la modalidad de selección establecida en el Título I, Artículo 2, Numeral 2, literal a) de la Ley 1150 de 2007 el cual establece:

> "ARTÍCULO 2o. DE LAS MODALIDADES DE SELECCIÓN. La escogencia del contratista se efectuará con arreglo a las modalidades de selección de licitación pública, selección abreviada, concurso de méritos y contratación directa, con base en las siguientes reglas:
>
> (…)
>
> *2. Selección abreviada. La Selección abreviada corresponde a la modalidad de selección objetiva prevista para aquellos casos en que, por las características del objeto a contratar, las circunstancias de la contratación o la cuantía o destinación del bien, obra o servicio puedan adelantarse procesos simplificados para garantizar la eficiencia de la gestión contractual*."

Asimismo, con el fin de dar cumplimiento a la norma mencionada, el Departamento Nacional de Planeación y para llevar a cabo el presente proceso contractual, utilizará el proceso de selección abreviada a través del procedimiento de Subasta Inversa de acuerdo con lo señalado en el artículo 2.2.1.2.1.2.2 (modificado por el artículo 6 del Decreto 1860 de 2021) y siguientes del Decreto 1082 de 2015.

Así mismo se indica que, realizada la consulta en la Tienda Virtual del Estado Colombiano (Colombia Compra Eficiente) no hay un Acuerdo Marco de Precios sobre el objeto a contratar, ni tampoco Instrumentos de Agregación de Demanda vigentes a la fecha de la consulta, que satisficiera o que contemple la renovación del licenciamiento por suscripción en su modalidad enterprise de la Suite de Seguridad Trellix, con las funcionalidades técnicas requeridas por la entidad y equivalentes a las de la solución Trellix..

En consecuencia, al no encontrarse disponible en la Tienda Virtual del Estado Colombiano un instrumento que permita la adquisición de una solución con las características técnicas y funcionales requeridas se concluye que no es posible atender esta necesidad mediante los mecanismos de compra por Catálogo.

Ahora bien, en cumplimiento del artículo 2 del Decreto 310 de 2021, se evaluó la utilización del Mercado de Compras Públicas de la Bolsa Mercantil de Colombia como mecanismo alternativo para la adquisición requerida, como resultado del análisis, se evidenció que el objeto contractual no identificó que dicho mecanismo genere ventajas económicas frente a la subasta inversa electrónica. Dicho análisis se encuentra incorporado en el estudio del sector.

En consecuencia, se prevé el uso de la Subasta Inversa como herramienta para la selección abreviada que corresponde, teniendo en cuenta que la herramienta a contratar posee las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos, que permite que su contratación sea desarrollada a través de la precitada modalidad.

Así las cosas, si bien el objeto contractual comprende la renovación del licenciamiento por suscripción de la Suite de Seguridad Trellix con soporte especializado y actualización (upgrade), las condiciones técnicas del bien se encuentran definidas y estandarizadas por el fabricante, permitiendo establecer especificaciones objetivas y homogéneas para todos los oferentes. En consecuencia, la comparación de las ofertas recae esencialmente sobre variables económicas, configurándose un bien de características técnicas uniformes y de común utilización, conforme lo previsto en el citado marco normativo, razón por la cual resulta procedente la selección abreviada mediante subasta inversa electrónica.

En atención con lo dispuesto en el artículo 2.2.1.2.1.2.5 del Decreto 1082 de 2015, la Entidad utilizará la modalidad de subasta inversa a realizarse será a través de la plataforma SECOP II.

## 4. VALOR ESTIMADO DEL CONTRATO - PRESUPUESTO OFICIAL.

Con la finalidad de establecer el valor del presupuesto oficial para el presente proceso de selección, se publicó por medio de la plataforma del SECOP II un evento de cotización para dicho requerimiento (DNP-SIP 037-2026)[6], del cual se recibieron tres (3) cotizaciones de proveedores interesados en el proceso, las cuales corresponden a una gran empresa y dos medianas empresas, las cuales se relacionan a continuación:

| NIT | RAZÓN SOCIAL | TAMAÑO |
|---|---|---|
| 901223827 | DATASEC SAS | MEDIANA EMPRESA |
| 900425697 | HEIMCORE | GRAN EMPRESA |
| 800210453 | MULTISOFT | MEDIANA EMPRESA |

**Cotizaciones recibidas:** a continuación, se presenta el resumen de las cotizaciones:

[6]Link de evento de cotización SECOP II:
**https://community.secop.gov.co/Public/Tendering/ContractNoticePhases/View?PPI=CO1.PPI.47869267&isFromPublicArea=True&isModal=False**

| COTIZANTE | SUBTOTAL | IVA | VALOR TOTAL COTIZACIÓN |
|---|---|---|---|
| COTIZANTE 1 | $753.436.511 | $143.151.160 | $896.587.671,00 |
| COTIZANTE 2 | $755.643.752 | $143.571.792 | $899.215.544,00 |
| COTIZANTE 3 | $757.370.408 | $143.902.733 | $901.273.141,00 |

**8.2. Valor estimado del proceso**

Como consecuencia del estudio de mercado, y para establecer el presupuesto oficial se analizaron las tres (3) cotizaciones recibidas por medio de estadística descriptiva con medidas de tendencia central, de tal manera que se pueda determinar la opción más adecuada para definir el presupuesto oficial del presente proceso de contratación, las cuales se relacionan a continuación:

| | |
|---|---|
| Media | $899.025.452 |
| Mediana | $899.215.544 |
| Desviación estándar | $2.348.512 |
| **Coeficiente de Variación** | **0,26%** |

El análisis evidencia una diferencia no significativa entre la media aritmética y la mediana, así como un coeficiente de variación de 0,26%, lo que confirma la alta homogeneidad[7] de las cotizaciones y la ausencia de valores atípicos que hagan necesario acudir a metodologías alternativas de estimación.

La baja dispersión observada se explica por las características del objeto contractual, el cual corresponde a la renovación del licenciamiento por suscripción en modalidad Enterprise de la Suite de Seguridad Trellix, incluyendo las actualizaciones (upgrade) y el soporte especializado asociado, este tipo de soluciones tecnológicas se comercializa bajo esquemas de licenciamiento definidos por el fabricante, con condiciones técnicas y comerciales estandarizadas para los canales autorizados.

Por tal motivo, los proveedores estructuran sus cotizaciones sobre una misma base de requerimientos funcionales, cantidades, niveles de servicio y condiciones de soporte, lo que genera una alta uniformidad en la formación de precios y adicionalmente, al tratarse de una renovación de licenciamiento de una solución específica utilizada por la Entidad, los márgenes de variación entre las ofertas tienden a ser reducidos, toda vez que las condiciones comerciales se encuentran estrechamente ligadas a las políticas de licenciamiento y soporte establecidas por el fabricante.

En este contexto, la baja dispersión de las cotizaciones no obedece a una anomalía en el análisis, sino a las características propias del mercado de licenciamiento especializado de software de ciberseguridad y a la estandarización de las condiciones de suministro, circunstancia que valida la utilización de la media aritmética como criterio técnico para la estimación del presupuesto oficial.

[7] El coeficiente de variación es el número de veces que la desviación estándar incluye a la media, a mayor coeficiente de variación, mayor dispersión, si 0≤CV≤0,3 existe poca dispersión, por lo tanto la media es representativa. Si 0,3 ≤CV<1 la dispersión es alta. La dispersión será baja si CV es cercano a 0,3 y alta si es cercano a 1.

En consecuencia, la media aritmética constituye una medida técnicamente representativa para la estimación del presupuesto oficial, al reflejar el comportamiento homogéneo de los precios del mercado. Bajo estas condiciones, el presupuesto oficial garantiza la suficiencia presupuestal para atender el alcance técnico requerido, la viabilidad financiera del proceso y la participación de potenciales oferentes en condiciones de competencia

## ITEMS COTIZADOS

| Ítem | Descripción | Cantidad Licencias |
|---|---|---|
| 1 | Renovación y actualización (upgrade) del licenciamiento por suscripción de Trellix EDR for Endpoint en su edición Enterprise, con Business Software Support por un (1) año. La suscripción cubre hasta cinco (5) dispositivos asignados por usuario, incluyendo funcionalidades avanzadas de detección, investigación y respuesta extendida ante amenazas. | 2655 |
| 2 | Renovación de la licencia por suscripción Trellix Cloud Workload Security CWSE-S con Business Software Support por un (1) año en su edición Enterprise | 127 |
| 3 | Renovación de la licencia por suscripción Trellix Mobile Security Advanced con Business Software Support por un (1) año. Cubre hasta 5 dispositivos asignados por usuario en su edición Enterprise | 55 |
| 4 | Renovación de la licencia por suscripción Trellix Data Loss Prevention (DLP) con Business Software Support por un (1) año en su edición Enterprise | 2212 |
| 5 | Soporte, transferencia de conocimiento de acuerdo con lo requerido en el anexo técnico y con nivel Gold. | 1 |

## ANALISIS DE LAS COTIZACIONES

| Ítem | Descripción | Cantidad Licencias | COTIZANTE 1 | | COTIZANTE 2 | | COTIZANTE 3 | |
|---|---|---|---|---|---|---|---|---|
| | | | Valor unitario | Valor total | Valor unitario | Valor total | Valor unitario | Valor total |
| 1 | Renovación y actualización (upgrade) del licenciamiento por suscripción de Trellix EDR for Endpoint en su edición Enterprise, con Business Software Support por un (1) año. La suscripción cubre hasta cinco (5) dispositivos asignados por usuario, incluyendo funcionalidades avanzadas de detección, investigación y respuesta extendida ante amenazas. | 2655 | 151.786,00 | 402.991.830,00 | 159.394,00 | 423.191.070,00 | 155.387,00 | 412.552.485,00 |
| 2 | Renovación de la licencia por suscripción Trellix Cloud Workload Security CWSE-S con Business Software Support por un (1) año en su edición Enterprise | 127 | 645.139,00 | 81.932.653,00 | 555.837,00 | 70.591.299,00 | 630.495,00 | 80.072.865,00 |
| 3 | Renovación de la licencia por suscripción Trellix Mobile Security Advanced con Business Software Support por un (1) año. Cubre hasta 5 dispositivos asignados por usuario en su edición Enterprise | 55 | 332.392,00 | 18.281.560,00 | 339.293,00 | 18.661.115,00 | 315.394,00 | 17.346.670,00 |

| Ítem | Descripción | Cantidad Licencias | COTIZANTE 1 | | COTIZANTE 2 | | COTIZANTE 3 | |
|---|---|---|---|---|---|---|---|---|
| | | | Valor unitario | Valor total | Valor unitario | Valor total | Valor unitario | Valor total |
| 4 | Renovación de la licencia por suscripción Trellix Data Loss Prevention (DLP) con Business Software Support por un (1) año en su edición Enterprise | 2212 | 59.844,00 | 132.374.928,00 | 60.039,00 | 132.806.268,00 | 57.650,00 | 127.521.800,00 |
| 5 | Soporte, transferencia de conocimiento de acuerdo con lo requerido en el anexo técnico y con nivel Gold. | 1 | 117.855.540,00 | 117.855.540,00 | 110.394.000,00 | 110.394.000,00 | 119.876.588,00 | 119.876.588,00 |
| **VALOR ANTES DE IVA** | | | | 753.436.511,00 | | 755.643.752,00 | | 757.370.408,00 |
| **VALOR IVA** | | | | 143.151.160,00 | | 143.571.792,00 | | 143.902.733,00 |
| **VALOR INCLUIDO IVA** | | | | **896.587.671,00** | | **899.215.544,00** | | **901.273.141,00** |

| COTIZANTE | ÍTEM 1 | ÍTEM 2 | ÍTEM 3 | ÍTEM 4 | ÍTEM 5 |
|---|---|---|---|---|---|
| COTIZANTE 1 | $151.786 | $645.139 | $332.392 | $59.844 | $117.855.540 |
| COTIZANTE 2 | $159.394 | $555.837 | $339.293 | $60.039 | $110.394.000 |
| COTIZANTE 3 | $155.387 | $630.495 | $315.394 | $57.650 | $119.876.588 |

| | | | | | |
|---|---|---|---|---|---|
| PROMEDIO DEL COMPONENTE | $155.522,00 | $610.490,00 | $329.026,00 | $59.178,00 | $116.042.043,00 |
| VALOR X CANTIDAD | $412.910.910,00 | $77.532.230,00 | $18.096.430,00 | $130.901.736,00 | $116.042.043,00 |
| VALOR TOTAL | $755.483.349 | | | | |
| IVA | $143.541.836 | | | | |
| **VALOR TOTAL ESTIMADO** | **$899.025.185** | | | | |
| **VALOR TOTAL ESTIMADO SMMLV** | **513,46** | | | | |

Debido a lo expuesto, el DNP establece como presupuesto oficial para este proceso es hasta la suma de ***OCHOCIENTOS NOVENTA Y NUEVE MILLONES VEINTICINCO MIL CIENTO OCHENTA Y CINCO PESOS M/CTE (899.025.185),*** incluido IVA y todos los tributos a los que haya lugar.

### 8.3 Certificado de disponibilidad presupuestal

El presente proceso cuenta con dos fuentes de financiación, correspondientes al Presupuesto General de la Nación (PGN) y a los recursos de funcionamiento del Sistema General de Regalías (SGR), en este sentido, se hace necesario establecer un criterio técnico que permita definir la distribución proporcional de los recursos entre dichas fuentes, garantizando coherencia con el uso y la demanda del servicio.

En relación con la distribución de los recursos entre las fuentes PGN y SGR, esta se fundamenta en la proporción de usuarios activos que hacen uso de los servicios asociados al proceso, como se evidencia en el siguiente cuadro:

| FUENTE | No DE CUENTAS ASOCIADAS | PARTICIPACIÓN |
|---|---|---|

| | | |
|---|---|---|
| PGN | 1.791 | 73,92% |
| SGR | 632 | 26,08% |
| TOTAL | 2.423 | 100% |

En consecuencia, la distribución presupuestal definida (73,92% PGN y 26.08% SGR) guarda coherencia con la proporción real de uso del servicio, medida a partir del número de cuentas activas, este criterio permite asegurar una asignación equitativa y proporcional de los recursos, en función de la demanda efectiva de cada fuente de financiación. Por lo anterior, se evidencia que la distribución de los recursos no es arbitraria, sino que responde a un análisis cuantitativo verificable, alineado con las necesidades operativas y el número de usuarios que soportan el funcionamiento tanto del DNP como del SGR.

El compromiso presupuestal que demande el gasto que se derive del presente proceso de contratación, el cual se encuentra incluido en el Plan Anual de Adquisiciones de la entidad (Versión 19) para la vigencia 2026 con los PABS 110407626 y 110409126, respaldado con el Certificado de Disponibilidad Presupuestal DNP nro. 139226 del 23 de julio de 2026 expedido por la Coordinadora del Grupo de Presupuesto del DNP y el Certificado de Disponibilidad presupuestal SGR nro. 33626 del 23 de julio de 2026 expedido por la directora Corporativa SGSGR distribuidos con los siguientes rubros:

**Cuadro Distribución de Rubro Presupuestal**

| USO | % PARTICIPACIÓN | VALOR | CDP |
|---|---|---|---|
| C-0399-1000-8-0-0399066-02 ADQUISICIÓN DE BIENES Y SERVICIOS - SERVICIOS TECNOLOGICOS - FORTALECIMIENTO DE LAS TIC PARA EL CUMPLIMIENTO DE LOS OBJETIVOS DEL DNP A NIVEL NACIONAL | 73,92% | $ 664.559.417,00 | 139226 |
| A-02-01-01-006-002-03-1-01 PAQUETES DE SOFTWARE - FUN OPERATIVIDAD Y ADMINISTRACIÓN - 1103012 FTO- ÓRGANO | 26,08% | $ 234.465.768,00 | 33626 |
| **TOTAL** | **100%** | **$ 899.025.185,00** | |

**NOTA 1:** Se entiende que en el Valor Total del presupuesto estimado incluye tasas, gravámenes, impuestos y todos los costos directos e indirectos derivados de la ejecución del contrato, así como todos los gastos que deberá hacer el contratista como: administración, salarios, prestaciones sociales, y otros que graven el capital, renta, utilidad del Contratista, y en general todo cuanto sea necesario y conveniente para dar cumplimiento al objeto del presente proceso, la suma anterior, se obtuvo de la información contenida en el estudio de mercado que realizó internamente la entidad y hace parte del estudio del sector.

**a. Determinación de la concordancia del objeto del contrato con el rubro presupuestal a través del cual se financia:**

La presente contratación está encaminada a dar cumplimiento al objetivo general del proyecto de inversión BPIN 2022011000029 "FORTALECIMIENTO DE LAS TIC PARA EL CUMPLIMIENTO DE LOS OBJETIVOS DEL DNP A NIVEL NACIONAL", el cual es *"Fortalecer la adopción, uso y apropiación de tecnologías orientadas a la gestión de la información institucional del DNP"* y en particular con el objetivo específico *"Mejorar la gestión de la información y*

*tecnologías, y su integración para la toma de decisiones"* con el cual se garantiza una Infraestructura tecnológica operativa, que satisfaga la dinámica de solicitudes de servicios de TIC de la Entidad.

La contratación por realizar tiene directa concordancia con la misión de la Oficina de Tecnología y Sistemas de Información del DNP y está, asociado con el siguiente producto del plan de acción **7259: Informe de seguimiento actividades acorde al plan anual de mantenimiento a la plataforma de TIC entregado.**

## 5. JUSTIFICACIÓN DE LOS FACTORES DE SELECCIÓN

De acuerdo con el artículo 2 de la Ley 1150 de 2007, la escogencia del contratista se efectúa con arreglo a las modalidades de selección, entre las cuales está la selección abreviada. Como causal de selección abreviada está la adquisición de bienes y servicios de características técnicas uniformes y de común utilización. El Artículo 5 de la misma ley establece el principio de selección objetiva, con base en el cual se debe escoger el ofrecimiento más favorable a la entidad y a los fines que ella busca, con lo cual, los factores de escogencia y calificación que se establecen en los términos y condiciones para la contratación deben atender a este principio.

Conforme lo establece el artículo 5 de la Ley 1150 de 2007 y el artículo 2.2.1.1.1.5.3 del Decreto 1082 de 2015, se tendrán en cuenta los criterios que le permiten al DNP la escogencia del ofrecimiento más favorable a la Entidad y a los fines que ella busca con la contratación, teniendo en cuenta los criterios de habilitación y evaluación de las ofertas. Dentro de los primeros, se encuentran:

a) Capacidad Jurídica,
b) Condiciones de Experiencia,
c) Capacidad financiera, y
d) Capacidad Organizacional;

Dentro de los segundos, están aquellos aspectos que determinan la mejor oferta para la entidad que por tratarse de una selección abreviada para la adquisición de bienes y servicios de características técnicas uniformes y de común utilización, para la obtención de la oferta más favorable (de las presentadas por proponentes habilitados) se hará uso exclusivamente del precio, obtenido a través de una subasta inversa electrónica.

Entiéndase por bienes y servicios de común utilización aquellos con especificaciones técnicas y patrones de desempeño y calidad iguales o similares, que en consecuencia pueden ser agrupados como bienes y servicios homogéneos para su adquisición, y a los que se refiere el literal (a) del numeral 2 del artículo 2 de la Ley 1150 de 2007.

Es de anotar que el servicio que pretende adquirir el DNP en la presente contratación se considera de características técnicas uniformes y de común utilización, el cual es ofrecido de manera masiva en el mercado, tal como se demuestra en el anexo técnico.

En ejercicio de lo señalado, la Entidad ha previsto la verificación de los siguientes factores:

### 5.1. REQUISITOS HABILITANTES

### 5.1.1 REQUISITOS JURÍDICOS HABILITANTES (CAPACIDAD JURÍDICA)

**1. Carta de Presentación de la Oferta (Anexo 2)**

El proponente aportará una carta de presentación que deberá identificar claramente el sujeto jurídico que hace la oferta; hacer un ofrecimiento incondicional de celebrar el contrato propuesto; y manifestar el compromiso de acoger y respetar las reglas de este proceso de selección.

Esta deberá estar suscrita por el interesado que será la persona natural o el representante legal para personas jurídicas, del consorcio o unión temporal, o por el apoderado debidamente constituido, evento en el cual se debe anexar poder donde se especifique que se otorga para presentar la carta de presentación y la oferta.

Para facilitar este trámite el pliego de condiciones dispondrá del Anexo 2 – "Carta de presentación de la oferta"- para tal fin. El contenido de dicho documento podrá ser variado a criterio de los proponentes, siempre y cuando conserve sus elementos esenciales. El proponente NO podrá señalar condiciones diferentes a las establecidas en el pliego de condiciones.

Se entenderá con la suscripción de la carta de presentación de la Oferta que el proponente cumple con las condiciones señaladas en la FICHA TÉCNICA Y CONDICIONES EXIGIDAS.

**2. Documento de Conformación del Consorcio o Unión Temporal, si es la condición del oferente**

Consorcio o Unión Temporal: Los proponentes que se presenten bajo una de estas modalidades deberán presentar el documento que acredite la conformación del Consorcio o Unión Temporal con el lleno de los requisitos exigidos por el parágrafo 1º del artículo 7º de la Ley 80 de 1993.

En el documento de constitución deberá constar la siguiente información:

a. Los proponentes indicarán si su participación es a título de Consorcio o Unión Temporal.
b. En caso de unión temporal deberán señalar los términos y porcentaje de su participación en la propuesta y en la ejecución del contrato, los cuales no podrán ser modificados sin el consentimiento previo del Departamento Nacional de Planeación.
c. Designar la persona que para todos los efectos representará el Consorcio o a la Unión Temporal y señalarán las reglas básicas que regulen las relaciones entre ellos y su responsabilidad.
d. Indicar el término de duración del Consorcio o Unión temporal el cual no podrá ser inferior al plazo de ejecución del contrato y tres (3) años más.

Para la presentación de los documentos que se enuncian como capacidad jurídica del proponente (requisitos habilitantes jurídicos), se deberá tener en cuenta cuando se señale expresamente que cada uno de los integrantes del Consorcio o de la Unión Temporal deberá acreditarlos en forma individual, sin perjuicio del documento de constitución del Consorcio o Unión Temporal.

En los casos en que se conformen sociedades bajo cualquiera de las modalidades previstas en la ley con el único objeto de presentar una propuesta, celebrar y ejecutar un contrato estatal, la responsabilidad y sus efectos se regirá por las disposiciones previstas en la ley para los consorcios, por lo tanto en caso de uniones temporales es obligatorio

señalar los términos y porcentaje de participación de cada integrante en la propuesta y en la ejecución del contrato, so pena de ser tomada como consorcio.

**3. Garantía de Seriedad de la Oferta.**

El oferente deberá garantizar el cumplimiento de la oferta que presenta en el proceso de contratación, la suscripción del respectivo contrato y la constitución de la garantía única, en caso de que este le sea adjudicado, mediante la constitución de una garantía de seriedad de la misma, a favor del DEPARTAMENTO NACIONAL DE PLANEACIÓN identificado con NIT 899.999.011-0, por un valor equivalente al diez (10 %) del valor del presupuesto oficial determinado para la contratación, válida como mínimo por TRES (3) MESES contados a partir de la fecha definitiva de cierre del presente proceso de selección.

La garantía no podrá tener cláusulas excluyentes adicionales a las timbradas en ella.

El oferente, por el acto de ofertar, acepta que el Departamento Nacional de Planeación solicite ampliar el término de vigencia de la garantía, en la medida en que ello sea necesario. Los costos que se causen por la expedición o prorrogas de la garantía estarán a cargo del oferente.

Salvo fuerza mayor o caso fortuito debidamente comprobado, la garantía de seriedad de la oferta se hará efectiva a favor del Departamento Nacional de Planeación de conformidad con el artículo 2.2.1.2.3.1.6 del Decreto 1082 de 2015.

> *"Artículo 2.2.1.2.3.1.6. Garantía de los Riesgos derivados del incumplimiento de la oferta. La garantía de seriedad de la oferta debe cubrir la sanción derivada del incumplimiento de la oferta, en los siguientes eventos:*
>
> *La no ampliación de la vigencia de la garantía de seriedad de la oferta cuando el plazo para la adjudicación o para suscribir del contrato es prorrogado, siempre que tal prórroga sea inferior a tres (3) meses.*
>
> *El retiro de la oferta después de vencido el plazo fijado para la presentación de las ofertas.*
> *La no suscripción del contrato sin justa causa por parte del adjudicatario.*
> *La falta de otorgamiento por parte del proponente seleccionado de la garantía de cumplimiento del contrato."*

Lo anterior, sin menoscabo de las acciones legales conducentes al reconocimiento de perjuicios causados y no cubiertos por la cuantía de esta garantía y sin perjuicio de que el Departamento Nacional de Planeación, pueda optar por adjudicar al oferente calificado en segundo lugar.

Nota 1: En caso de que la Garantía de Seriedad allegada por el proponente no cumpla con los requisitos establecidos en el presente numeral, se podrá subsanar la misma de acuerdo con lo establecido por la Ley 1882 de 2018 y la Circular Única de Colombia Compra Eficiente, siempre que la subsanación recaiga sobre la póliza inicialmente aportada. No podrá en ningún caso subsanarse la Garantía de Seriedad de la propuesta con una garantía diferente a la inicialmente allegada.

Nota 2: En el caso de consorcios o uniones temporales la garantía deberá tomarse por todos sus integrantes, señalando su porcentaje de participación y NIT.

**4. Poder cuando la propuesta se presente por intermedio de un apoderado.**

Cuando el proponente actúe a través de apoderado, debe presentar el poder especial debidamente autenticado para presentar la propuesta, y para firmar el contrato respectivo, si es el caso.

**5. Apoderado para oferentes extranjeros.**

Los proveedores extranjeros pueden estar representados por apoderados o representantes legales, caso en el cual el interesado debe acreditar que quien presenta la oferta está legalmente facultado para comprometer al interesado, presentar el documento correspondiente bien sea un poder o un nombramiento en el cual consten las facultades otorgadas y acreditar la identidad del apoderado o representante legal con su documento de identificación.

La persona natural o jurídica de origen extranjero, que no sea residente en Colombia, podrá presentar propuesta, previo cumplimiento de los requisitos generales establecidos para tal fin, aplicables a los oferentes nacionales con las excepciones del caso y especialmente cumpliendo los siguientes requisitos:

a. Deberá adjuntar el certificado de existencia y representación legal o el documento equivalente del país en que se haya constituido legalmente. Si el mismo se encuentra en idioma distinto al español o castellano oficial de la República de Colombia, debe presentarse en su lengua original junto con la traducción oficial al castellano. En el evento en que el oferente extranjero ostente limitación en su capacidad de contratación o de oferta, deberá adjuntar el documento mediante el cual se remueva dicha limitación. En lo no previsto aquí expresamente, se aplicará el régimen dispuesto para los nacionales colombianos y que le sea aplicable a los extranjeros.

b. En cumplimiento de lo ordenado por el Parágrafo 2° del artículo 6 de la Ley 1150 de 2007, modificado por el artículo 221 del Decreto Ley 019 de 2012, el oferente extranjero, persona natural sin domicilio en Colombia o persona jurídica extranjera que no tenga establecida sucursal en el país, NO se encuentra obligado a inscribirse ni calificarse en el RUP.

c. El oferente extranjero deberá relacionar y certificar la experiencia exigida en este proceso. En el evento en que dicha experiencia se haya obtenido en país distinto a Colombia, para efectos de certificarla deberá adjuntar la certificación respectiva que deberá cumplir con los requisitos establecidos en este documento. Adicionalmente, si la certificación se encuentra en idioma distinto al de la República de Colombia, deberá adjuntarse además del documento en idioma extranjero, la traducción simple del documento y entregar la traducción oficial al castellano dentro del plazo previsto para la subsanación, tal y como lo establece la Circular Externa Única expedida por Colombia Compra Eficiente.

Nota: En el evento de resultar favorecido con la adjudicación, el oferente deberá presentar la traducción oficial al castellano de los documentos presentados en idioma extranjero, antes de la fecha de suscripción del contrato prevista en el cronograma del proceso. La traducción oficial debe ser el mismo texto presentado, de acuerdo con lo dispuesto en la Circular Externa Única expedida por Colombia Compra Eficiente y el artículo 251 del Código General del Proceso. Vencido este plazo sin que se hubiera presentado los documentos, se considerará que no existe interés para suscribir el Contrato y se hará efectiva la Garantía de Seriedad.

En el evento de resultar favorecido con la adjudicación un proponente extranjero sin domicilio ni sucursal en Colombia, para efectos de poder ejecutar el contrato deberá previamente constituir una sucursal en Colombia en los términos del Código de Comercio, de acuerdo con lo señalado en los artículos 471 y 474 del citado Código.

**6. Fotocopia del documento de identidad del representante legal y/o su apoderado o persona natural.**

Las personas naturales colombianas deberán presentar copia de su cédula de ciudadanía. Las personas naturales extranjeras, deberán acreditar su existencia mediante la presentación de la copia de su pasaporte, y si se encuentran residenciadas en Colombia, mediante la presentación de la copia de la cédula de extranjería expedida por la autoridad colombiana competente o visa de residente.

En caso de personas jurídicas, se aportará copia de la cédula de ciudadanía del representante legal y en el evento de consorcio, unión temporal, copia de la cédula de ciudadanía del representante legal de los mismos y del representante legal o persona natural de cada uno de los integrantes que lo conforman.

**7. Certificaciones sobre el cumplimiento de las obligaciones de seguridad social y pago de aportes parafiscales. (Anexo 3 MODELO DE CERTIFICACIÓN DE PAGO SEGURIDAD SOCIAL Y DE APORTES PARAFISCALES).**

De conformidad con lo establecido en el artículo 23 Ley 1150 de 2007, artículo 50 de la Ley 789 de 2002 Ley 828 de 2003 y Ley 1562 de 2012, el oferente deberá certificar el pago de los aportes realizados en cumplimiento de sus obligaciones y pago de aportes de sus empleados a los sistemas de salud, riesgos laborales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar, Servicio Nacional de Aprendizaje, cuando a ello haya lugar, mediante certificación expedida por el revisor fiscal, cuando éste exista de acuerdo con los requerimientos de ley, o en su defecto por el representante legal, que acredite el cumplimiento de la obligación por lo menos durante los últimos seis (6) meses calendario legalmente exigibles a la fecha de cierre del presente proceso de selección.

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

Si se trata de un consorcio o unión temporal, se deberá allegar la certificación de cumplimiento antes mencionada para cada uno de los miembros.

Las personas naturales deberán declarar bajo la gravedad de juramento, que han efectuado el pago por concepto de aportes y el de sus empleados (eso último en caso de tener empleados a cargo) a los sistemas de salud, pensiones, riesgos laborales, cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar -ICBF- y Servicio Nacional de Aprendizaje -SENA-, cuando a ello hubiere lugar, durante los últimos seis (6) meses calendario legalmente exigibles a la fecha de presentación de Propuesta para el presente proceso de selección. (Anexo No. 3 MODELO DE CERTIFICACIÓN DE PAGO SEGURIDAD SOCIAL Y DE APORTES PARAFISCALES).

En el evento en que la sociedad no tenga más de seis (6) meses de constituida, deberá acreditar los pagos a partir de la fecha de su constitución.

En caso de que el proponente, persona natural o jurídica, no tenga personal a cargo y por ende no esté obligado a efectuar el pago de aportes parafiscales y seguridad social debe, bajo la gravedad de juramento, indicar esta circunstancia en la mencionada certificación.

Nota 1: Esta información deberá ser certificada de acuerdo con el Anexo 3 –Modelo De Certificación De Pago Seguridad Social y de Aportes Parafiscales-, dispuesto por el DNP para tal efecto en el Pliego de Condiciones.

Nota 2: Para la persona jurídica, en caso de que la certificación de aportes de seguridad social ARL y parafiscales sea expedida por revisor fiscal esta deberá venir acompañada de la tarjeta profesional del revisor fiscal y el certificado de antecedentes vigente expedido por la Junta Central de Contadores.

Nota 3: En el caso de que el proponente sea extranjero sin domicilio o sucursal en Colombia, en cuyo país de origen no exista la obligación de realizar aportes parafiscales y/o al sistema de seguridad social, deberá indicar esta circunstancia en documento suscrito bajo la gravedad del juramento por la proponente persona natural o por el representante legal de la persona jurídica, consorcio o unión temporal. De igual manera lo acreditará, en el caso de que en su país de origen se tenga la obligación de cumplir con las obligaciones de seguridad social y pago de aportes parafiscales.

**8. Registro Único de Proponentes.**

Inscripción en el RUP:

De conformidad con el Artículo 2.2.1.1.1.5.1 del Decreto 1082 de 2015, para el presente proceso de contratación el Proponente singular o cada uno de los miembros del consorcio o unión temporal (si el Proponente es plural) debe acreditar que está inscrito en el RUP de la Cámara de Comercio con jurisdicción en su domicilio principal, inscripción que debe estar en firme al cierre del Proceso de Contratación.

El Proponente deberá presentar el registro único de proponentes con fecha de expedición no mayor a un (1) mes anterior a la fecha del cierre del presente proceso de selección.

Renovación y firmeza del RUP:

El RUP debe renovarse a más tardar el quinto día hábil del mes de abril de cada año, de lo contrario cesan sus efectos.

Al cierre del presente proceso de contratación, es decir, hasta el plazo para presentar ofertas, el RUP debe encontrarse vigente, esto es, que el proponente haya presentado la información para renovar el registro en el término anteriormente establecido. Para verificar que los efectos del RUP no han cesado, es necesario que el certificado contenga la anotación de que el inscrito ya radicó los documentos para la renovación o el soporte idóneo que así lo demuestre.

La información contenida en el RUP, previa a la suministrada para renovar el registro, continúa en firme hasta que finalice el trámite de renovación correspondiente. Así, en el periodo comprendido entre el momento de la solicitud de

renovación y el momento en que adquiera firmeza la información renovada, es válido el RUP del año anterior, cuyos efectos no han cesado y se encuentre vigente y en firme.

El proponente puede acreditar la firmeza del RUP dentro del término de traslado del informe de evaluación, en todo caso, el DNP dará aplicación a lo dispuesto en el artículo 5 de la Ley 1882 de 2018, que adiciono el parágrafo 4 al artículo 5 de Ley 1150 de 2007; estos son, hasta antes del inicio del evento de subasta.

Cuando el proponente sea consorcio o unión temporal cada uno de sus integrantes deberá anexar el documento aquí descrito.

Dicho registro debe permanecer vigente durante la ejecución del contrato y hasta la liquidación de este.

Respecto a las personas naturales extranjeras sin domicilio en el país y las personas jurídicas privadas extranjeras que no tengan establecida sucursal en Colombia, no requieren inscripción en el Registro único de Proponentes.

**9. Certificado de existencia y representación legal o certificado de matrícula mercantil**

Las personas jurídicas deberán presentar el certificado de existencia y representación legal o el documento que haga sus veces, con fecha de expedición no mayor a 30 días calendario anteriores a la fecha límite de recepción de ofertas, donde conste que, de acuerdo con su objeto social, cuenta con la capacidad jurídica para celebrar y ejecutar contratos relacionados con el objeto de este proceso, acreditar que su duración no es inferior al término del plazo de ejecución del contrato y tres (3) años más.

Las personas jurídicas extranjeras sin sucursal o domicilio en Colombia, bien sea como interesados individuales o integrantes de consorcio, unión temporal, acreditaran su existencia y representación legal mediante el certificado equivalente al que expiden las Cámaras de Comercio colombianas, emitido por organismo o autoridad competente del país de origen de la persona jurídica extranjera con fecha de expedición no superior a treinta (30) días calendario antes de la fecha límite de recepción de ofertas.

Si el PROPONENTE es una persona natural comerciante, deberá presentar un Certificado de Inscripción en el Registro Mercantil expedido por la Cámara de Comercio en donde conste que su actividad se encuentra relacionada con el objeto de la presente convocatoria. Este certificado debe tener fecha de expedición no mayor a treinta (30) días calendario anteriores a la fecha límite de recepción de ofertas. En caso de personas naturales que no estén obligadas a inscribirse en el registro mercantil, como es el caso de las profesiones liberales, no deberán acreditar tal requisito.

Si la oferta se presenta a nombre de una Sucursal, se deberá anexar los Certificados, tanto de la Sucursal como de la Casa Principal.

Para el caso de las Universidades o cualquier otra entidad o empresa que no tengan la obligación de contar con el Certificado de Existencia o representación legal o certificado de matrícula mercantil, deberá aportar los estatutos o su equivalente o cualquier otro documento, donde conste que, de acuerdo con su objeto social, cuenta con la capacidad jurídica para celebrar y ejecutar contratos relacionados con el objeto de este proceso y acreditar que su duración

abarca como mínimo tres (3) años a partir de la fecha de terminación del plazo de ejecución del contrato que se suscriba.

Si del Certificado de Existencia y Representación Legal, de los Estatutos de Sociedad o del documento equivalente, se desprende que las facultades del representante legal están limitadas por razón de la naturaleza o cuantía del negocio jurídico, el oferente deberá presentar el acta respectiva en la cual se autoriza al representante legal para firmar la propuesta y celebrar el correspondiente contrato en caso de que le sea adjudicado, y para constituir el consorcio, la unión temporal si a ello hubiere lugar.

De igual manera ocurrirá si del Certificado de Existencia y Representación Legal, de los Estatutos de Sociedad o del documento equivalente, no se evidencian las facultades del representante legal, y las de sus suplentes en caso de que las ofertas son presentadas por estos.

El objeto social del interesado, persona jurídica o de cada uno de sus miembros en caso de consorcios o uniones temporales, debe estar relacionado con el objeto del presente proceso, objeto que se debe constatar en el Certificado de existencia y representación legal, los estatutos u otro documento idóneo según su actividad que acredite dicho objeto social.

Para el caso de Consorcios, Uniones Temporales, todos los miembros deberán aportar el certificado de existencia y representación legal en los términos anteriormente señalado.

**10. Consulta Antecedentes Fiscales de la Contraloría General de la República**

El DNP conforme el artículo 60 de la ley 610 de 2000, consultará y verificará, de la página web de la Contraloría General de la República, los antecedentes fiscales del proponente persona natural, o persona jurídica, de los representantes legales de los integrantes del proponente plural, que no se encuentren relacionados en el Boletín de Responsables Fiscales.

La certificación acorde con la Ley 962 de 2005 y la Circular 005 del 25 de febrero de 2008, debe estar suscrita por el Contralor General de la República.

En caso de que un PROPONENTE se encuentre relacionado en dicho boletín, se le hará la advertencia que debe acreditar la cancelación de las obligaciones contraídas o la vigencia de un acuerdo de pagos.

**11. Consulta de Antecedentes Disciplinarios de la Procuraduría General de la Nación.**

El DNP conforme la Ley 1238 de 2008, consultará y verificará, de la página web de la Procuraduría General de la Nación, los antecedentes disciplinarios del proponente, representante legal de la persona jurídica, de los representantes legales del proponente plural, que van a participar en el presente proceso, que no le inhabiliten o impidan presentar la propuesta y celebrar el contrato.

**12. Consulta de Antecedentes Judiciales.**

El DNP conforme el Decreto 019 de 2012, consultará en la página Web de Policía Nacional de Colombia los antecedentes judiciales del proponente persona natural, representante legal de la persona jurídica, de los representantes legales del proponente plural que van a participar en el presente proceso y verificará que no le inhabiliten o impidan presentar la propuesta y celebrar el contrato.

**13. Consulta del Sistema Registro Nacional de Medidas Correctivas.**

El DNP conforme al artículo 183 del Código Nacional de Policía, Ley 1801 de 2016, consultará y verificará, de la página Web de Policía Nacional de Colombia – Portal de Servicio al Ciudadano, el Sistema Registro Nacional de Medidas Correctivas, si existen multas en mora en los últimos seis (6) meses, impuestas a la persona natural, el representante legal de la persona jurídica, de los representantes legales del proponente plural que van a participar en el presente proceso, que no le inhabiliten o impidan presentar la propuesta y celebrar el contrato.

En caso de que un PROPONENTE se encuentre con multas en mora, se le hará la advertencia que debe acreditar la cancelación de las obligaciones contraídas o la vigencia de un acuerdo de pagos.

**14. Compromiso anticorrupción e Inhabilidades e Incompatibilidades. (Anexo 4)**

La propuesta debe estar acompañada del Anexo 4 – "Compromiso Anticorrupción e Inhabilidades e Incompatibilidades" firmado por el proponente o por el representante legal o apoderado, constituido en debida forma para el efecto, con la correspondiente prueba de ello, la cual debe ser diligenciada según el formato del pliego de condiciones.

**15. Registro Nacional de Deudores alimentarios morosos**

De conformidad con lo dispuesto en el numeral 1 del artículo 6 de la Ley 2097 de 20218, el representante legal de la persona jurídica proponente singular o integrante del proponente plural, no podrá encontrarse reportado en el registro de Deudores Alimentarios Morosos – REDAM -.

Para el efecto el proponente deberá:

**Persona natural**, anexar el certificado de la consulta de deudores alimentarios – REDAM -.
**Persona jurídica**, anexar el certificado de consulta de deudores alimentarios de su representante legal. – REDAM -.
**Para los proponentes plurales** deberá anexar certificado de consulta – REDAM -. de cada uno de los representantes que lo conforman.

Lo anterior, teniendo en cuenta que el Registro de Deudores Alimentarios Morosos – REDAM- es un mecanismo de control para garantizar el cumplimiento de las obligaciones alimentarias en todo el territorio nacional, y que una de sus

[8] **ARTÍCULO 6o. CONSECUENCIAS DE LA INSCRIPCIÓN EN EL REGISTRO DE DEUDORES ALIMENTARIOS MOROSOS.** La inscripción en el Registro de Deudores Alimentarios Morosos generará las siguientes consecuencias:1. El deudor alimentario moroso solo podrá contratar con el Estado una vez se ponga a paz y salvo con sus obligaciones alimentarias. Esta inhabilidad también se predica del deudor alimentario moroso que actúe como representante legal de la persona jurídica que aspira a contratar con el Estado.

consecuencias, es que impide o inhabilita a la persona para la celebración de contratos con el Estado, por lo que los proponentes deberán realizar la consulta del certificado de deudores alimentarios REDAM a través de la Carpeta Ciudadana Digital del Portal Único del Estado Colombiano.gov.co;

Link: https://carpetaciudadana.and.gov.co/

De acuerdo con la sentencia C-032 de 2021, la H. Corte Constitucional señaló las responsabilidades penales, disciplinarias y patrimoniales que se deben asumir en materia de manejo de la información del REDAM, así como las obligaciones establecidas en las Leyes 1581 de 2012 de protección de datos personales y 1266 de 2008 de habeas data, en consecuencia, el proponente al cargar el documento debe marcarlo como confidencial.

En caso de que no se marque como confidencial la entidad le dará el tratamiento establecido en las normas anteriores; es decir, en caso de que la certificación aportada registre alguna sanción por obligaciones alimentarias.

**16 verificación existencia de situaciones de control.**

Verificación existencia de situaciones de control. En aplicación a lo establecido en el Art. 2.1.4.3.2.1., del Decreto 1600 de 2024, en concordancia con lo dispuesto en los artículos 260 y 261 del código de comercio, las personas jurídicas oferentes y/o de los proponentes plurales, que se presenten como proponentes en éste proceso de selección, en el término máximo de Un (1) día después del momento en que se cierre definitivamente la presentación de ofertas, deberán poner de presente la existencia o no de situaciones de control de las personas jurídicas que participen y, en particular, si son controlantes, controladas o comparten alguna de estas condiciones con otras personas que se encuentren participando en éste mismo proceso de contratación. Para el caso de los proponentes plurales, deberán indicar si las personas jurídicas que los conforman se encuentran en alguna de las situaciones descritas anteriormente. En este sentido, los proponentes deberán allegar suscrito por el representante legal el anexo 15 DECLARACIÓN SITUACIONES DE CONTROL, en la cual se señale la existencia o no de las citadas situaciones.

### 5.1.2. REQUISITOS TÉCNICOS HABILITANTES (Capacidad Técnica)

Se entenderá con la suscripción de la carta de presentación de la Oferta que el proponente cumple con las condiciones señaladas en la FICHA TÉCNICA Y CONDICIONES EXIGIDAS.

#### 5.1.2.1. Documentos técnicos

Los documentos técnicos deben ser presentados en la propuesta inicial, sin tachaduras, ni enmendaduras, completamente diligenciados, con las especificaciones técnicas propuestas y firmados por el oferente o su representante legal, según el caso.

**a. CERTIFICACIÓN DE DISTRIBUIDOR Y/O COMERCIALIZADOR AUTORIZADO DEL SOFTWARE**

El oferente debe presentar certificado expedido por el fabricante Trellix, en donde especifique que el proveedor es un distribuidor autorizado GOLD con fecha de expedición no superior a sesenta (60) días calendarios anterior al cierre del presente proceso de selección.

Cuando se trate de un consorcio o una unión temporal, cualquiera de sus integrantes podrá presentar dicha certificación.

**b. CERTIFICACIONES**

El oferente deberá acreditar, como mínimo, una de las siguientes certificaciones

- El oferente deberá contar con certificación vigente del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022, expedida por un organismo de certificación acreditado. La certificación deberá estar vigente a la fecha de cierre del proceso y cubrir los servicios asociados a la solución ofertada

- El oferente deberá contar con certificación vigente del Sistema de Gestión de Servicios de TI conforme a la norma ISO/IEC 20000-1:2018, expedida por un organismo de certificación acreditado. La certificación deberá estar vigente a la fecha de cierre del proceso y cubrir la prestación y gestión de los servicios de tecnología de la información relacionados con la solución ofertada.

**c. AVAL DE LA PROPUESTA**

De conformidad con lo establecido en el Artículo 20 de la Ley 842 de 2003, el oferente deberá allegar su propuesta avalada por un ingeniero de sistemas, o electrónico, o de telecomunicaciones, o de software, junto con la matrícula y/o tarjeta profesional en la rama de la ingeniería, certificado de vigencia y antecedentes disciplinarios profesionales.

Para el caso de proponentes extranjeros, la propuesta deberá estar avalada por un ingeniero de sistemas o ingeniero electrónico o ingeniero de telecomunicaciones o ingeniero de software o su equivalente en el exterior, cuyo título esté debidamente convalidado en Colombia.

Por lo anterior, el ingeniero que avala la propuesta deberá suscribir la carta de presentación de la Oferta junto con el representante legal del proponente. En caso, de que el representante legal del proponente sea profesional en alguna de las ingenierías antes citadas, el requisito se entiende cumplido con la suscripción de la carta de presentación de la propuesta junto con la matrícula y/o tarjeta profesional en la respectiva rama de la ingeniería, certificado de vigencia y antecedentes disciplinarios profesionales.

### 5.1.2. Experiencia del Proponente Relacionada en el RUP

Para acreditar la experiencia conforme con lo establecido en el numeral 1° del Artículo 2.2.1.1.1.5.3 del Decreto 1082 de 2015, el proponente deberá acreditar en el **Registro Único de Proponentes** (RUP) **la ejecución de hasta dos (2) contratos** que cumplan los siguientes requisitos:

**a.** Los **contratos acreditados deben estar identificados con alguno de los códigos** del **clasificador de bienes y servicios** de Naciones Unidas a nivel de clase señalados en el siguiente cuadro:

**Clasificación UNSPSC**

| CLASIFICACIÓN UNSPSC | SEGMENTO | FAMILIA | CLASE |
|---|---|---|---|
| 43232700 | Difusión de Tecnologías de Información y Telecomunicaciones | Software | Software de aplicaciones de red |

| | | | |
|---|---|---|---|
| 43232800 | Difusión de Tecnologías de Información y Telecomunicaciones | Software | Software de administración de redes |
| 43233200 | Difusión de Tecnologías de Información y Telecomunicaciones | Software | Software de seguridad y protección |
| 81111600 | Servicios Basados en Ingeniería, Investigación y Tecnología | Servicios informáticos | Programadores de computador |
| 81112200 | Servicios Basados en Ingeniería, Investigación y Tecnología | Servicios informáticos | Mantenimiento y soporte de software |

**b. Valor:** La sumatoria del valor de los contratos deberá ser igual o superior al 100% del presupuesto oficial equivalente a 513,46 SMMLV.

**c. Contratante**: entidades públicas, o mixtas, u organismos multilaterales, o privados totalmente.

**d. Estado de los contratos:** Totalmente ejecutados a la fecha del cierre del proceso de selección y desarrollados en los últimos cinco (5) años[9] (contados hacia atrás a partir de la fecha de apertura del presente proceso de contratación).

***e.* Certificación:** Como quiera que en el RUP no figura toda la información suficiente para acreditar la experiencia, los proponentes deben adjuntar el certificado de experiencia o acta de liquidación o documento equivalente a esta acta[8], cuyo objeto u obligaciones o actividades estén relacionado con la: "*Adquisición y/o renovación de soluciones de ciberseguridad, y al menos un contrato debe cumplir con alguno de los siguientes ítems:*
● *Adquisición o renovación de licenciamiento/servicios de DLP.*
● *Adquisición o renovación de licenciamiento/servicios de EDR., de acuerdo con el objeto de contrato[10]., lo cual será verificado en dicha certificación."*

De la citada certificación o acta de liquidación o documento equivalente se debe evidenciar como mínimo la siguiente información:

i. Nombre o razón social del contratante.
ii. Nombre o razón social del contratista.
iii. Objeto y/u obligaciones y/o actividades y/o funciones del contrato identificado.
iv. Valor del contrato, incluidos los adicionales o modificaciones, si los hubiere.
v. Plazo de ejecución del contrato y/o fecha de inicio y de terminación del contrato (dd/mm/aaaa)
vi. En caso de certificación deberá contener el nombre, cargo, firma y teléfono de contacto de quien expide la certificación.
vii. El certificado de experiencia o acta de liquidación o documento equivalente a esta acta con la que se pretenda acreditar el requisito deberá estar suscrito por la persona competente.

[9] Se requiere que la experiencia acreditada sea de los últimos cinco (5) años, en virtud de los avances, cambios tecnológicos y buenas prácticas de TIC, que en materia del objeto contractual se producen día a día, de tal forma que se garantice que el adjudicatario tenga la experiencia óptima para el desarrollo del contrato. Una experiencia mínima de cinco (5) años permite evidenciar que el proveedor ha gestionado múltiples ciclos operativos, actualizaciones tecnológicas, incidentes de seguridad y cambios en los entornos de TI, reduciendo el riesgo de implementación y operación de una solución crítica para la organización.
10 las certificaciones requeridas deben contemplar actividades de implementación, administración o soporte de soluciones EDR o DLP que tiene la Entidad actualmente

**Nota 1:** La clasificación de la experiencia con alguno de los códigos del clasificador de bienes y servicios de Naciones Unidas a nivel de clase y el valor de los contratos requeridos se verificará únicamente en el RUP.

**Nota 2**: Para verificar este requisito, el proponente deberá indicar mediante un anexo incluido en los soportes de la propuesta cuál de los contratos certificados en el Registro Único de Proponentes (RUP) debe considerar la entidad para habilitarlo. El no diligenciamiento del formato no es causal de rechazo de la oferta.

**5.1.2.1. Criterios Diferenciales de Experiencia del Proponente Relacionada en el RUP**

Con el fin de acogerse a la experiencia habilitante establecida como criterios diferenciales, los proponentes interesados deben manifestarlo expresamente en el Anexo 2 – Carta de Presentación de la Oferta-, señalando si se constituyen como Mipymes domiciliadas en Colombia o emprendimientos y empresas de personas con discapacidad.

Teniendo en cuenta lo analizado en el estudio del sector, y de acuerdo con lo consagrado en el Decreto No. 1860 de 2021 el cual promueve y facilita la participación en los procedimientos de selección competitivos de las Mipyme domiciliadas en Colombia, así como con lo establecido en el artículo 2.2.1.2.4.2.7.3 del Decreto No. 287 del 19 de marzo de 2026 el cual establece requisitos habilitantes diferenciales, proporcionales al objeto contractual, que faciliten la participación de empresas de personas con discapacidad en los procesos de contratación, estos actores podrán cumplir con la experiencia habilitante a través de la acreditación de **hasta 3 contratos** que cumplan con las condiciones antes señaladas, cuya sumatoria sea igual o superior al 100% del presupuesto oficial, expresado en salarios mínimos legales mensuales vigentes.

De igual manera deberá cumplir con los requisitos de presentación de las certificaciones señaladas en los numerales anteriores.

En primera medida, el proponente que pretenda acreditar experiencia como Mipyme deberá adjuntar los documentos que evidencien que se encuentra en dicha situación, de acuerdo con la definición establecida en el Artículo 2.2.1.2.4.2.4 del Decreto 1082 de 2015, así:

i. Las personas naturales mediante certificación expedida por ellos y un contador público, adjuntando copia del registro mercantil.
ii. Las personas jurídicas mediante certificación expedida por el representante legal y el contador o revisor fiscal, si están obligados a tenerlo, adjuntando copia del certificado de existencia y representación legal expedido por la Cámara de Comercio o por la autoridad competente para expedir dicha certificación.
iii. Las Mipyme también podrán acreditar esta condición con la copia del certificado del Registro Único de Proponentes, el cual deberá encontrarse vigente y en firme al momento de su presentación.

Los documentos antes señalados deberán haber sido expedidos conforme las exigencias establecidas en los requisitos jurídicos habilitantes.

Para la acreditación se tendrán en cuenta los rangos de clasificación empresarial establecidos de conformidad con la Ley 590 de 2000 y el Decreto 1074 de 2015, o las normas que lo modifiquen, sustituyan o complementen.

De conformidad con lo establecido por los artículos 4o de la Ley 79 de 1988 y 6o de la Ley 454 de 1998 de la Ley 2069 de 2020, las cooperativas y demás entidades de la economía solidarla son empresas, por lo tanto, las entidades de economía solidaria serán clasificadas como Mipymes en los términos establecidos por el artículo 2o de la Ley 590 de 2000 y por el Decreto 957 de 2019.

De la misma forma las asociaciones conformadas por sujetos de especial protección constitucional, asociaciones de pequeños productores locales y productores locales agropecuarios cuyos sistemas productivos pertenezcan a la agricultura campesina, familiar y comunitaria, podrán ser clasificados como Mipymes en los términos previstos en el art 23 de la ley 2069 de 2020, el art 2 de Ley 590 de 2000 y el Decreto 957 de 20219 y 143 de 2023 o las normas que los modifiquen

En segunda medida, el proponente que pretenda acreditar experiencia como EMPRENDIMIENTOS Y EMPRESAS DE PERSONAS CON DISCAPACIDAD, en concordancia con lo dispuesto en el artículo 2.2.1.2.4.2.7 del Decreto 287 del 19 de marzo de 2026 y siguientes y en el marco de las Leyes 361 de 1997 y 1618 de 2013 deberá adjuntar los documentos que evidencien que se encuentra en dicha situación, así:

1) Personas naturales con discapacidad que ejerzan una profesión liberal. Esta circunstancia se acreditará mediante la copia de cedula de ciudadanía, la cedula de extranjería o el pasaporte, el certificado de discapacidad expedido de acuerdo con la normativa del Ministerio de Salud y Protección Social, así coma el título profesional correspondiente.

2) Personas naturales con discapacidad que hayan realizado actividades comerciales a través de un establecimiento de comercio, durante al menos el último año anterior a la fecha de cierre del proceso de selección. Esta circunstancia se acreditará mediante la copia de cedula de ciudadanía, la cedula de extranjera o el pasaporte, el certificado de discapacidad expedido de acuerdo con la normativa del Ministerio de Salud y Protección Social, así coma la copia del registro mercantil.

3) Personas jurídicas donde más del cincuenta por ciento (50%) de sus acciones, partes de interés o cuotas de participación pertenezcan a personas con discapacidad y los derechos de propiedad hayan pertenecido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección.

La circunstancia de la propiedad de la persona jurídica se acreditará mediante certificación expedida por el representante legal y el revisor fiscal, cuando exista, de acuerdo con los requerimientos de ley o, el contador, donde conste la distribución de los derechos en la sociedad y el tiempo en el que las personas con discapacidad han mantenido su participación. Adicionalmente se debe adjuntar la copia de cedula de ciudadanía, la cedula de extranjera o el pasaporte, el certificado de discapacidad expedido de acuerdo con la normativa del Ministerio de Salud y Protección Social, así como la copia del certificado de existencia y representación legal.

4) Personas jurídicas que tengan vinculadas laboralmente al menos una persona con discapacidad en empleos del nivel directivo de la empresa durante al menos el último año anterior a la fecha de cierre del Proceso de Selección en el mismo cargo u otro del mismo nivel.

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

Esta circunstancia se acreditará mediante certificación expedida por el representante legal y el revisor fiscal, cuando exista de acuerdo con los requerimientos de ley, o el contador, donde se señale de manera detallada las personas con discapacidad que ocupan cargos de nivel directivo del proponente y el tiempo de vinculación.

La certificación deberá relacionar el nombre completo y el número de documento de identidad de las personas con discapacidad que ocupan cargos de nivel directivo del proponente. Como soporte, se anexará copia de los respectivos

documentos de identidad, copia de los contratos de trabajo o certificación laboral con las funciones, así como el certificado de aportes a seguridad social del último año en el que se demuestren los pagos realizados por el empleador, y el certificado de discapacidad expedido de acuerdo con la normativa del Ministerio de Salud y Protección Social

**Nota**. Respecto de los incentivos contractuales para los emprendimientos y empresas de personas con discapacidad, las certificaciones de que trata los anteriores numerales deben expedirse bajo la gravedad de juramento con una fecha de máxima treinta (30) días calendario anteriores a la prevista para el cierre del procedimiento de selección.

**5.1.2.2. Personas Naturales, Extranjeras Sin Domicilio en el País y las Personas Jurídicas Extranjeras que no Tengan Establecida Sucursal en Colombia.**

En virtud a que las Personas naturales, extranjeras sin domicilio en el país y las personas jurídicas extranjeras que no tengan establecida sucursal en Colombia, no están obligadas a tener RUP, acreditarán el cumplimiento de este requisito únicamente mediante la presentación de **hasta dos (2) certificaciones** de experiencia y/o copias de contratos con sus respectivas actas de liquidación, de contratos ejecutados y desarrollados en los últimos cinco (5) años (contados hacia atrás a partir de la fecha de apertura del presente proceso de contratación), asociados con la: *Adquisición y/o renovación de soluciones de ciberseguridad, y al menos un contrato debe cumplir con alguno de los siguientes ítems:*

- *Adquisición o renovación de licenciamiento/servicios de DLP.*
- *Adquisición o renovación de licenciamiento/servicios de EDR., de acuerdo con el objeto de contrato*[11]*., lo cual será verificado en dicha certificación.* La suma de los contratos aportados deberá ser igual o superior al presupuesto oficial.

Para certificar experiencia de contratos ejecutados en moneda diferente al peso colombiano, se dará cumplimiento a lo dispuesto en el artículo 874 del Código de Comercio, el valor en pesos colombianos del contrato o contratos celebrados en moneda distinta será el de la fecha de su suscripción o firma, de acuerdo con la tasa de cambio oficial que indique el Banco de la República. Este soporte deberá ser adjuntado a la oferta por el proponente y podrá ser validado por la entidad"

En caso de que la fecha de suscripción del contrato aportado sea anterior a los rangos establecidos en el enlace, el proponente deberá aportar certificación de la tasa de cambio vigente para esa fecha, expedida directamente por el Banco de la República de Colombia.

El oferente extranjero deberá relacionar y certificar la experiencia exigida en este proceso. Para certificarla deberá adjuntar la certificación respectiva que deberá cumplir con los requisitos establecidos en este documento.

**Nota**: Se entiende que el cálculo de los valores de los contratos expresados en salarios SMMLV para acreditar la experiencia, será tomado del salario fijado por el Ministerio del Trabajo y de Hacienda y Crédito Público para la vigencia de la fecha de terminación del contrato.

**5.1.2.3. Reglas Generales de la Experiencia**

a. Para la verificación de este requisito, el proponente con su oferta deberá indicar en el Anexo: **Formato para la presentación de la experiencia habilitante del proponente** en formato Excel (*.xls o * xlsx), cuál contrato o contratos certificados en el Registro Único de Proponentes (RUP) debe ser tenido en cuenta por la entidad. En caso de que el proponente no precise tal información, el DNP podrá tomar el primer contrato o contratos registrados en el

[11] las certificaciones requeridas deben contemplar actividades de implementación, administración o soporte de soluciones EDR o DLP que tiene la Entidad actualmente

RUP en orden consecutivo ascendente, que cumplan las condiciones establecidas en la sección EXPERIENCIA DEL PROPONENTE RELACIONADA EN EL RUP y CRITERIOS DIFERENCIALES DE EXPERIENCIA DEL PROPONENTE RELACIONADA EN EL RUP, con el propósito de habilitar al proponente.

b. En caso de que el proponente no esté obligado a estar inscrito en el RUP, deberá adjuntar el Anexo: Formato para la presentación de la experiencia habilitante del proponente en formato Excel (*.xls o * xlsx), **según sea el caso**. La experiencia relacionada en el Anexo debe corresponder a las certificaciones de experiencia o actas de liquidación de contratos aportadas para acreditar la experiencia. En caso de diligenciarse en este anexo experiencia diferente a la contenida en las certificaciones aportadas, esta no será tenida en cuenta y en todo caso prevalecerán las certificaciones que se anexen a la propuesta. Para la acreditación de experiencia de habilitante dicha experiencia deberá estar relacionada el objeto de este proceso.

c. De acuerdo con el numeral 2.5, del numeral 2 del artículo 2.2.1.1.1.5.2 del Decreto 1082 de 2015, las personas jurídicas, con menos de tres (3) años de constituidas, podrán acreditar su experiencia con base en la de sus socios o accionistas, asociados o constituyente.

   Si la persona jurídica con menos de tres años de constituida registra la experiencia de sus socios en el RUP, y éste es renovado, puede continuar utilizando la experiencia inscrita mientras no cesen los efectos del RUP. Por el contrario, si no se renueva y la persona jurídica supera los tres años de constituida, la experiencia que registró de sus socios no puede ser inscrita nuevamente, puesto que el RUP ha cesado sus efectos.

d. No podrán acumularse a la vez, la experiencia de los socios y la de la persona jurídica cuando estos se asocien entre sí para presentar propuesta bajo alguna de las modalidades previstas en el artículo 7 de la Ley 80 de 1993.

e. En caso de que no coincida el valor del contrato ejecutado expresado en SMMLV en el RUP con el valor de la certificación aportada por el oferente para acreditar la experiencia, prevalecerá la información contenida en el RUP.

f. Si la certificación incluye el contrato principal con sus adicciones, prórrogas y Otrosí, se entenderá como un solo contrato certificado, lo cual es válido.

g. Si la documentación con la que se pretende acreditar la experiencia requerida no es aportada, o está incompleta, será requerida por la entidad para subsanar el requisito habilitante.

h. Toda la información que se acredite en el RUP, para cumplir con el requisito exigido, el DNP dará aplicación a lo dispuesto en el artículo 5 de la Ley 1882 de 2018, que adiciono el parágrafo 4 al artículo 5 de la Ley 1150 de 2007; esto es, hasta antes del inicio del evento de subasta.

i. No se aceptan certificaciones acumulativas de varios contratos que, individualmente consideradas, no cumplan con los requisitos aquí exigidos, salvo lo previsto en el numeral “Criterios Diferenciales de Experiencia del Proponente Relacionada en el RUP”.

j. En caso de que alguna información referente a la acreditación de experiencia provenga de un país extranjero el proponente deberá aportar el documento o documentos equivalentes, con el cumplimiento de los requisitos dispuesto en este numeral, de los cuales se pueda obtener la información requerida antes de la fecha prevista para el cierre del proceso.

k. En el evento en que la certificación de experiencia o acta de liquidación no contenga toda la información requerida, se podrá aportar además la copia del contrato en el momento de presentar la oferta, con el fin de completar la información solicitada.

l. No se aceptan auto certificaciones ni certificaciones expedidas por el mismo proponente o los otros miembros de consorcios o uniones temporales.

m. La Entidad se reserva el derecho de verificar y solicitar durante la evaluación y hasta la adjudicación, la información y soportes que considere necesarios para verificar la información presentada.

n. Cuando el proponente pretenda acreditar la experiencia con certificaciones de contratos que reposan en la entidad, deberá mediante un oficio firmado por el Representante Legal, relacionar la siguiente información:

- Número del proceso en el cual se aportó la certificación.
- Número de contrato.
- Nombre exacto del contratista, consorcio o unión temporal.
- Objeto del contrato.
- Estado del contrato.
- Fecha de suscripción y terminación (día, mes, año).

**5.2.2.4. Reglas aplicables a la experiencia habilitante del proponente plural (CONSORCIO, UNIÓN TEMPORAL):**

1. Cuando los contratos con los cuales se pretenda acreditar esta experiencia sean ejecutados bajo la modalidad de proponente plural, se deberá especificar el porcentaje (%) de participación de cada uno de los miembros, o anexar copia del contrato en el que se mencione el porcentaje de participación y únicamente será tenido en cuenta el valor del contrato en forma proporcional a su porcentaje de participación.
2. En caso de proponente plural, esta experiencia deberá ser acreditada por todos de los integrantes del Consorcio o Unión Temporal, acorde a su porcentaje de participación.
3. Tratándose de proponentes plurales, los criterios diferenciales solo se aplicarán si por lo menos uno de los integrantes acredita la calidad de Mipyme o Emprendimientos y Empresas de persona con discapacidad, si es del caso, y tiene una participación igual o superior al diez por ciento (10%) en el consorcio o la unión temporal, aportando la experiencia requerida, como mínimo, en una proporción equivalente a su participación en la conformación del proponente plural.

**5.2.2.5 VERIFICACIÓN DE CUMPLIMIENTO DE LOS REQUERIMIENTOS Y ESPECIFICACIONES MÍNIMAS (FICHA TÉCNICA**

Con la suscripción de la carta de presentación de la oferta (Anexo), se entienden conocidas y aceptadas todas y cada una de las especificaciones técnicas contenidas en el Anexo Técnico de este documento.

Los documentos técnicos deben ser presentados en la propuesta inicial, sin tachaduras, ni enmendaduras, completamente diligenciados, con las especificaciones técnicas propuestas y firmados por el oferente o su representante legal, según el caso.

### 5.1.3. CAPACIDAD FINANCIERA Y ORGANIZACIONAL

**REQUISITOS DE CAPACIDAD FINANCIERA HABILITANTES**

En cumplimiento del artículo 2.2.1.1.1.5.3. numeral 3º del Decreto 1082 de 2015, la Capacidad Financiera y Organizacional de los proponentes se acredita mediante el RUP vigente y firme al finalizar el traslado del informe de evaluación el cual deberá ser presentado por los oferentes, lo anterior teniendo en cuenta que esta información ha sido objeto de verificación documental por parte de la Cámara de Comercio.

En el componente financiero de las empresas que están dispuestas a ofertar, es importante tener en cuenta indicadores para verificar la capacidad financiera y organizacional con fecha de corte de los estados financieros al 31 de diciembre de 2025 en este sentido, a continuación, se definen los más útiles para obtener información pertinente tomando como base las recomendaciones del Decreto 1082 de 2015 y la Guía para la Elaboración del Estudios del Sector de Colombia Compra Eficiente.

NOTA 1: Las personas jurídicas extranjeras con sucursal en Colombia deberán acreditar las condiciones financieras a través del RUP.

NOTA 2: Para acreditar la capacidad financiera y la capacidad organizacional de las personas jurídicas extranjeras sin sucursal en Colombia, se utilizará certificados suscritos por el representante legal y el revisor fiscal o auditor del proponente, y si el proponente no está obligado a tener revisor fiscal, será por su contador, y deberá estar acompañado de los estados financieros auditados de corte anual más reciente, así mismo deberá incluir en los Documentos del Proceso la siguiente información relevante para la presentación de ofertas por parte de proponentes extranjeros:

Fecha de corte de los Estados Financieros: Los oferentes extranjeros deben presentar sus estados financieros a la fecha de corte establecida en los países de origen o en sus estatutos sociales.

Moneda: Los oferentes deben presentar sus estados financieros en la moneda legal del país en el cual fueron emitidos y adicionalmente en pesos colombianos. El proponente y la Entidad Estatal para efectos de acreditar y verificar los requisitos habilitantes tendrán en cuenta la tasa representativa del mercado vigente en la fecha en la cual los estados financieros fueron expedidos. Para el efecto, el proponente y la Entidad Estatal tendrán en cuenta las tasas de cambio certificadas por la Superintendencia Financiera.

NOTA 3: Debido a que hay indicadores que resultan de realizar divisiones entre valores, cuando el denominador es cero, será válido para la administración y por lo tanto será habilitado, asignándole el puntaje mínimo exigido.

El Departamento Nacional de Planeación advierte que la información financiera acreditada se realiza con los efectos previstos en el artículo 43 de la Ley 222 de 1995, que al tenor reza:

(…) Responsabilidad penal. Sin perjuicio de lo dispuesto en otras normas, serán sancionados con prisión de uno a seis años, quienes a sabiendas:

2. Suministren datos a las autoridades o expidan constancias o certificaciones contrarias a la realidad.
3. Ordenen, toleren, hagan o encubran falsedades en los estados financieros o en sus notas (…).

La Entidad se reserva el derecho de solicitar de manera adicional los documentos de carácter financiero que requiera para realizar la constatación de la información consignada en el RUP, la cual deberá ajustarse a las Normas de Contabilidad Generalmente Aceptadas en Colombia.

#### 5.1.3.1. CAPACIDAD FINANCIERA

**ÍNDICE DE LIQUIDEZ**

Índice de Liquidez= Activo Corriente/Pasivo Corriente

**Liquidez:** Deberá ser mayor o igual a **UNO PUNTO TRES VECES (≥ 1.3 VECES)**

**Condición**: Sí el índice de liquidez es Mayor o igual que 1.3 veces la propuesta se calificará HABILITADA.

Para el caso del Índice de Liquidez, y de acuerdo con lo señalado en el Manual para determinar y verificar los requisitos habilitantes en los Procesos de Contratación expedido por Colombia Compra Eficiente, en el caso de consorcios y/o Uniones Temporales el cálculo se realizará tomando la suma del Activo corriente de cada uno de los integrantes sobre la suma del Pasivo corriente de cada uno de los integrantes, de acuerdo con la siguiente fórmula:

$$\text{(iii) Indicador}=\frac{(\sum_{i=1}^{n}\text{Componente 1 del indicador}_i)}{(\sum_{i=1}^{n}\text{Componente 2 del indicador}_i)}$$

**ÍNDICE DE ENDEUDAMIENTO**

Índice de Endeudamiento= Pasivo Total/Activo Total

**Endeudamiento:** Deberá ser menor o igual que SESENTA Y SIETE POR CIENTO (≤ 67%)

**Condición:** Sí el índice de endeudamiento es Menor o igual que 67% la propuesta se calificará HABILITADA.

Para el caso del Índice de Endeudamiento, y de acuerdo con lo señalado en el Manual para determinar y verificar los requisitos habilitantes en los Procesos de Contratación expedido por Colombia compra Eficiente, en el caso de consorcios y/o Uniones Temporales el cálculo se realizará tomando la suma del Pasivo Total de cada uno de los integrantes sobre la suma del Activo Total de cada uno de los integrantes, de acuerdo con la siguiente fórmula:

$$\text{(iii) Indicador}=\frac{(\sum_{i=1}^{n}\text{Componente 1 del indicador}_i)}{(\sum_{i=1}^{n}\text{Componente 2 del indicador}_i)}$$

**RAZÓN DE COBERTURA DE INTERESES**

Razón de Cobertura de Intereses = Utilidad Operacional/Gastos de Intereses

**Cobertura de Intereses**: Deberá ser mayor o igual que **UNA VEZ (≥ 1 VECES)**

**Condición**: Sí el índice de Cobertura de Intereses es Mayor o igual que **≥ 1** la propuesta se calificará HABILITADA

Para los consorcios y uniones temporales, el cálculo se realizará tomando la suma de la Utilidad Operacional de cada uno de los integrantes sobre la suma de los Gastos de Intereses de cada uno de los integrantes.

En el caso que el indicador "Razón de Cobertura de Intereses", arroje como resultado "indeterminado", será válido para la entidad y el proponente será habilitado, siempre y cuando la cuenta "gastos de intereses" sea valor cero (0).

Para el caso de consorcios y uniones temporales, el indicador "Razón de Cobertura de Intereses" cuando arroje como resultado "indeterminado" para algún miembro del consorcio o unión temporal, se realizará el cálculo a los demás integrantes de la estructura plural y sí cumplen con la condición establecida, será válido para la entidad y por lo tanto serán habilitados, asignándoles el mínimo exigido de (1) veces.

De conformidad con el Manual para determinar y verificar los requisitos habilitantes en los Procesos de Contratación expedido por Colombia Compra Eficiente, LA FORMULA que se tendrá en cuenta será la siguiente:

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

En los casos en que las empresas a presentarse estén constituidas como Empresas sin ánimo de lucro - ESAL o Universidades Públicas, para la verificación de la razón cobertura de intereses, se entenderá que cumple independiente de su resultado.

#### 5.1.3.2. CAPACIDAD ORGANIZACIONAL

En cumplimiento del artículo 2.2.1.1.1.5.3. del Decreto 1082 de 2015, la Capacidad Organizacional de los proponentes se acredita mediante el RUP vigente y en firme que deberá ser presentado por los oferentes. El DNP verificará el cumplimiento de los siguientes indicadores financieros a título de requisito habilitante.

En los casos en que las empresas a presentarse estén constituidas como Empresas sin ánimo de lucro - ESAL o Universidades Públicas, para la verificación de la capacidad organizacional independientemente de su resultado, se entenderá que cumple con la Capacidad Organizacional.

Para los casos en que los Consorcios o Uniones Temporales estén integrados por Empresas con Ánimo de Lucro y Empresas sin Ánimo de Lucro – ESAL o Universidades Públicas, independientemente del número de integrantes, se tendrán en cuenta para la verificación de la capacidad organizacional los resultados individuales de los integrantes; es decir, se evaluarán únicamente los integrantes de la estructura plural constituidos como empresas con ánimo de lucro y deberán cumplir con los criterios de capacidad organizacional establecidos en el pliego de condiciones.

**A. RENTABILIDAD DEL PATRIMONIO**

$$\text{Rentabilidad sobre patrimonio} = \text{Utilidad Operacional} / \text{Patrimonio}$$

**Rentabilidad del patrimonio**: Deberá ser mayor o igual que **CERO PUNTO CERO CUATRO (≥ 0.04)**

**Condición:** Sí el índice de Rentabilidad del Patrimonio es Mayor o igual que **0.04** la propuesta se calificará HABILITADA.

Para el caso del Índice rentabilidad de patrimonio, y de acuerdo con lo sugerido en el Manual expedido por la Agencia Nacional de Colombia compra Eficiente, en el caso de consorcios y/o Uniones Temporales el cálculo se realizará tomando la suma de la Utilidad Operacional de cada uno de los integrantes sobre la suma del Patrimonio de cada uno de los integrantes, de acuerdo con la siguiente fórmula:

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

**B. RENTABILIDAD DEL ACTIVO**

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

**Rentabilidad del Activo:** Deberá ser mayor o igual que **CERO PUNTO CERO TRES (≥ 0.03)**

**Condición:** Sí el índice de Rentabilidad del Activo es Mayor o igual que **0.03** la propuesta se calificará HABILITADA

Para el caso del Índice de rentabilidad del activo, y de acuerdo con lo sugerido en el Manual expedido por la Agencia Nacional de Colombia compra Eficiente, en el caso de consorcios y/o Uniones Temporales el cálculo se realizará tomando la suma de la Utilidad Operacional de cada uno de los integrantes sobre la suma del Activo Total de cada uno de los integrantes, de acuerdo con la siguiente fórmula:

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

Se considera que el oferente cumple con la Capacidad Financiera y Capacidad Organizacional solicitada y que está habilitado para continuar en el proceso, si obtiene en cada indicador los márgenes anteriormente establecidos

**MÁRGENES ESTABLECIDOS PARA CADA INDICADOR FINANCIERO**

| ÍNDICE | FORMULA | VALORES ACEPTABLES |
|---|---|---|
| Índice de Liquidez | Activo Corrientes / Pasivo Corrientes | ≥ 1.3 Veces |
| Índice de endeudamiento | Pasivo Total / Activo Total | ≤ 67 % |
| Razón de cobertura de intereses | Utilidad Operacional / Gastos de Intereses | ≥ 1 Veces o indeterminado |
| Rentabilidad del Patrimonio | Utilidad Operacional / Patrimonio | ≥ 0.04 |
| Rentabilidad del active | Utilidad Operacional/ Activo | ≥ 0.03 |

En caso de que la propuesta no cumpla con alguno de los indicadores anteriormente mencionados, será calificada como NO HABILITADO.

La exigencia de los anteriores requisitos tiene la finalidad de garantizar que el proponente adjudicatario tenga la capacidad financiera, experticia y respaldo necesario para el cumplimento adecuado de cada una de las obligaciones surgidas del contrato que se llegue a celebrar, y se ajustan a la naturaleza y cuantía del negocio jurídico resultante del presente proceso

## 6. CRITERIOS DE EVALUACIÓN.

El cumplimiento de los requisitos mínimos que acreditan su capacidad jurídica, financiera, técnica, las condiciones de experiencia, capacidad de organización y condiciones técnicas mínimas aquí previstas, tiene por objeto establecer si las propuestas cumplen con las condiciones exigidas, solo se establecerá que estarán habilitados para participar de la subasta inversa.

Teniendo en cuenta que los bienes y servicios que se pretenden adquirir son de características técnicas uniformes y de común utilización, conforme a lo expresado en el numeral 3 del artículo 5 de la Ley 1150 de 2007, en concordancia con el artículo 2.2.1.2.1.2.2 del Decreto 1082 de 2015 modificado por el artículo 6 del Decreto 1860 de 2021, el ofrecimiento más favorable corresponderá a aquel proponente que ofrezca el MENOR PRECIO por la totalidad de los bienes y/o servicios requeridos.

Los errores u omisiones en la estimación del valor no darán lugar a modificaciones posteriores del precio ofrecido, el proponente deberá asumir los costos adicionales que su omisión o error le ocasione para cumplir con su ofrecimiento.

El proponente deberá presentar en el espacio establecido para tal fin en la Plataforma SECOP II, su oferta económica en pesos colombianos. Esta oferta será abierta antes del evento de subasta inversa electrónica de acuerdo con el cronograma.

### 6.1. Oferta Económica

El proponente deberá presentar su oferta económica en pesos colombianos diligenciando únicamente la información en la plataforma de SECOP II. Esta oferta será desencriptada en la plataforma de SECOP II el día programado para el evento de subasta.

En consideración a que el sobre económico será abierto hasta el día programado para el evento de subasta se reitera al proponente que en el sobre económico del SECOP II no deberá incluirse información diferente o correspondiente a los factores habilitantes, ya que esta no podrá ser evaluada y por tanto no se tendrá en cuenta.

Serán de cuenta del CONTRATISTA todos los gastos como derechos e impuestos que se causen con ocasión de la legalización del contrato, y que se requieran cancelar para dar cumplimiento a las disposiciones legales vigentes sobre el particular.

Se entiende que en el valor total de la oferta quedan incluidos todos los gastos que deberá hacer el contratista como: administración, salarios, prestaciones sociales, dotación del personal a su cargo, equipos, medios de transporte para el personal, todos los impuestos, tasas, contribuciones, gastos, administración, imprevistos y utilidades a que haya lugar, y en general todo cuanto sea necesario y conveniente para dar cumplimiento al objeto del presente proceso y la totalidad de las actividades y productos descritos en el Anexo Técnico.

Así mismo, será de exclusiva responsabilidad del oferente los errores u omisiones en que incurra al indicar el valor de su propuesta económica inicial y de los ofrecimientos que lleve a cabo dentro de la subasta inversa electrónica,

debiendo asumir los mayores costos y/o pérdidas que se deriven de dichos errores u omisiones, sin que por esta razón haya lugar a alegar ruptura del equilibrio contractual.

El oferente al momento de determinar el valor de su propuesta deberá tener en cuenta que asumirá el riesgo cambiario y los posibles incrementos que puedan presentar los costos directos e indirectos para el cumplimiento del contrato.

El valor por ofertar será el que el proponente estime conveniente, de acuerdo con sus condiciones económicas, financieras y organizacionales.

**Nota 1:** El valor total ofertado, no podrá superar el PRESUPUESTO OFICIAL asignado, (so pena de rechazo de esta).

**Nota 2:** Los valores ofertados no deben utilizar centavos; por lo tanto, el valor total de la propuesta económica y el valor de los impuestos a que hubiere lugar, deben presentarse en números enteros, es decir, el proponente deberá aproximar al peso, ya sea por exceso, si la suma es mayor a 0.50, o por defecto, si la suma es menor o igual a 0.49, en todo caso los valores ofertados deberán ser consignados en la plataforma SECOP II, formulario “oferta económica”.

**Nota 3:** Se entiende que en el valor total de la oferta se encuentran incluidos todos los tributos y gastos en que incurra el contratista para dar cumplimiento al objeto del presente proceso.

**Nota 4:** Igualmente, al momento de determinar el valor de su propuesta, tenga en cuenta que asumirá el riesgo cambiario y los posibles incrementos que puedan presentar los costos directos e indirectos para el cumplimiento del contrato, por ello el plazo de validez de su oferta debe ser igual o superior a noventa (90) días

## 7. DESARROLLO DE LA SUBASTA

### 7.1. PROCEDIMIENTO PARA EFECTUAR LOS LANCES – MARGEN MÍNIMO DE MEJORA

Para efectos de la Subasta Inversa se seguirá el procedimiento previsto en los artículos 2.2.1.2.1.2.2 y siguientes del Decreto 1082 de 2015 y los requeridos por la plataforma SECOP II., la cual consiste en una puja dinámica efectuada en la plataforma, mediante la reducción uniforme y sucesiva de precios.

Hay subasta inversa siempre que haya como mínimo dos (2) oferentes habilitados cuyos bienes o servicios cumplan con la ficha técnica, es decir que estén habilitados, los cuales deberán participar obligatoriamente en el evento, a través de la cuenta del oferente en la plataforma SECOP II, para efectuar lances, por lo que se entenderá que, si un oferente admitido para participar en la subasta ingresa, podrá presentar lances y se entenderán realizados por el oferente.

Si en el proceso de contratación se presenta un único oferente cuyos bienes o servicios cumplen con la ficha técnica y está habilitado, la entidad estatal puede adjudicar el contrato al único oferente si el valor de la oferta es igual o inferior a la disponibilidad presupuestal para el contrato, caso en el cual no hay lugar a la subasta inversa.

A partir de la apertura del sobre económico electrónico NO se reciben más documentos de subsanación. La Entidad revisará las debidas subsanaciones allegadas, previo a la instalación del evento de subasta electrónica, así como las observaciones allegadas con posterioridad a la publicación del informe final y tras su análisis, en el evento en que

proceda algún ajuste de dicho informe, lo pondrá en conocimiento de los oferentes (vía mensaje en la plataforma del SECOP II). Posteriormente procederá a crear la subasta electrónica.

**SUBASTA ELECTRÓNICA: CORRESPONDE A LA PUJA EN EL CURSO DEL EVENTO ELECTRÓNICO.**

Se dará apertura al evento de la subasta electrónica según la hora establecida en el cronograma del presente proceso. Por tal motivo, desde la instalación del evento los oferentes deberán estar atentos a los mensajes que remita la Entidad, pues por este medio se indicará la hora exacta del inicio efectivo de la puja. La subasta tendrá una duración de veinte (20) minutos siendo este el tiempo máximo que los oferentes tendrán para efectuar los diferentes lances para lo cual tendrá en cuenta que la reducción del valor para cada lance deberá ser mínimo de **DOS POR CIENTO (2%)**

Para efectos de realizar los lances, los proponentes lo harán a través de la plataforma electrónica SECOP II.

El tiempo de la subasta será susceptible de prórroga. Los oferentes deben tener en cuenta que la plataforma no acepta lances por debajo de **DOS POR CIENTO (2%)** con respecto del precio más bajo que se informe en la subasta. En consecuencia, sólo serán válidos los lances que igualen o que superen este margen.

Todos los lances deben respetar el margen mínimo de mejora dado por la Entidad para todos los artículos ofertados; los lances efectuados por debajo del margen de mejora no serán tenidos en cuenta. Este porcentaje aplica y reduce simultáneamente cada uno de los valores ofertados para el proceso subastado. La plataforma indicará a cada oferente la posición que ocupa en la subasta de acuerdo con sus propuestas.

En el caso que un proponente no haga lances, durante el tiempo que se ha establecido para la subasta, se entenderá que su propuesta económica inicial es su propuesta económica definitiva.

**Un lance es válido si mejora la oferta en mínimo DOS POR CIENTO (2%) con relación al valor de lance anterior**

Entiéndase por lance, cada una de las posturas que hacen los oferentes en el marco de una subasta, es decir, una nueva oferta económica expresada en moneda legal colombiana, que mejora a favor de la Entidad el precio de la oferta base. El Margen Mínimo de Mejora debe entenderse como el valor mínimo en el cual el oferente en una subasta inversa debe reducir el valor de su Lance para que sea válido, el cual es expresado en pesos colombianos del precio de inicio de la subasta. Para el presente proceso, se considerarán válidos los lances que tengan una diferencia mínima de **DOS POR CIENTO (2%)**[12]

Para efectos de realizar los lances, los proponentes lo harán a través de la plataforma electrónica SECOP II.

La plataforma transaccional controla el margen mínimo configurado por el DNP desde el primer lance que realice cada uno de los proponentes, éste entendido como valor mínimo que un proponente aplica en un evento de subasta inversa con respecto al total del último lance válido.

[12] El margen mínimo de mejora se determinó a partir de dos ejercicios: (i) la comparación de las cotizaciones allegadas, que mostró una variación mínima del 1%, y (ii) la revisión de antecedentes de procesos de contratación similares, cuyo promedio fue del 2%. Con base en ello, se estableció un promedio simple del 2%, el cual se adopta como parámetro técnico para este proceso, garantizando competitividad y uso eficiente de los recursos públicos

El SECOP II informa en tiempo real el valor del mejor lance, permitiendo a los proponentes conocer en línea el último lance realizado durante el evento de subasta, sin identificar el oferente que lo presenta. De igual forma, el proponente que no cumpla con el margen mínimo establecido por el DNP, SECOP II no le permitirá presentar el lance hasta que este sea válido conforme a las reglas del proceso.

Una vez finalizado el tiempo establecido para la subasta inversa, la plataforma determinará como ganador al oferente que ocupe la primera posición, posteriormente se descargará el informe de la subasta que arroja la plataforma, el cual será el soporte para la adjudicación.

**Configuración de tiempo adicional**

Si se realiza una postura por uno cualquiera de los proponentes habilitados en el último minuto de duración del evento, y esta postura mejora la oferta que al momento se encuentra en la posición número uno (1), la subasta se extenderá dos (2) minutos más. Lo anterior se ejecutará de forma sucesiva y automática hasta que no se presenten posturas ó lances en los últimos dos (2) minutos. Será importante establecer que, por restricciones técnicas de los sistemas electrónicos, la autoextensión se realiza de manera automática siempre y cuando medien diez (10) segundos entre el momento del lance que da origen a la autoextensión y el momento en que culmina dicha autoextensión o el término establecido para la finalización del evento.

**Posibilidad de enviar mensajes durante la subasta electrónica a todos los Proveedores:**

El DNP podrá enviar mensajes a todos los Proveedores habilitados para participar en la subasta electrónica así:

- SECOP II, identifica desde la cuenta de Entidad Estatal el estado de conexión de los Proveedores en la subasta electrónica.
- El canal de mensajes estará habilitado entre Entidad Estatal y Proveedores durante el desarrollo de la subasta electrónica, independientemente del estado de conexión de los Proveedores.
- El canal de mensajes estará habilitado desde que la subasta electrónica se encuentre “En curso”. Por lo cual, los mensajes enviados por la Entidad Estatal a los Proveedores serán recibidos por ellos cuando se conecten a la subasta.
- Todos los mensajes intercambiados por la Entidad Estatal y los Proveedores pueden ser consultados en la sección de “Mensajes” del módulo de subasta electrónica. Una vez, finalice el evento de subasta la Entidad Estatal podrá exportar esta información desde el informe en Excel que genera la plataforma.
- Los Proveedores pueden exportar el inventario de mensajes intercambiados durante la subasta en la sección de “Mensajes” a través de la funcionalidad de “Exportar”, esta acción generará un documento en formato PDF con el registro de estos mensajes, inclusive los mensajes generados por la Entidad Estatal cuando el Proveedor no se encontraba conectado.

**Retiro del evento de subasta.**

La herramienta para la subasta del SECOP II permite que cualquier proponente pueda desistir del evento de Subasta Electrónica de manera libre y voluntaria. Para ello, tendrá habilitado la funcionalidad de “Finalizar participación” y de

esta manera indicar la justificación correspondiente. Esta acción es irreversible, es decir, la plataforma bloquea al proponente que se retire del evento de Subasta Electrónica para que no pueda ingresar nuevamente.

**Finalización del evento de subasta**

Una vez finalizado el tiempo establecido para la subasta inversa, la plataforma determinará como ganador al oferente que ocupe la primera posición, posteriormente se descargará el informe de la subasta que arroja la plataforma, el cual será el soporte para la adjudicación.

**Precio artificialmente bajo**

Cuando el comité técnico evaluador considere que el lance final es artificialmente bajo, la Entidad, adelantará el procedimiento establecido en el artículo Articulo 2.2.1.1.2.2.4. del Decreto 1082 de 2015 y la Guía para el manejo de ofertas artificialmente bajas en Procesos de Contratación[13] y podrá requerir al proponente con el mejor lance efectuado a través de la sección de "Mensajes" del expediente del proceso.

**Indisponibilidad de la plataforma en el evento de subasta**

Si llegare a presentarse una falla y/o indisponibilidad en la plataforma durante el desarrollo de la subasta electrónica, esta se suspenderá y/o cancelará y los proponentes deben estar atentos a las comunicaciones generadas por la entidad una vez restablecido el servicio; el evento de subasta electrónica se reanudará dentro de las 24 horas hábiles siguientes a la superación de la falla. En consecuencia, los lances efectuados en la audiencia cancelada no se tendrán en cuenta y los nuevos lances se realizarán a partir del margen mínimo establecido en la subasta inicial.

En el evento que el proponente presente inconvenientes para el ingreso a la plataforma SECOP II y su módulo de subasta, no imputables a la plataforma, se aplicará lo definido en el Artículo 2.2.1.2.1.2.6. del Decreto 1082 de 2015 que señala:

> *"(…) Si por causas imputables al oferente o a su proveedor de soluciónes de tecnología de la información y telecomunicaciones, durante la subasta inversa electrónica la conexión con el sistema se pierde, la subasta continuará y la entidad estatal entiende que el proveedor que pierde su conexión ha desistido de participar en la misma".*

Lo anterior, salvo que logre volver a conectarse antes de la terminación del evento, entendiendo que su propuesta está constituida por la presentación de oferta inicial de precio dentro del proceso de selección de conformidad con el Articulo 2.2.1.2.1.1.1 del Decreto 1082 de 2015, o por el último lance mientras estuviera conectado a la plataforma tecnológica de subasta.

La Entidad no se hará responsable por fallas ajenas a las ocurridas por parte de la plataforma SECOP II, las cuales deberán ser debidamente certificadas por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente.

[13] https://www.colombiacompra.gov.co/sites/cce_public/files/cce_documents/cce_guia_artificialmente_bajas.pdf

**REGLAS QUE SE DEBEN TENER EN CUENTA EN EL EVENTO DE SUBASTA INVERSA ELECTRÓNICA**

- Los lances para mejorar la propuesta económica serán calculados en pesos colombianos.
- Un lance es válido si mejora el último lance del evento en por lo menos el margen mínimo correspondiente al DOS POR CIENTO (2%).
- La subasta iniciará a la hora establecida por la Entidad y se desarrollará por el lapso de 20 minutos.
- Los proponentes podrán presentar una nueva propuesta si disminuye mínimo en DOS POR CIENTO (2%) la propuesta económica base, de lo contrario la plataforma lo considerará como no válido y se mantendrá la OFERTA anterior.
- Todo lance posterior anula el anterior del mismo proponente, de tal forma que al final del proceso el último lance que se toma de cada proponente se constituirá como la propuesta económica definitiva.
- La Entidad publicará el resultado de la subasta inversa en el sitio destinado en el SECOP II para el presente proceso contractual y el proponente ganador será aquel que haya ofertado el menor precio válido.

De igual manera, se recomienda a los participantes que previa realización del evento de subasta, verifiquen la información contenida en los documentos, instructivos y guías establecidos por Colombia Compra Eficiente para la presentación de las ofertas por parte de los proveedores, y en caso de ser necesario o tener dudas consulten a la mesa de ayuda de Colombia Compra Eficiente.

## 8. CRITERIOS DE DESEMPATE

En caso de empate, la Entidad Compradora agotará los factores de desempate establecidos en los numerales 1 al 11 del Artículo 35 de la Ley 2069 de 2020 y el Artículo 3 del Decreto 1860 de 2021, con el fin de dirimir un empate cuando respecto del puntaje total se llegue a presentar esta situación en la puntuación de dos o más ofertas de manera que una u otra queden ubicadas en el primer lugar.

### 8.1. PREFERIR LA OFERTA DE BIENES O SERVICIOS NACIONALES FRENTE A LA OFERTA DE BIENES O SERVICIOS EXTRANJEROS.

Se entiende por servicio de origen nacional aquellos prestados por empresas constituidas de acuerdo con la legislación nacional, por personas naturales de Colombia o por residentes en Colombia.

a) Lo anterior será verificado del certificado de existencia y representación legal para personas jurídicas.
b) Para personas naturales se verificará con la copia de la cédula de ciudadanía, de extranjería o visa de residente, si es el caso.

**Nota 1:** Para el caso de los proponentes plurales, todos los integrantes deberán acreditar el origen nacional de la oferta en las condiciones señaladas en la ley.

### 8.2. PREFERIR LA PROPUESTA DE LA MUJER CABEZA DE FAMILIA, MUJERES VÍCTIMAS DE LA VIOLENCIA INTRAFAMILIAR O DE LA PERSONA JURÍDICA EN LA CUAL PARTICIPE O PARTICIPEN MAYORITARIAMENTE; O, LA DE UN PROPONENTE PLURAL CONSTITUIDO POR

**MUJERES CABEZA DE FAMILIA, MUJERES VÍCTIMAS DE VIOLENCIA INTRAFAMILIAR Y/O PERSONAS JURÍDICAS EN LAS CUALES PARTICIPE O PARTICIPEN MAYORITARIAMENTE.**

La acreditación para este factor se hará de la siguiente manera según el caso correspondiente.

**A.** **Mujer cabeza de familia**: Su acreditación se realizará en los términos del artículo 1 de la Ley 1232 de 2008, o la norma que lo modifique, aclare, adicione o sustituya.

La condición de mujer cabeza de familia y la cesación de esta se otorgará desde el momento en que ocurra el respectivo evento y se declare ante un notario. En la declaración que se presente para acreditar la calidad de mujer cabeza de familia deberá verificarse que la misma dé cuenta del cumplimiento de los requisitos establecidos en el artículo 2 de la Ley 82 de 1993, modificado por el artículo 1 de la Ley 1232 de 2008.

Por tanto, para acreditar esta condición se deberá adjuntar a la propuesta declaración por parte de la mujer ante notario, expresando las circunstancias básicas del respectivo caso, junto con la copia de los documentos de identidad. Esta declaración debe tener una fecha de expedición no mayor a treinta (30) días calendarios anteriores a la fecha del cierre del proceso de selección.

**B.** Mujeres víctimas de la violencia intrafamiliar:

Se acreditará esta condición de conformidad con el artículo 21 de la Ley 1257 de 2008 o la norma que lo modifique, aclare, adicione o sustituya. De acuerdo con lo anterior deberá adjuntar copia de la medida de protección que establezca la medida de protección procedente, la debe impartir el comisario de familia del lugar donde ocurrieron los hechos y a falta de este el juez civil municipal o promiscuo municipal, o la autoridad indígena, según se el caso.

Copia de los documentos de identidad.

**C.** En caso de personas jurídicas

En el caso de las personas jurídicas se preferirá a aquellas en las que participen mayoritariamente mujeres cabeza de familia y/o mujeres víctimas de violencia intrafamiliar, para lo cual el representante legal o el revisor fiscal, según corresponda, presentará un certificado, mediante el cual acredita, bajo la gravedad de juramento, que más del cincuenta por ciento (50 %) de la composición accionaria o cuota parte de la persona jurídica está constituida por mujeres cabeza de familia y/o mujeres víctimas de violencia intrafamiliar, Además, deberá acreditar la condición indicada de cada una de las mujeres que participen en la sociedad, aportando los documentos de cada una de ellas, de acuerdo con los literales anteriores.

**D.** En el caso de los proponentes plurales

Se preferirá la oferta cuando cada uno de los integrantes acredite alguna de las condiciones señaladas anteriormente en este numeral.

**Nota:** De acuerdo con el artículo 5 de la Ley 1581 de 2012, el titular de la información de estos datos sensibles, como es el caso de las mujeres víctimas de violencia intrafamiliar, deberá autorizar de manera previa y expresa el tratamiento de esta información, en los términos del literal a) del artículo 6 de la precitada Ley, como requisito para el otorgamiento del criterio de desempate.

### 8.3. PREFERIR LA PROPUESTA PRESENTADA POR EL OFERENTE QUE ACREDITE EN LAS CONDICIONES ESTABLECIDAS EN LA LEY QUE POR LO MENOS EL DIEZ POR CIENTO (10%) DE SU NÓMINA ESTÁ EN CONDICIÓN DE DISCAPACIDAD A LA QUE SE REFIERE LA LEY 361 DE 1997

Dicho personal deberá haber sido contratado por lo menos un (1) año de anterioridad a la fecha de cierre del proceso de contratación o desde el momento de la constitución de la persona jurídica cuando esta es inferior a un (1) año y que manifieste adicionalmente que mantendrá dicho personal por un lapso igual al término de ejecución del contrato.

Deberá acreditar esta situación presentando los siguientes documentos:

a) Certificación vigente expedida por la Oficina del Ministerio del Trabajo respectiva.
b) El proponente debe adjuntar a su oferta el Anexo "Acreditación de vinculación laboral de personas en condiciones de Discapacidad", formato que debe estar suscrito por la persona natural o por Representante Legal de la persona jurídica que acredita el personal con discapacidad y el revisor fiscal o quien haga sus veces en la respectiva jurisdicción, según sea el caso, en donde se evidencie que el personal referido ha sido contratado por lo menos con un (1) año de anterioridad a la fecha de cierre o desde el momento de la constitución de la persona jurídica cuando esta sea inferior a un año y se manifesté el compromiso de mantener vinculado a dicho personal por un lapso igual al de la contratación.

**Si la oferta es presentada por un proponente plural**, el integrante del oferente que acredite que el diez por ciento (10%) de su nómina está en condición de discapacidad en los términos del presente numeral, debe tener una participación de por lo menos el veinticinco por ciento (25%) en el consorcio, unión temporal y aportar mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta**.**

El tiempo de vinculación en la planta referida de que trata este numeral se acreditará con el certificado de aportes a seguridad social del último año o del tiempo de su constitución cuando su conformación es inferior a un (1) año, en el que se demuestren los pagos realizados por el empleador.

### 8.4. PREFERIR LA PROPUESTA PRESENTADA POR EL OFERENTE QUE ACREDITE LA VINCULACIÓN EN MAYOR PROPORCIÓN DE PERSONAS MAYORES QUE NO SEAN BENEFICIARIOS DE LA PENSIÓN DE VEJEZ, FAMILIAR O DE SOBREVIVENCIA Y QUE HAYAN CUMPLIDO EL REQUISITO DE EDAD DE PENSIÓN ESTABLECIDO EN LA LEY.

- El proponente debe adjuntar a su oferta el Anexo "*Acreditación de vinculación de personas mayores*" (certificación bajo la gravedad de juramento) la cual debe estar suscrita por la

persona natural o por Representante Legal de la persona jurídica, o revisor fiscal según sea el caso, manifestando que las personas relacionadas no son beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que han cumplido el requisito de edad de pensión establecido en la ley.

Solo se tendrá en cuenta la acreditación de aquellas personas mayores que hayan cumplido el requisito de edad de pensión, y que hayan estado vinculadas con una anterioridad igual o mayor a un año de la fecha de cierre del proceso.

Para los casos de constitución inferior a un año se tendrá en cuenta a aquellos que hayan estado vinculados desde el momento de la constitución de la persona jurídica.

El tiempo de vinculación en la planta referida, se acreditará con el certificado de aportes a seguridad social del último año o del tiempo de constitución de la persona jurídica, cuando su conformación es inferior a un (1) año, en el que se demuestren los pagos realizados por el empleador.

- **En el caso de los oferentes plurales**, el representante del mismo deberá certificar el número de personas mayores que no sean beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de edad de pensión establecido en la Ley, vinculadas por cada uno de sus integrantes, o por la unión temporal o consorcio; junto con los documentos de identificación de cada una de las personas vinculadas.

En cualquiera de los dos supuestos anteriores, para el otorgamiento del criterio de desempate, cada uno de los trabajadores que cumpla las condiciones previstas por la ley, allegará un certificado, mediante el cual acredita, bajo la gravedad de juramento, que no es beneficiario de pensión de vejez, familiar o sobre vivencia, y cumple la edad de pensión; además, se deberá allegar el documento de identificación del trabajador que lo firma.

La mayor proporción se definirá en relación con el número total de trabajadores vinculados en la planta de personal, por lo que se preferirá al oferente que acredite un porcentaje mayor. En el caso de proponentes plurales, la mayor proporción se definirá con la sumatoria de trabajadores vinculados en la planta de personal de cada uno de sus integrantes.

### 8.5. PREFERIR LA PROPUESTA PRESENTADA POR EL OFERENTE QUE ACREDITE, EN LAS CONDICIONES ESTABLECIDAS EN LA LEY, QUE POR LO MENOS DIEZ POR CIENTO (10%) DE SU NÓMINA PERTENECE A POBLACIÓN INDÍGENA, NEGRA, AFROCOLOMBIANA, RAIZAL, PALANQUERA, RROM O GITANAS.

Para lo cual el proponente deberá adjuntar:

a. Certificación expedida por la persona natural, el representante legal o el revisor fiscal, según corresponda, bajo la gravedad de juramento señalando las personas vinculadas a su nómina y el número de identificación, nombre de las personas que pertenecen a la población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitana.

Solo se tendrá en cuenta la vinculación de aquellas personas que hayan estado vinculadas con una anterioridad igual o mayor a un (1) año contado a partir de la fecha del cierre del proceso. Para los casos de constitución inferior a un (1) año, se tendrá en cuenta a aquellos que hayan estado vinculados desde el momento de constitución de la persona jurídica.

b. Certificado de aportes a seguridad social del último año o del tiempo de su constitución cuando su conformación es inferior a un (1) año, en el que se demuestren los pagos realizados por el empleador, para acreditar el tiempo de vinculación en la planta referida,

c. Certificación expedida por el Ministerio del Interior en la cual acredite que el trabajador pertenece a la comunidad indígena, comunidades negras, afrocolombianas, raizales, palenqueras, Rrom o gitanas en los términos del Decreto 2893 de 2011, o la norma que lo modifique, sustituya o complemente.

**En el caso de los proponentes plurales**, su representante legal presentará un certificado, mediante el cual acredita que por lo menos diez por ciento (10%) del total de la nómina de sus integrantes pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitana. Este porcentaje se definirá de acuerdo con la sumatoria de la nómina de cada uno de los integrantes del proponente plural. Las personas enunciadas anteriormente podrán estar vinculadas a cualquiera de sus integrantes. En todo caso, deberá aportar la copia de la certificación expedida por el Ministerio del Interior, en la cual acredite que el trabajador pertenece a la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana en los términos del Decreto Ley 2893 de 2011, o la norma que lo modifique, sustituya o complemente.

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

### 8.6. PREFERIR LA PROPUESTA DE PERSONAS EN PROCESO DE REINTEGRACIÓN O REINCORPORACIÓN O DE LA PERSONA JURÍDICA EN LA CUAL PARTICIPE O PARTICIPEN MAYORITARIAMENTE; O, LA DE UN PROPONENTE PLURAL CONSTITUIDO POR PERSONAS EN PROCESO DE REINCORPORACIÓN, Y/O PERSONAS JURÍDICAS EN LAS CUALES PARTICIPE O PARTICIPEN MAYORITARIAMENTE.

Se adjuntará alguno de estos documentos según corresponda:

a. La certificación en las desmovilizaciones colectivas que expide la Oficina de Alto Comisionado para la Paz.
b. Certificado que expida el Comité Operativo para la Dejación de las Armas respecto de las personas desmovilizadas en forma individual.
c. El certificado que emita la Agencia para la Reincorporación y la Normalización que acredite que la persona se encuentra en proceso de reincorporación o reintegración
d. U otro documento que para el efecto determine la ley

e. Copia del documento de identificación de la persona en proceso de reintegración o reincorporación.

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

**Tratándose de proponentes plurales**, se preferirá la oferta cuando todos los integrantes sean personas en proceso de reincorporación, para lo cual se entregará alguno de los certificados señalados en los literales de este numeral, y/o personas jurídicas donde más del cincuenta por ciento (50 %) de la composición accionaria o cuotas parte esté constituida por personas en proceso de reincorporación, para lo cual el representante legal, o el revisor fiscal, si está obligado a tenerlo, acreditará tal situación aportando los documentos de identificación de cada una de las personas en proceso de reincorporación.

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

**8.7 PREFERIR LA OFERTA PRESENTADA POR UN PROPONENTE PLURAL** siempre que se cumplan los siguientes literales:

**A.** Esté conformado por al menos una madre cabeza de familia y/o una persona en proceso de reincorporación o reintegración.

Para lo cual se acreditarán estas condiciones de acuerdo con lo previsto en el inciso 1 del numeral 2 y/o el inciso 1 del numeral 6 del artículo 2.2.1.2.4.2.17 adicionado al decreto 1082 de 2015, por el decreto 1860 de 2021:

> *Preferir la propuesta de la mujer cabeza de familia. Su acreditación se realizará en los términos del parágrafo del artículo 2 de la Ley 82 de 1993, modificado por el artículo 1 de la Ley 1232 de 2008, o la norma que lo modifique, aclare, adicione o sustituya. Es decir, la condición de mujer cabeza de familia y la cesación de esta se otorgará desde el momento en que ocurra el respectivo evento y se declare ante un notario. En la declaración que se presente para acreditar la calidad de mujer cabeza de familia deberá verificarse que la misma dé cuenta del cumplimiento de los requisitos establecidos en el artículo 2 de la Ley 82 de 1993, modificado por el artículo 1 de la Ley 1232 de 2008.*

**Para el caso de la mujer cabeza de familia**: Su acreditación se realizará en los términos del artículo 1 de la Ley 1232 de 2008, o la norma que lo modifique, aclare, adicione o sustituya.

*La condición de mujer cabeza de familia y la cesación de esta se otorgará desde el momento en que ocurra el respectivo evento y se declare ante un notario. En la declaración que se presente para acreditar la calidad de mujer cabeza de familia deberá verificarse que la misma dé cuenta del cumplimiento de los requisitos establecidos en el artículo 2 de la Ley 82 de 1993, modificado por el artículo 1 de la Ley 1232 de 2008.*

*Por tanto, para acreditar esta condición se deberá adjuntar a la propuesta declaración por parte de la mujer ante notario, expresando las circunstancias básicas del respectivo caso, junto con la copia de los documentos de identidad. Esta declaración debe tener una fecha de expedición no mayor a treinta (30) días calendarios anteriores a la fecha del cierre del proceso de selección.*

**Para el caso de personas en proceso de reincorporación o** reintegración Se adjuntará alguno de estos documentos según corresponda:

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

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

c. El certificado que emita la Agencia para la Reincorporación y la Normalización que acredite que la persona se encuentra en proceso de reincorporación o reintegración

d. U otro documento que para el efecto determine la ley

e. Copia del documento de identificación de la persona en proceso de reintegración o reincorporación.

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

**Tratándose de proponentes plurales**, se preferirá la oferta cuando todos los integrantes sean personas en proceso de reincorporación, para lo cual se entregará alguno de los certificados señalados en los literales de este numeral, y/o personas jurídicas donde más del cincuenta por ciento (50 %) de la composición accionaria o cuotas parte esté constituida por personas en proceso de reincorporación, para lo cual el representante legal, o el revisor fiscal, si está obligado a tenerlo, acreditará tal situación aportando los documentos de identificación de cada una de las personas en proceso de reincorporación

- O por una persona jurídica en la cual participe o participen mayoritariamente madres cabeza de familia y/o

**personas en proceso de reincorporación o reintegración**, se acreditará de la siguiente manera:

-Certificado bajo la gravedad de juramento expedido por el representante legal o el revisor fiscal, si están obligados a tenerlo en el cual acrediten, que más del cincuenta por ciento (50 %) de la composición accionaria o cuota parte de la persona jurídica está constituida por madres cabeza de familia y/o personas en proceso de reincorporación o reintegración.

-Además, deberá acreditar la condición indicada de cada una de las personas que participen en la sociedad que sean mujeres cabeza de familia y/o personas en proceso de reincorporación o reintegración, aportando los documentos de cada uno de ellos, de acuerdo con lo previsto en este numeral. Este integrante debe tener una participación de por lo menos el veinticinco por ciento (25 %) en el proponente plural.

**B.** El integrante del proponente plural de que trata el anterior numeral debe aportar mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta.

**C.** En relación con el integrante del literal A ni la madre cabeza de familia o la persona en proceso de reincorporación o reintegración, ni la persona jurídica, ni sus accionistas, socios o representantes legales podrán ser empleados, socios o accionistas de otro de los integrantes del proponente plural, para lo cual el integrante del que trata el literal A, lo manifestará en un certificado suscrito por la persona natural o el representante legal de la persona jurídica.

**NOTA**: Debido a que para el otorgamiento de este criterio de desempate se entregan certificados que contienen datos sensibles, de acuerdo el artículo 5 de la Ley 1581 de 2012, se requiere que el titular de la información de estos, como es el caso de las personas en proceso de reincorporación y/o reintegración autoricen de manera previa y expresa el tratamiento de esta información, en los términos del literal a) del artículo 6 de la Ley 1581 de 2012, como requisito para el otorgamiento del criterio de desempate.

### 8.8 PREFERIR LA OFERTA PRESENTADA POR UNA MIPYME O COOPERATIVAS O ASOCIACIONES MUTUALES; O UN PROPONENTE PLURAL CONSTITUIDO POR MIPYMES, COOPERATIVAS O ASOCIACIONES MUTUALES.

**a.** Preferir la oferta presentada por una Mipyme: lo cual se verificará en los términos del artículo 2.2.1.2.4.2.4 del presente Decreto, en concordancia con el parágrafo del artículo 2.2.1.13.2.4 del Decreto 1074 de 2015.[14]

[14] Artículo 2.2.1.2.4.2.4. Acreditación de requisitos para participar en convocatorias limitadas. La Mipyme colombianas deben acreditar que tiene el tamaño empresarial establecido por la ley de la siguiente manera: Las personas naturales mediante certificación expedida por ellos y un contador público, adjuntando copia del registro mercantil. Las personas jurídicas mediante certificación expedida por el representante legal y el contador o revisor fiscal, si están obligados a tenerlo, adjuntando copia del certificado de existencia y representación legal expedido por la Cámara de Comercio o por la autoridad competente para expedir dicha certificación. Para la acreditación deberán observarse los rangos de clasificación empresarial establecidos de conformidad con la Ley 590 de 2000 y el Decreto 1074 de 2015, o las normas que lo modifiquen, sustituyan o complementen.
[7] Decreto 1074 de 2015: PARÁGRAFO. Para la aplicación de los incentivos del sistema de compras y contratación pública, la acreditación del tamaño empresarial se efectuará de acuerdo con lo previsto en el artículo 2.2.1.2.4.2.4 del Decreto 1082 de 2015 y demás normas que lo aclaren, modifiquen o adicionen.

**b.** Se preferirá la oferta presentada por una cooperativa o asociaciones mutuales, para lo cual se aportará el certificado de existencia y representación legal expedido por la Cámara de Comercio o la autoridad respectiva.

**Tratándose de proveedores plurales**, se preferirá la oferta cuando cada uno de los integrantes acredite alguna de las condiciones señaladas anteriormente de este numeral.

En el caso específico en que el empate se presente entre cooperativas o asociaciones mutuales que tengan el tamaño empresarial de grandes empresas junto con micro, pequeñas o medianas, se preferirá la oferta las cooperativas o asociaciones mutuales que cumplan con los criterios de clasificación empresarial definidos por el Decreto 1074 de 2015, que sean micro, pequeñas o medianas.

En el evento en que el empate se presente entre proponentes plurales cuyos integrantes estén conformados únicamente por cooperativas y asociaciones mutuales que tengan la calidad de grandes empresas junto con otras en las que los integrantes tengan la calidad de micro, pequeñas o medianas, se preferirá la oferta de aquellos proponentes plurales en los cuales al menos uno de sus integrantes sea una cooperativa o asociación mutual que cumpla con los criterios de clasificación empresarial definidos por el Decreto 1074 de 2015, que sean micro, pequeñas o medianas.

### 8.9 PREFERIR LA OFERTA PRESENTADA POR EL PROPONENTE PLURAL CONSTITUIDO POR MICRO Y/O PEQUEÑAS EMPRESAS, COOPERATIVAS O ASOCIACIONES MUTUALES.

**a.** *Para las empresas micro y/o pequeñas empresas: se verificará en los términos del artículo 2.2.1.2.4.2.4 del presente Decreto, en concordancia con el parágrafo del artículo 2.2.1.13.2.4 del Decreto 1074 de 2015.*

**b.** *Cooperativas o Asociaciones se acreditará mediante el certificado de existencia y representación legal*

---

"*Decreto 1082 de 2015- Artículo 2.2.1.2.4.2.4. Modificado por el Articulo 5 del Decreto 1860 de 2021- Acreditación de requisitos para participar en convocatorias limitadas. La Mipyme colombianas deben acreditar que tiene el tamaño empresarial establecido por la ley de la siguiente manera:*
***1.** Las personas naturales mediante certificación expedida por ellos y un contador público, adjuntando copia del registro mercantil.*
***2.** Las personas jurídicas mediante certificación expedida por el representante legal y el contador o revisor fiscal, si están obligados a tenerlo, adjuntando copia del certificado de existencia y representación legal expedido por la Cámara de Comercio o por la autoridad competente para expedir dicha certificación.*
*Para la acreditación deberán observarse los rangos de clasificación empresarial establecidos de conformidad con la Ley 590 de 2000 y el Decreto 1074 de 2015, o las normas que lo modifiquen, sustituyan o complementen.*
***PARÁGRAFO 1.** En todo caso, las Mipyme también podrán acreditar esta condición con la copia del certificado del Registro Único de Proponentes, el cual deberá encontrarse vigente y en firme al momento de su presentación.*
***PARÁGRAFO 2.** Para efectos de la limitación a Mipyme, los proponentes aportarán la copia del registro mercantil, del certificado de existencia y representación legal o del Registro Único de Proponentes, según corresponda conforme a las reglas precedentes, con una fecha de máximo sesenta*
*(60) días calendario anteriores a la prevista en el cronograma del Proceso de Contratación para el inicio del plazo para solicitar la convocatoria limitada.*
***PARÁGRAFO 3.** En las convocatorias limitadas, las Entidades Estatales independientemente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos, solo deberán aceptar las ofertas de Mipyme o de proponentes plurales integrados únicamente por Mipyme..*"

*expedido por la Cámara de Comercio o la autoridad respectiva.*

*Tratándose de proveedores plurales, cuyos integrantes estén conformados únicamente por cooperativas y asociaciones mutua/es que tengan la calidad de grandes empresas junto con otras en las que los integrantes tengan la calidad de micro, pequeñas o medianas, se preferirá la oferta de aquellos proponentes plurales en los cuáles al menos uno de sus integrantes sea una cooperativa o asociación mutual que cumpla con los criterios de clasificación empresarial definidos por el Decreto 1074 de 2015, que sean micro, pequeñas o medianas.*

**8.10 PREFERIR AL OFERENTE QUE ACREDITE DE ACUERDO CON SUS ESTADOS FINANCIEROS O INFORMACIÓN CONTABLE CON CORTE A 31 DE DICIEMBRE DEL AÑO ANTERIOR, POR LO MENOS EL VEINTICINCO POR CIENTO (25%) DEL TOTAL DE PAGOS REALIZADOS A MIPYMES, COOPERATIVAS O ASOCIACIONES MUTUALES POR CONCEPTO DE PROVEEDURÍA DEL OFERENTE, REALIZADOS DURANTE EL AÑO ANTERIOR** para lo cual:

**a.** El proponente persona natural y contador público; o el representante legal de la persona jurídica y revisor fiscal para las personas obligadas por ley; o del representante legal de la persona jurídica y contador público, según corresponda, entregará un certificado expedido bajo la gravedad de juramento, en el que conste que por lo menos el veinticinco por ciento (25%) del total de pagos fueron realizados a Mipyme, cooperativas o asociaciones mutuales.

**b.** Igualmente, cuando la oferta es presentada por un proponente plural se preferirá a este siempre que:

- Esté conformado por al menos una Mipyme, cooperativa o asociación mutual que tenga una participación de por lo menos el veinticinco por ciento (25%) en el proponente plural, para lo cual se presentará el documento de conformación del proponente plural y, además, ese integrante acredite la condición de Mipyme, cooperativa o asociación mutual en los términos del numeral 8 del presente artículo;
- La Mipyme, cooperativa o asociación mutual aporte mínimo el veinticinco por ciento (25 %) de la experiencia acreditada en la oferta; y
- Ni la Mipyme, cooperativa o asociación mutual ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los otros integrantes del proponente plural, para lo cual el integrante respectivo lo manifestará mediante un certificado suscrito por la persona natural o el representante legal de la persona jurídica.

**En el evento en que el empate se presente entre proponentes plurales**, que cumplan con los requisitos de los incisos anteriores, cuyos integrantes estén conformados únicamente por cooperativas y asociaciones mutuales que tengan la calidad de grandes empresas junto con otras en las que los integrantes tengan la calidad de micro, pequeñas o medianas, se preferirá la oferta de aquellos proponentes plurales en los cuales al menos uno de sus integrantes sea una cooperativa o asociación mutual que cumpla con los criterios de clasificación empresarial definidos por el Decreto 1074 de 2015, que sean micro, pequeñas o medianas.

### 8.11 PREFERIR LAS EMPRESAS RECONOCIDAS Y ESTABLECIDAS COMO SOCIEDAD DE BENEFICIO E INTERÉS COLECTIVO O SOCIEDAD BIC, DEL SEGMENTO MIPYMES

Para lo cual se presentará el certificado de existencia y representación legal en el que conste el cumplimiento a los requisitos del artículo 2 de la Ley 1901 de 2018, o la norma que la modifique o la sustituya. Asimismo, acreditará la condición de Mipyme en los términos del numeral 8 del artículo 2.2.1.2.4.2.17.

### 8.12 PREFERIR LA PROPUESTA PRESENTADA POR PERSONAS QUE ACREDITEN:

(a) Ser jóvenes Egresados del Sistema de Protección del ICBF, en las condiciones previstas en la Ley 2479 de 2025; (b) De la persona jurídica con más del 50% de composición accionaria o cuota parte constituida por jóvenes egresados del Sistema de Protección del ICBF; o (c) proponente plural con al menos un 25% de participación de una persona Egresada del Sistema de Protección del ICBF o persona jurídica con participación mayoritaria de jóvenes egresados del Sistema de Protección del ICBF. Lo anterior de conformidad con el artículo 22 de la Ley 2479 de 2025, que modificó el artículo 35 de la Ley 2069 de 2020.

### 8.13 UTILIZAR UN MÉTODO ALEATORIO PARA SELECCIONAR EL OFERENTE, MÉTODO QUE DEBERÁ HABER SIDO PREVISTO PREVIAMENTE EN LOS DOCUMENTOS DEL PROCESO.

Por último, de persistir el empate, se hará un sorteo mediante el método de suerte y azar, en el que se utilizarán los centavos del valor de la Tasa Representativa del Mercado (TRM) certificada por la Superintendencia Financiera de Colombia, indicador económico que expresa el valor promedio diario de la tasa de cambio entre el peso colombiano y el dólar norteamericano[15] para lo cual el DNP ordenará a los Proponentes con Ofertas empatadas en el orden alfabético según el nombre registrado. Una vez ordenados, EL DNP asignará un número entero a cada uno de estos de forma ascendente, de tal manera que al primero de la lista le corresponde el número 1.

Seguidamente, EL DNP tomará la parte entera (números a la izquierda de la coma decimal) de la TRM del día del cierre del Proceso de Contratación y la divide entre el número total de Proponentes en empate, para posteriormente tomar su residuo y utilizarlo en la selección final. Realizados estos cálculos, el DNP seleccionará a aquel Proponente que presente coincidencia entre el número asignado y el residuo encontrado. En caso de que el residuo sea cero (0), EL DNP seleccionará al Proponente con el mayor número asignado. Este procedimiento se repetirá en caso de que persistan empates entre Proponentes.

**Nota 1**: La acreditación de los criterios de desempate, deberán ser presentados y acreditados junto con la propuesta el día del cierre del proceso señalado en el cronograma del proceso. Por lo anterior y dado que estos documentos no son subsanables toda vez que sirven para la comparación de las ofertas en caso de empate, en el evento que se alleguen con posterioridad a esta fecha, no se tendrán en cuenta.

**Nota 2** En la plataforma del SECOP no se publicará para conocimiento de terceros la información relacionada con los factores de desempate de personas en procesos de reincorporación o reintegración o mujeres víctimas de violencia intrafamiliar o la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana, puesto que su público conocimiento puede afectar el derecho a la intimidad de los oferentes o de sus trabajadores o socios o accionistas. El

[15] https://www.superfinanciera.gov.co/inicio/informes-y-cifras/cifras/establecimientos-de-credito/informacion-periodica/diaria/tasa-de-cambio-representativa-del-mercado-trm-60819

proponente deberá activar la casilla de confidencial cada vez que realice el cargue de estos documentos en la plataforma

## 9. SOPORTE QUE PERMITA LA ESTIMACIÓN, TIPIFICACIÓN Y ASIGNACIÓN DE LOS RIESGOS PREVISIBLES QUE PUEDAN AFECTAR EL EQUILIBRIO CONTRACTUAL

De conformidad con el artículo 4 de la Ley 1150 de 2007 y el numeral 6 del artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015, se identifican los riesgos asociados al proceso de contratación, los cuales se encuentran relacionados en el anexo Matriz de Riesgos, (Ver formato anexo en Excel).

## 10. GARANTÍAS

De conformidad con lo dispuesto en la Ley 80 de 1993, Ley 1150 de 2007 y el Decreto 1082 de 2015, el contratista se obligará a garantizar el cumplimiento de las obligaciones surgidas a favor del **DNP**, con ocasión de la ejecución del contrato y de su liquidación a través de cualquiera de los mecanismos de cobertura del riesgo señalados en el Artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015 (Contrato de seguro contenido en una póliza, patrimonio autónomo y garantía bancaria).

De acuerdo con naturaleza, el objeto del contrato, las obligaciones establecidas y los riesgos definidos, el DNP considera que dentro del presente contrato se debe cubrir los siguientes riesgos:

- Cumplimiento del contrato: cubrirá a la entidad de los perjuicios directos derivados del incumplimiento total o parcial del contrato, así como de su cumplimiento tardío o de su cumplimiento defectuoso, cuando ellos son imputables al contratista. Además de esos riesgos, este amparo comprenderá siempre el pago del valor de las multas y de la cláusula penal pecuniaria que se hayan pactado en el contrato.
- Calidad del servicio: Cubre a la entidad estatal contratante de los perjuicios derivados de la deficiente calidad del servicio prestado.
- Pago de salarios, prestaciones sociales e indemnizaciones laborales: Cubrirá a la entidad estatal contratante de los perjuicios que se le ocasionen como consecuencia del incumplimiento de las obligaciones laborales a que esté obligado el contratista, derivadas de la contratación del personal utilizado en el territorio nacional para la ejecución del contrato amparado.

De otro lado el DNP requiere que la garantía para cada riesgo tenga la siguiente suficiencia:

**Análisis de exigencias de garantías**

| Riesgo | Valor | Vigencia |
|---|---|---|
| Cumplimiento | 20% del valor del Contrato | Plazo de ejecución y seis (6) meses más, contado partir del perfeccionamiento del contrato. |
| Pago de Salarios y prestaciones sociales | 10% del valor del Contrato | Plazo de ejecución del contrato y tres (3) años más partir del a partir del perfeccionamiento del contrato. |

| | | |
|---|---|---|
| Calidad del servicio | 20% del valor del Contrato | Un (1) año contados a partir de la terminación del contrato. |

**Nota 1. -** En todo caso EL CONTRATISTA se compromete a mantener vigente la garantía durante todo el tiempo que demande la ejecución del contrato y hasta su liquidación, so pena de que el DNP haga efectiva la cláusula penal compensatoria de este contrato.

**Nota 2. -** EL CONTRATISTA deberá reponer la garantía antes mencionada, cuando debido a las sanciones impuestas, o de otros hechos, se disminuyere o agotare o cuando su valor se viere afectado por razón de siniestros, durante el término de ejecución del presente contrato, según sea el caso. Así mismo, deberá hacerlo en los eventos contemplados en el artículo 2.2.1.2.3.1.18. del Decreto 1082 de 2015.

**Nota 3. -** En el evento en que la entidad que expida la póliza de seguro que sirva de garantía del presente contrato, sea intervenida, tomado su control o liquidada por el Gobierno Nacional a través de entidad competente, y con ello se genere incertidumbre sobre el pago o efectividad de la garantía aportada, EL CONTRATISTA deberá de manera inmediata presentar nuevas pólizas o reemplazar la expedida por la compañía de seguros intervenida, sujeta a toma de control o en proceso de liquidación.

**Nota 4. -** El contratista deberá constituir a favor del Departamento Nacional de Planeación (DNP), NIT 899.999.011-0, las garantías del contrato de conformidad con lo establecido en el Decreto 1082 de 2015, a más tardar a los dos (2) días hábiles siguientes de la aceptación de la oferta y deberá cargarla por la plataforma de Secop II para la cual será aprobada por la Entidad, siempre y cuando reúna los requisitos legales y contractuales exigidos. Posteriormente, será aprobada por el DNP. Si al vencimiento de dicho término el contratista no ha presentado las garantías pertinentes a la Subdirección de Contratación del DNP, este último podrá dejar constancia que el contrato no inició su ejecución.

## 11. CONVOCATORIA LIMITADA A MIPYMES

Una vez verificado el umbral para convocatorias limitadas a Mipyme, en la página de Colombia Compra Eficiente en donde indican como umbral la suma de $511.708.497 COP (equivalente a USD 125.000) y teniendo en cuenta que el valor del presupuesto oficial destinado para el presente proceso de selección corresponde a la suma de ***OCHOCIENTOS NOVENTA Y NUEVE MILLONES VEINTICINCO MIL CIENTO OCHENTA Y CINCO PESOS M/CTE (899.025.185)*** incluido los tributos a que haya lugar, de conformidad con lo establecido en los artículos 2.2.1.2.4.2.2 , 2.2.1.2.4.2.4 del Decreto 1082 de 2015, modificado por el artículo 5 del decreto 1860 de 2021, la convocatoria del presente proceso de Selección Abreviada **NO** se limitará a Mipymes.

## 12. INDICACIÓN DE SI LA CONTRATACIÓN RESPECTIVA ESTÁ COBIJADA POR UN ACUERDO INTERNACIONAL O UN TRATADO DE LIBRE COMERCIO VIGENTE PARA EL ESTADO COLOMBIANO

De conformidad con el Manual para el Manejo de los Acuerdo Comerciales en Procesos de Contratación, publicado por Colombia Compra Eficiente, a continuación, se relaciona el análisis para el presente proceso:

Tabla 9 Análisis según Acuerdos Comerciales Vigentes

| ACUERDOS COMERCIALES | VIGENTE | | VALOR DEL PROCESO DE CONTRATACIÓN | EXCEPCIÓN APLICABLE AL | PROCESO DE CONTRATACIÓN CUBIERTO POR |
|---|---|---|---|---|---|

| | | | ENTIDAD ESTATAL CUBIERTA | SUPERIOR AL UMBRAL DEL ACUERDO COMERCIAL | PROCESO DE CONTRATACIÓN | EL ACUERDO COMERCIAL |
|---|---|---|---|---|---|---|
| Alianza del Pacífico | Chile | SI | SI | SI | NO | SI |
| | México | SI | SI | SI | NO | SI |
| | Perú | SI | SI | SI | NO | SI |
| Canadá | | SI | SI | SI | NO | SI |
| Chile | | SI | SI | SI | NO | SI |
| Corea | | SI | SI | SI | NO | SI |
| Costa Rica | | SI | SI | SI | NO | SI |
| Estados Unidos | | SI | SI | SI | NO | SI |
| Estados AELC | | SI | SI | SI | NO | SI |
| Unión Europea | | SI | SI | SI | NO | SI |
| Israel | | SI | SI | SI | NO | SI |
| México | | SI | SI | SI | NO | SI |
| Reino Unido e Irlanda del Norte | | SI | SI | SI | NO | SI |
| Comunidad Andina[16] | | SI | SI | SI | NO | SI |
| Triángulo Norte | El Salvador | SI | SI | SI | NO | SI |
| | Guatemala | SI | SI | SI | NO | SI |
| | Honduras | SI | SI | SI | NO | SI |

Lo anterior teniendo en cuenta las reglas previstas en el Manual para el Manejo de los Acuerdos Comerciales en procesos de contratación, publicado en la página web de Colombia Compra Eficiente.

**Nota 1:** Los Acuerdos Comerciales establecen plazos mínimos para presentar las ofertas con el fin de dar el tiempo suficiente a los interesados para preparar sus propuestas, por lo cual, los Documentos del Proceso deben establecer, en su Cronograma, el espacio suficiente para cumplir con esta obligación.

Así las cosas, para el presente proceso, los Acuerdos Comerciales establecen plazos generales para presentar las ofertas, correspondientes a 30 o 40 días calendario contados a partir de la fecha de la publicación del aviso de convocatoria y hasta el día en que vence el término para presentar ofertas, de igual forma establecen la reducción de estos plazos, cuando la Entidad Estatal: (i) Publica en el SECOP los Documentos del Proceso, (ii) Adquiere Bienes o Servicios de Características Técnicas Uniformes, o (iii) Cuando la información del Proceso de Contratación haya sido publicada oportunamente en el Plan Anual de Adquisiciones entre 40 días y 12 meses antes de la expedición del aviso de convocatoria.

**Nota 2:** De conformidad al artículo 2.2.1.2.4.1.3. del Decreto 1082 de 2015 se debe conceder trato nacional a:

> *"[…] (a) Los oferentes, bienes y servicios provenientes de Estados con los cuales Colombia tenga Acuerdos Comerciales, en los términos establecidos en tales Acuerdos Comerciales;*

[16] *"La Decisión 439 de 1998 de la Comisión de la CAN es aplicable a todos los Procesos de Contratación de las Entidades Estatales del nivel nacional, independientemente del valor del Proceso de Contratación".* Fuente. Manual manejo de acuerdos comerciales. Pág. 19 y 25.

*(b) a los bienes y servicios provenientes de Estados con los cuales no exista un Acuerdo Comercial pero respecto de los cuales el Gobierno Nacional haya certificado que los oferentes de Bienes y Servicios Nacionales gozan de trato nacional, con base en la revisión y comparación de la normativa en materia de compras y contratación pública de dicho Estado; y*

*(c) a los servicios prestados por oferentes miembros la Comunidad Andina de Naciones teniendo en cuenta la regulación andina aplicable a la materia.*

*El Ministerio de Relaciones Exteriores debe expedir el certificado por medio del cual se acredite la situación mencionada en el literal (b) anterior en relación con un Estado en particular, lo cual no es requerido para acreditar las situaciones a las que se refieren los literales (a) y (c) anteriores. Para constatar que los oferentes de Bienes y Servicios Nacionales gozan de trato nacional en un Estado, el Ministerio de Relaciones Exteriores debe revisar y comparar la normativa en materia de compras y contratación pública del respectivo Estado para lo cual puede solicitar el apoyo técnico del Ministerio de Comercio, Industria y Turismo y de Colombia Compra Eficiente, dentro de sus competencias legales.*

*Los certificados para acreditar la condición a la que se refiere el literal (b) anterior deben ser publicados en la forma y oportunidad que para el efecto disponga Colombia Compra Eficiente. La vigencia de los certificados será de dos años contados a partir de la fecha de su expedición, sin perjuicio de que el Ministerio de Comercio, Industria y Turismo o Colombia Compra Eficiente soliciten al Ministerio de Relaciones Exteriores su revisión con ocasión de la expedición de nueva normativa en el Estado sobre el cual se expide el certificado. Colombia Compra Eficiente puede determinar vía circular la forma como el Ministerio de Relaciones Exteriores debe constatar que los oferentes de Bienes y Servicios Nacionales gozan de trato nacional y de revisar y comparar la normativa en materia de compras y contratación pública para la expedición del certificado […]".*

## 13. ASPECTOS GENERALES DEL CONTRATO

### 13.1 Identificación del Contrato

El contrato que surja del presente proceso de selección corresponde a **COMPRAVENTA** regulado por Ley 80 de 1993, la Ley 1150 de 2007 y demás normas que las modifiquen, adicionen o deroguen y en las materias no reguladas en dichas leyes a las disposiciones civiles y comerciales.

### 13.2 Plazo de ejecución

El plazo de ejecución del contrato será de **1 mes** contado a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución.

**13.2.1 Vigencia:** La vigencia del licenciamiento, soporte y mantenimiento será de un (1) año, a partir del 1 de octubre de 2026

### 13.3 Valor del contrato

**OCHOCIENTOS NOVENTA Y NUEVE MILLONES VEINTICINCO MIL CIENTO OCHENTA Y CINCO PESOS M/CTE** (899.025.185), equivalentes a 513,46 SMLMV**,** incluidos tributos a los que haya lugar. No obstante, se adjudicará por el valor resultante del evento de subasta.

### 13.4 Forma de pago

El DNP, pagará el cien por ciento (100%) del valor del contrato en un solo pago previo recibo a satisfacción de los siguientes requisitos:

1. Factura o cuenta de cobro según sea el caso con el lleno de los requisitos legales.
2. Aportar los soportes de entrega de los bienes hardware, software y licencias a nombre del DNP.
3. Aportar el documento con las condiciones de atención de requerimientos e incidentes.
4. Recibo de cumplimiento a satisfacción por parte del supervisor del contrato.
5. Copia del comprobante del pago de seguridad social y/o aportes parafiscales (persona natural) o certificación original y/o Copia expedida por el representante legal o revisor fiscal de encontrarse al día en el pago al sistema de seguridad social de sus empleados y en los aportes parafiscales y ARL, si estuviere obligado a este pago (persona jurídica), de acuerdo con lo establecido en el artículo 50 de la Ley 789 de 2002 y artículo 23 de la Ley 1150 de 2007.
6. RUT
7. Certificación de cuenta bancaria

**Nota 1:** Los pagos se efectuarán dentro de los treinta (30) días calendarios siguientes a la radicación de la factura o cuenta de cobro en el Grupo de Central de Cuentas del DNP con el lleno de los requisitos legales, y la presentación de los documentos antes citados. Previa disponibilidad del PAC.

**Nota 2:** Atendiendo lo dispuesto en la Resolución No. 0042 de 2020, expedida por la Dirección de Impuestos y Aduanas Nacionales – DIAN, en sus modificaciones y en la Directiva Presidencial No. 09 de 2020 aquellos proponentes responsables de IVA se encuentran obligados a presentar facturación electrónica.

**Nota 3:** El DNP no se hace responsable por las demoras presentadas en el trámite para el pago al Contratista cuando ellas fueren ocasionadas por encontrarse incompleta la documentación de soporte o no ajustarse a cualquiera de las condiciones establecidas en los documentos que integran el proceso o si las facturas o cuentas de cobro no han sido correctamente elaboradas o no se acompañan los documentos requeridos para el pago, por lo que el término para éste sólo efecto empezará a contarse desde la fecha en que se haya aportado el último de los documentos.

**Nota 4:** Se entienden incluidos como parte del precio todos los derechos, gastos directos o indirectos, impuestos, tasas y contribuciones que se generen con ocasión o como efecto del presente contrato, los cuales corren a cargo del CONTRATISTA.

**Nota 5:** Sin perjuicio de lo anterior, queda entendido que la forma de pago supone la prestación real y efectiva de los servicios pactados y del cumplimiento de las obligaciones generales y específicas.

**Nota 6:** El proveedor debe radicar factura o cuenta de cobro en el Grupo de Central de Cuentas del DNP por cada fuente de financiación que respalda el contrato, si aplica más de una fuente.

**13.5 Obligaciones de las partes:**

**13.5.1 Obligaciones del Contratista:**

Además de las previstas en la Ley 80 de 1993, Ley 1150 de 2007, Decreto 1082 de 2015 y normas reglamentarias inherentes a la naturaleza del contrato, a las obligaciones derivadas de las disposiciones legales vigentes que regulan su actividad y las contenidas en los documentos que forman parte del contrato, el contratista debe cumplir con las siguientes obligaciones:

**13.5.2 Obligaciones Generales:**

Además de las previstas en la Ley 80 de 1993, Ley 1150 de 2007, Decreto 1082 de 2015 y normas reglamentarias inherentes a la naturaleza del contrato, a las obligaciones derivadas de las disposiciones legales vigentes que regulan su actividad y las contenidas en los documentos que forman parte del contrato, el contratista debe cumplir con las siguientes obligaciones:

1. Cumplir con todas las especificaciones técnicas establecidas en los estudios previos, análisis del sector, pliegos de condiciones, adendas, la oferta y el contrato que se suscriba como resultado del presente proceso de selección.
2. Constituir la garantía de cumplimiento para amparar la ejecución del contrato, de acuerdo con los requerimientos realizados por la Entidad, y mantener actualizadas las vigencias y montos de los amparos de las garantías constituidas con ocasión de la suscripción del Contrato, en el evento de presentarse modificaciones en valor y/o plazo, suspensiones, y demás modificaciones que afecten su vigencia o monto.
3. Atender los lineamientos y políticas generales, así como dar cumplimiento a los procesos, subprocesos e instructivos de los sistemas de gestión establecidos en el DNP (Sistema Integrado de Gestión, Sistema de Gestión en Seguridad y Salud Ocupacional, Sistema de Gestión de Seguridad de la Información y Sistema de Gestión Documental) y que se relacionen con el objeto del contrato.
4. Acreditar a la Supervisión del contrato, para cada pago, que se encuentra al día por conceptos de seguridad social y aportes parafiscales, de conformidad con lo establecido en el artículo 50 de la Ley 789 de 2002 y en el artículo 23 de la Ley 1150 de 2007, en lo relacionado con los sistemas de salud, riesgos laborales, pensiones y aportes a las cajas de compensación familiar, SENA e ICBF cuando haya lugar a ello, de conformidad con las normas y reglamentos que rigen la materia. Ante el incumplimiento de estas obligaciones, el DNP dará aviso de tal situación a las autoridades competentes. Garantizar que ninguna de las condiciones y especificaciones técnicas establecidas en el Anexo Técnico generan costos adicionales para la Entidad.
5. Abstenerse de utilizar la información entregada por la Entidad para cualquier fin distinto a la ejecución del Contrato.
6. Responder ante el DNP y ante terceros por la divulgación indebida o el manejo inadecuado de la información entregada por la Entidad para el desarrollo de las actividades contratadas.
7. Mantener la debida confidencialidad de la información que pueda llegar a conocer durante la ejecución del contrato.
8. Responder a los reclamos, consultas y/o solicitudes de la Entidad, eficaz y oportunamente, de acuerdo con lo establecido en el anexo técnico
9. Recopilar y gestionar toda la información requerida para la ejecución del contrato.
10. Asistir a todas las reuniones convocadas por el Supervisor del contrato. Asimismo, les corresponde resolver los inconvenientes que se evidencien y presentar los informes requeridos, presencial y/o virtualmente, en los términos que establezca el supervisor.
11. Informar inmediatamente al Supervisor del Contrato, si durante la ejecución de este surgen hechos de fuerza mayor, o caso fortuito, o alguna situación que ocasionen dilaciones en la ejecución del contrato.

12. Colaborar con el DNP en lo que sea necesario para que el objeto contratado se cumpla y que éste sea de la mejor calidad.
13. Atender los requerimientos realizados por el Supervisor durante el desarrollo del contrato.
14. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando las dilaciones que pudieran presentarse.
15. Conocer y Aplicar los lineamientos establecidos en la política y propósitos del Sistema Integrado de Gestión (SIG).
16. Cumplir con las políticas del Sistema de Gestión de Seguridad de la Información de la Entidad, en las actividades donde el **CONTRATISTA** interactúe con cualquier activo de información (plataforma e infraestructura tecnológica) del DNP.
17. Aportar unos documentos (obligaciones en SST) previo inicio a la ejecución, de acuerdo con lo señalado en el Manual Operativo de SST del DNP y de conformidad con la normativa vigente, en el marco del contrato, y una vez remitidos al supervisor deberán allegarse al Grupo SST para su revisión.
18. Dar cumplimiento a la normatividad vigente relacionada con la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo, debiendo aportar al supervisor del DNP una certificación firmada por el representante legal o su delegado, que evidencien el compromiso con la seguridad y salud de sus colaboradores, así mismo aportar los soportes requeridos por Seguridad y Salud en el Trabajo del DNP[17].

**La certificación debe dar constancia de lo siguiente:**

a. Que cuenta con un Sistema de Gestión de Seguridad y en el Trabajo –SGSST.
b. Que cuenta con una Política en Seguridad y Salud en el Trabajo-SST.
c. Que da cumplimiento a la normativa aplicable en la realización de los exámenes ocupacionales al personal que labora y preocupacionales al personal que presta sus servicios para la empresa.
d. Que su equipo de trabajo se encuentre afiliado a la ARL.
e. Que cuenta con un programa de capacitación en SST para su equipo de trabajo
f. Que cuenta con una Matriz de identificación de los peligros prioritarios y control de los riesgos para su equipo de trabajo.
g. Que realiza la Autoevaluación y la calificación de los Estándares Mínimos de su SGSST en concordancia con la normatividad legal vigente.
h. Que reporta a su ARL e informa al GSST del DNP los accidentes de trabajo y enfermedades laborales que le ocurran a su equipo de trabajo en el cumplimiento del objeto contractual, así mismo realizará las investigaciones a que haya lugar para que el empleador o contratante ejerza las acciones de prevención y control que estén bajo su responsabilidad.
i. Que cumple y atiende todas las medidas sanitarias preventivas y correctivas para la protección de la salud y establecer las medidas de bioseguridad necesarias para la protección de sus colaboradores de conformidad con lo señalado en la legislación vigente y demás normas que la adicionen, modifiquen y sustituyan.
j. El Contratista garantiza que su equipo de trabajo cuente con todos los elementos e implementos de seguridad y salud, necesarios para garantizar la integridad del recurso humano.

[17] De acuerdo con el correo electrónico del 06 de abril de 2026 recibido por la Coordinadora del Grupo SST del DNP se indica: "De acuerdo con el documento Requisitos para la verificación de cumplimiento en seguridad y salud en el trabajo para proveedores y outsorsing que se encuentra publicado en la Rebeca en el siguiente enlace: https://colaboracion.dnp.gov.co/CDT/DNP/SIG/Botones%20de%20componentes/SST/Requisitos%20verificaci%c3%b3n%20cumplimiento%20SST%20para%20Proveedores%20y%20Outsourcing.pdf.".

k. El Contratista se compromete a velar por la seguridad y salud de su equipo de trabajo durante el desarrollo del Contrato.

**Deberá entregar en materia de Seguridad y Salud en el Trabajo lo siguiente:**

a. Copia de la Política en Seguridad y Salud en el Trabajo, firmada por el representante legal, que evidencie el compromiso con la seguridad y salud de sus colaboradores en misión.

b. Aportar previo inicio a la ejecución de las actividades un listado de los colaboradores que realizarán las actividades en el marco del contrato, donde se consignen por cada uno, los datos del grupo sanguíneo (RH), EPS y ARL a la que se encuentre afiliado, nombre y número de contacto en caso de emergencia y enfermedades preexistentes. Este listado deberá ser actualizado por el contratista conforme a las novedades por cambio de personal u otras variables (SI APLICA).
c. Asegurar la participación en la inducción del componente de SST del SIG del DNP de todos sus colaboradores, coordinada a través del supervisor del contrato con el GSST. En caso de rotación o cambio de personal el proveedor garantizará que el nuevo personal reciba la inducción (APLICA)
d. Aportar copia de la matriz de identificación de los peligros prioritarios y control de los riesgos de sus colaboradores. (SI APLICA)
e. Aportar copia del programa de capacitaciones en SST y enviar mensualmente los soportes de ejecución. (SI APLICA)
f. Aportar copia de la matriz de Elementos de Protección Personal y enviar mensualmente los soportes de entrega. (SI APLICA)
g. Aportar el soporte de la autoevaluación y calificación de los estándares mínimos de su SGSST en concordancia con la normatividad vigente.
h. Reportar a su ARL e informar al GSST del DNP los accidentes de trabajo - AT ocurridos a sus colaboradores en el cumplimiento del objeto contractual, así mismo realizará las investigaciones a que haya lugar de conformidad con la normativa vigente en SST contando con la presencia del GSST para que el empleador o contratante ejerza las acciones de prevención y control que estén bajo su responsabilidad. (Cuando se presente un AT).

**Nota 1**: De acuerdo con el tipo de servicio o producto a contratar en caso de que no requiera de la presencia del contratista en la entidad, el contratista podrá aportar solo la certificación firmada por la representante legal señalada dentro del manual.

**Nota 2**: En caso de que la modalidad a contratar no se encuentre señalada dentro de este manual, se procederá a revisar y validar estos requisitos con la Subdirección de Contratación de acuerdo con la normatividad vigente.

**Nota 3:** Las áreas que se encuentren adelantando procesos de contratación, durante la fase de elaboración de estudios previos, deben solicitar al GSST asesoría para que se incluyan estos requisitos; el Grupo de Contratación verifica la inclusión de estos requisitos en los estudios previos y contratos.

**19. En materia ambiental aplican las siguientes obligaciones:**

Atender los lineamientos establecidos por el componente de Gestión Ambiental del DNP, incluyendo las buenas prácticas para el ahorro y uso eficiente de los recursos naturales como agua, energía y papel, así como el manejo

integral de residuos sólidos. De igual forma, dar cumplimiento a la legislación ambiental vigente a nivel distrital y nacional aplicable al desarrollo del objeto contractual y toda aquella que sea expedida durante la ejecución del contrato.

### 13.5.3. Obligaciones Específicas:

1. Entregar todas las soluciones / equipos en los sitios/sedes indicadas por la entidad.
2. Instalar, Implementar, configurar y poner en marcha las soluciones de seguridad y conectividad ofertadas.
3. Realizar la instalación y configuración de los equipos con personal certificado por el fabricante con el cual se esté presentando.
4. Entregar todas las plataformas deberán ser de propósito específico, no se aceptan soluciones genéricas.
5. Dar soporte incluyendo atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas en horario Hábil y No Hábil por el tiempo contratado.
6. Entregar implementada y funcionando las soluciones completas, de acuerdo con los requerimientos y políticas.
7. Planear cada una de las actividades, validadas en conjunto con el DNP.
8. Realizar la configuración y alistamiento del software a la última versión estable aprobada por el fabricante para la plataforma.
9. Afinar y estabilizar las plataformas.
10. Realizar Pruebas de Servicio de las plataformas.
11. Entregar las plataformas a satisfacción al DNP.
12. Realizar Las actividades de afinamiento de las plataformas deberán ser realizadas por personal certificado por el fabricante.
13. Realizar pruebas / muestras de las plataformas donde se evidencie la correcta configuración y afinamiento de cada plataforma.
14. Garantizar soporte y garantía para las plataformas ofertadas en un esquema 7x24 por un (1) año, con soporte remoto por parte del fabricante
15. Dar soporte el cual debe incluir atención de incidentes sobre las plataformas ofertadas.
16. Atender Consultas a través de llamadas telefónicas, correo electrónico.
17. Realizar Sesiones remotas en horario Hábil y No Hábil. Todo con respecto a las plataformas ofertadas y objeto del presente contrato.

### 13.5.4 Obligaciones del DNP:

**a)** Aprobar la garantía de cumplimiento que ampara el contrato
**b)** Pagar el valor del contrato de acuerdo con los términos establecidos.
**c)** Ejercer el respectivo control en el cumplimiento del contrato y expedir el recibo a satisfacción, para tal efecto deberá designar al supervisor el control de ejecución, quien estará en permanente contacto con EL CONTRATISTA, para la coordinación de cualquier asunto que así lo requiera.
**d)** Suministrar AL CONTRATISTA la información necesaria para la ejecución del Contrato.
**e)** Brindar al CONTRATISTA los medios para que conozca los lineamientos y políticas del Sistema Integrado de Gestión.
**f)** Divulgar al contratista la política y propósitos del SIG que aplican en la ejecución del contrato, así como los procesos, riesgos, lineamientos, controles, requisitos y/o responsabilidades del SIG que le aplican en el desarrollo del contrato.
**g)** Seguir los procedimientos y canales definidos para la apertura y atención de incidentes.

**h)** El DNP deberá adelantar la liquidación del contrato, en caso de que aplique.

### 13.6 Supervisión

La supervisión de la ejecución y cumplimiento de las obligaciones contraídas por el contratista a favor del DNP, estará a cargo del Profesional Especializado Grado 22 del Grupo de Gestión de Infraestructura Tecnológica de la Oficina de Tecnología y Sistemas de Información, o de la persona que designe el Subdirector de Contratación, mediante memorando, de acuerdo con la solicitud de la dependencia.

Para esos efectos, el supervisor estará sujeto a lo dispuesto en el Numeral 1 del artículo 4 y Numeral 1 del artículo 26 de la Ley 80 de 1993, la Ley 1150 de 2007, la Ley 1474 de 2011, Resolución Interna 2671 de 2023, por medio de la cual se modificó el Manual de Contratación del DNP, Resolución 2888 de 2023 (Manual de interventoría) y las demás normas establecidas sobre la materia.

### 13.7 Liquidación

El presente contrato estará sujeto a liquidación, salvo disposición contraria, de conformidad con lo dispuesto en el artículo 60 de la Ley 80 DE 1993 (modificado por el ART. 217, Decreto 019 DE 2012), en el artículo 11 de la Ley 1150 de 2007.

### 13.8 Lugar de ejecución y domicilio contractual

Las actividades se desarrollarán en la ciudad de Bogotá D.C. El domicilio contractual es la ciudad de Bogotá, D.C.

### 13.9 Formatos de la propuesta

**El anexo 1 y 2.**

Firma:

BENAVIDES SANTACRUZ ORLANDO

Firmado digitalmente por BENAVIDES SANTACRUZ ORLANDO
Fecha: 2026.08.20 10:40:16 -05'00'

**ORLANDO BENAVIDES SANTACRUZ**
Jefe Oficina de Tecnologías y Sistemas de Información

Elaboró: Gustavo Saldana Osorio, Contratista Oficina de Tecnologías y Sistemas de Información de la OTSI
Revisó: Marisol Olivera Garrido, Abogada OTSI
Nilgen Vargas, profesional financiero de la OTSI

**ANEXO n.° 1**
**FICHA TÉCNICA**

| Descripción | Cantidad Licencias |
|---|---|
| Renovación y actualización (upgrade) del licenciamiento por suscripción de Trellix EDR for Endpoint en su edición Enterprise, con Business Software Support por un (1) año. La suscripción cubre hasta cinco (5) dispositivos asignados por usuario, incluyendo funcionalidades avanzadas de detección, investigación y respuesta extendida ante amenazas. | 2655 |
| Renovación de la licencia por suscripción Trellix Cloud Workload Security CWSE-S con Business Software Support por un (1) año en su edición Enterprise | 127 |
| Renovación de la licencia por suscripción Trellix Mobile Security Advanced con Business Software Support por un (1) año. Cubre hasta 5 dispositivos asignados por usuario en su edición Enterprise | 55 |
| Renovación de la licencia por suscripción Trellix Data Loss Prevention (DLP) con Business Software Support por un (1) año en su edición Enterprise | 2212 |
| Soporte, transferencia de conocimiento de acuerdo con lo requerido en el anexo técnico y con nivel Gold. | 1 |

| **CARACTERÍSTICAS MÍNIMAS REQUERIDAS** |
|---|
| El DNP requiere la renovación y Upgrade de componentes para la solución de seguridad de estaciones cliente, servidores, dispositivos móviles y prevención de fuga de información (DLP). La solución está compuesta por capacidades de protección, detección y respuesta extendida (antivirus + EDR) para servidores y estaciones cliente (institucionales y personales), mediante Trellix EDR for Endpoint en su edición Enterprise ; protección de cargas de trabajo en entornos virtualizados on-premise y en la nube, mediante Trellix Cloud Workload Security (CWSE); protección avanzada para dispositivos móviles, mediante Trellix Mobile Security Advanced; y capacidades de prevención de fuga de información, mediante Trellix Data Loss Prevention (DLP). |
| En el DNP la información no pública incluye información pública clasificada y reservada de la Ley 1712 de 2014, los datos personales (semiprivados, privados, reservados, sensibles, menores de edad) de la Ley 1581 de 2012, Ley 1266 de 2008 y el decreto 1377 de 2013 y la información con clasificación interna (Confidencial, Uso interno, Uso privado). La clasificación de la información está incluida en el M-PG-07 Manual Operativo de Seguridad de la información disponible en https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-PG-07%20%20Manual%20Operativo.Pu.pdf |
| La renovación y Upgrade de componentes para la solución de seguridad debe cumplir con:<br><br>● Protección para Múltiples Sistemas Operativos: Debe incluir protección de seguridad para Windows, macOS y Linux.<br>● Control de Dispositivos y Aplicaciones: La solución debe incorporar funcionalidades de control de dispositivos periféricos y control de aplicaciones para equipos de escritorio.<br>● Detección y Análisis Avanzado: Debe proporcionar un escáner de línea de comandos y acceso a una capacidad de análisis de amenazas en la nube para el envío automatizado de muestras. |

| |
|---|
| ● Inteligencia y Proactividad: Debe incluir un módulo de análisis predictivo y proactivo que permita la priorización de amenazas, la predicción del impacto de contramedidas y la sugerencia de mejoras.<br>● Acceso a Ecosistema de Socios: La solución debe permitir el despliegue de productos de socios tecnológicos estratégicos.<br>● Análisis Forense: Debe incluir un módulo para la recolección y el análisis automatizado de datos forenses de los endpoints, el cual puede ser un módulo completamente separado del de EDR o puede ser desplegado en un único módulo que tenga las cualidades de EDR más las forenses, con características únicas que se detallarán más adelante. |
| **Renovación de licencias** |
| Renovación y actualización (upgrade) del licenciamiento por suscripción de Trellix EDR for Endpoint en su edición Enterprise, con Business Software Support por un (1) año. La suscripción cubre hasta cinco (5) dispositivos asignados a cada usuario. Se requieren dos mil quinientas cincuenta y dos (2.655) licencias. |
| Renovación de la licencia por suscripción Trellix Cloud Workload Security CWSE-S con Business Software Support por un (1) año. Se requieren 127 licencias en su edición Enterprise |
| Renovación de la licencia por suscripción Trellix Mobile Security Advanced con Business Software Support por un (1) año. Cubre hasta 5 dispositivos asignados a los usuarios. Se requieren 55 licencias en su edición Enterprise |
| Renovación de la licencia por suscripción Trellix Data Loss Preventi on (DLP) con Business Software Support por un (1) año. Se requieren 2212 licencias en su edición Enterprise. |
| **Soporte, mantenimiento y garantía** |
| El contratista debe prestar el soporte con categoría Gold de fábrica para todas las licencias adquiridas y renovadas por un (1) año, contados a partir del perfeccionamiento y legalización del contrato. |
| El contratista debe prestar el soporte, mantenimiento y actualización del producto, en instalación, configuración y afinamiento prestado directamente por el fabricante por un (1) año contado a partir de la aprobación de la garantía. |
| El contratista debe brindar soporte técnico relacionado con la solución de inconvenientes específicos, presentados en la instalación y utilización de los productos de licencia, durante la vigencia del contrato de acuerdo con los tiempos de respuesta registrados en el documento de “Acuerdo de niveles de servicio” entregado al DNP. |
| Personal de Servicios Profesionales en Latinoamérica: El fabricante debe contar con al menos tres (3) personas de servicios profesionales permanentes para implementar la solución en la región de Latinoamérica.<br>No se aceptará personal tercerizado para estas funciones. En caso de no contar con este personal, se requerirá que el fabricante contrate personal permanente a su nombre para cumplir con este requisito. |
| El contratista debe prestar un servicio de atención técnica, a través del cual se recibirán los incidentes reportados por el DNP, en el que se deberá hacer un registro que incluya mínimo los datos de fecha, hora, descripción y número del incidente asignado, el cual se utilizará para identificar y hacer seguimiento al caso reportado, correspondiente al nivel de servicio ofrecido. |
| El contratista debe ofrecer soporte de primer nivel y el soporte de segundo nivel debe ser ofrecido por el fabricante con soporte telefónico 7x24x365 en idioma español |

| |
|---|
| El contratista debe prestar el soporte en sitio, telefónico, sesión virtual y por correo electrónico durante el tiempo de licenciamiento, por 24 horas del día los 7 días a la semana (7x24), cuantas veces se requiera por parte del supervisor del contrato o ante un incidente de la solución de seguridad de estaciones clientes, servidores, dispositivos móviles y DLP. El tiempo de respuesta inicial no debe superar las dos (2) horas contadas a partir de la comunicación del incidente, con máximo 4 horas para atención en sitio cuando no se haya solucionado el problema telefónicamente. Por incidente se entenderán todos los casos de fallas, mal funcionamiento, cambios en la configuración, anomalías que se presenten en los bienes y servicios adquiridos en el objeto contractual. En el evento en que dicho soporte sea escalado al fabricante, el contratista realizará acompañamiento técnico en las instalaciones del DNP con mínimo un ingeniero certificado por el fabricante Trellix, y un tiempo de respuesta máximo de cuatro (4) horas. Se dejará un acta de la visita como soporte de las actividades realizadas, correspondiente al nivel de servicio ofrecido. |
| Durante la vigencia del mantenimiento y soporte técnico: El contratista deberá revisar periódicamente e instalar las nuevas actualizaciones que sean liberadas por el fabricante, enviar al DNP la actualización de correcciones que se realicen a los productos, y asesorar al DNP en la solución de problemas específicos que se presenten en la instalación y utilización de los productos de licencia. |
| El contratista debe presentar al supervisor del contrato tarjeta profesional, certificado COPNIA, hoja de vida y certificaciones vigentes de los cursos aprobados de los diferentes productos de Trellix del Ingeniero del sistemas o ingeniero electrónico designado, objeto del desarrollo del objeto contractual. |
| El contratista debe hacer una sesión presencial o virtual cada mes (1) con un ingeniero certificado y previamente aprobado por el DNP, para verificar la correcta instalación, configuración y funcionamiento de la solución de seguridad de estaciones clientes, servidores, dispositivos móviles y DLP. Se debe entregar un informe con las recomendaciones respectivas de la visita o sesión virtual realizada. De acuerdo con estas recomendaciones se deben generar las acciones necesarias para gestionarlas, las visitas o sesiones virtuales no serán acumulables. Durante las visitas o sesiones debe hacerse transferencia de conocimiento al personal técnico del DNP en los casos que se requieran, correspondiente al nivel de servicio ofrecido. |
| El contratista debe revisar y probar el plan de contingencia definido para este servicio en conjunto con el DNP |
| El contratista debe revisar el estado actual del Software y documentar las recomendaciones y/o configuraciones iniciales a que haya lugar. |
| El contratista debe realizar la instalación, cambio o actualización de las versiones de la solución y parches de acuerdo con las últimas versiones liberadas por el fabricante. |
| El contratista debe ofrecer las nuevas versiones del producto, libres de costo adicional al DNP, a medida que sean liberadas por el fabricante, mientras el soporte esté vigente. Dicha instalación debe ser realizada por el contratista. |
| **Transferencia de conocimiento** |
| El contratista debe transferir el conocimiento técnico necesario para la administración de los productos de la solución adquirida. El contratista deberá especificar el temario, a realizarse de la siguiente manera: Durante la vigencia del licenciamiento, el número requerido será de mínimo 16 horas. En cualquier caso, el agendamiento se realizará previa comunicación y coordinación del sitio y hora de común acuerdo con el supervisor del contrato. |
| El contratista debe programar actividades encaminadas a la sensibilización y mitigación de riesgos en seguridad de la información, a los funcionarios del DNP, con duración de un (1) día anual en las instalaciones del DNP o sesiones virtuales durante la ejecución del Contrato, la logística será coordinada por el DNP, y el proponente enviará el cronograma de las actividades a realizar. |

| |
|---|
| El contratista debe informar periódicamente mediante correo electrónico a la OTSI sobre la aparición de nuevos virus informáticos, así como las recomendaciones y acciones a seguir cuando el fabricante del software no haya liberado la versión que detecta y elimina el nuevo virus. |
| **Características generales** |
| El contratista debe instalar, configurar y poner en funcionamiento de los productos de la solución adquirida en la plataforma del DNP (equipos y servidores), sin que ello implique algún costo adicional, e indicar las recomendaciones de hardware mínimo requerido para la instalación en la plataforma del DNP. Al Inicio del contrato se construirá en conjunto con el DNP el cronograma de las actividades a realizar. |
| El contratista debe realizar la implementación, despliegue, configuración y soporte de la solución según los requerimientos del DNP. |
| El contratista debe instalar y configurar la solución de seguridad de estaciones clientes, servidores, dispositivos móviles y DLP, debe ser instalada y/o configurada en servidores con sistema operativo Windows Server 2019 y versiones posteriores, incluyendo Windows Server 2022 y Windows Server 2025, y base datos Microsoft SQL 2019 o superior. |
| El contratista debe instalar y configurar la solución de seguridad de estaciones clientes, servidores, dispositivos móviles y modulo DLP debe ser instalada y configurada en un ambiente virtual en Microsoft Hyper-v. |
| El contratista debe entregar un documento que contenga los manuales de usuario y técnico en medio magnético, en idioma español y/o inglés de acuerdo con la solución de seguridad de estaciones clientes, servidores, dispositivos móviles,DLP, Sandbox y Forense. |
| El contratista debe esta registrado con la membresía mínima de **Gold** en el portal del fabricante, para avalar este cumplimento debe anexar una certificación por parte del fabricante no mayor a 30 días de expedida |
| **Características generales Consolas de administración** |
| la renovación y upgrade de componentes para la solución de seguridad debe cumplir con consolas de Administración y Gestión de la siguiente manera:<br><br>• **Consola de Gestión en la Nube**: Una plataforma de gestión alojada en la nube que **debe ser compatible** con la mayoría de las características del producto.<br>• **Consola de Gestión Local**: Una consola para despliegues en las instalaciones del cliente.<br>• **Consola de Gestión en IaaS**: Para entornos de infraestructura como servicio.<br>• **Consola Análisis forense**: Plataformas para el análisis forense y la investigación de incidentes en equipos on premise, en la nube y virtualizadas<br>• **Consola Plataforma de Intercambio de Inteligencia**: Un sistema para el intercambio de inteligencia de amenazas.<br><br>Las consolas deben tener una **Autenticación MFA y SSO**: La solución debe permitir y soportar integración OIDC/SAML y MFA para asegurar las sesiones de los administradores.<br>**Debe tener una Capa de Intercambio de Datos**: Un framework de comunicación para la orquestación y el intercambio de datos en tiempo real entre los productos de seguridad. |
| **Características técnicas del componente de antivirus (Trellix Enterprise EDR for Endpoint y Trellix Cloud Workload Security CWSE-S)** |
| El componente antivirus debe permitir la protección de equipos de escritorio, estaciones de trabajo, servidores físicos, virtuales configurados en Hyper-V (stand Alone y en clúster) |

| |
|---|
| El componente antivirus debe ser compatible con cluster shared volumen de Microsoft |
| El componente antivirus debe ofrecer protección Antivirus para equipos con sistemas operativos Windows y Linux |
| El componente antivirus debe ofrecer protección para servidores con sistema operativo Linux (Centos y Ubuntu) |
| El componente antivirus debe permitir el cambio del sistema operativo de los servidores y estaciones cliente sin necesidad de adquirir un nuevo paquete o licencia. |
| El componente antivirus debe contar con un módulo de protección en tiempo real, el cual ofrezca protección continua frente a los virus que llegan a través de medios extraíbles, red, correo electrónico y diversas fuentes en Internet. |
| El componente antivirus debe permitir ocultar el icono en la barra de tareas. |
| El componente antivirus debe permitir establecer una contraseña de seguridad para todo el sistema antivirus. |
| El componente antivirus debe tener la capacidad de poder configurar procesos de alto riesgo, bajo riesgo y procesos predeterminados, generando distintas propiedades de exploración de virus para los diferentes tipos de procesos en estaciones y servidores. |
| El componente antivirus debe contar con un módulo que permita iniciar una exploración en cualquier momento, especificar los objetivos de análisis (discos duros, carpetas, memoria, mi PC, todas las unidades locales, todos los medios extraíbles, todas las unidades de red, la carpeta principal del usuario y las carpetas de perfil del usuario) y las exclusiones de la exploración, así como también determinar cómo debe responder el explorador cuando detecte un virus y ver informes detallados. |
| El componente antivirus debe permitir controlar el uso de la CPU para tareas de exploración en demanda. |
| El componente antivirus debe contar con un componente que permita explorar mensajes, archivos adjuntos y carpetas públicas a las que se tenga acceso en Microsoft Outlook 365 directamente sobre la estación de trabajo. |
| El componente antivirus debe permitir analizar el contenido de carpetas personales de correo Microsoft Outlook 365 almacenadas localmente, los archivos PST deben ser revisados en tiempo real y/o por demanda. |
| El componente antivirus debe ser configurable la acción a tomar ante la detección de virus, tales como: preguntar al usuario, limpiar, borrar, denegar acceso, e inclusive manejar carpeta de cuarentena para archivos infectados. |
| El componente antivirus debe tener la capacidad de configurar una segunda opción en caso de que la primera acción falle. |
| El componente antivirus debe proteger puertos, archivos, carpetas y recursos compartidos de intrusos restringiendo el acceso a ellos. |
| El componente antivirus debe permitir crear reglas para bloquear tráfico entrante y saliente por puertos específicos |
| El componente antivirus debe permitir crear reglas para restringir el acceso a recursos compartidos, carpetas o archivos. |
| El componente antivirus debe prevenir accesos de lectura o escritura a archivos, carpetas o recursos compartidos configurados, debe avisar, bloquear los intentos de acceso o bloquear y reportar los intentos de acceso. |
| El componente antivirus debe contar con un módulo de detección en tiempo real, en caso de un ataque debe mostrar la dirección IP del origen del ataque. |
| El componente antivirus debe permitir el bloqueo de las conexiones de máquinas remotas que estén infectadas y tratando de atacar un recurso compartido, debe permitir especificar cuánto tiempo estará bloqueado ese recurso para esa máquina remota. |

| |
|---|
| El componente antivirus debe permitir la exploración de los distintos tipos de lenguajes de scripting, tales como JScript (archivos .JS y .JSE), VBScript (archivos .VBS y .VBE), WSF- Windows File (permite combinar diferentes lenguajes scripting en un solo archivo, entre ellos Tcl, Perl, Python, Kixtart, Object REXX), ActionScript (Flash) y JavaScript antes de que sean ejecutados, interceptando la ejecución antes de que el script llegue al componente de Microsoft Windows Script Host. |
| El componente antivirus debe contar con un módulo independiente el cual permita bloquear explotaciones de desbordamiento de Buffer ejecutando código malicioso en el computador, este módulo debe trabajar en modo de aviso y en modo de protección. |
| El componente antivirus debe tener la capacidad de detectar los programas no deseados (adware), spyware, password crackers, entre otros, herramientas de administración remota, dialers y bromas. La solución debe tomar las siguientes acciones: detectar, limpiar, denegar el acceso a los archivos, permitir el acceso a los archivos, eliminar los archivos y mover los archivos. |
| El componente antivirus debe contar con la tecnología de análisis, detección y eliminación para evitar activación y propagación de virus, ransomware, macros, troyanos, gusanos, spyware, keylogger, programas publicitarios, rootkits, phishing y cualquier tipo de programa malicioso que afecte la seguridad de la información. |
| El componente antivirus debe permitir la actualización de las firmas de virus, el motor de exploración, actualizaciones de producto, hotfixes, parches, o service packs entre otros. |
| La solución debe mantener actualizados los equipos que salgan de las instalaciones corporativas y que se conecten a Internet desde otras locaciones, sin necesidad de reconfigurar localmente el cliente de antivirus. |
| El componente antivirus debe permitir la personalización de los programas de instalación del software antivirus, de manera que se pueda crear un solo paquete de instalación el cual contenga el último motor de exploración y las últimas definiciones, también permitir la personalización de la configuración y componentes del antivirus, para ser distribuidos de manera masiva. |
| El componente antivirus debe detectar y mitigar ataques de día cero. |
| El componente antivirus debe ser compatible con la plataforma tecnológica del DNP. |
| El componente antivirus debe contar con una consola que permita a uno o más administradores la gestión, configuración centralizada de las directivas de seguridad para mantener el antivirus actualizado en todos los equipos y servidores de la Entidad |
| El componente antivirus debe soportar “rollback” de actualizaciones evitando corrupción del sistema operativo donde fue instalado. |
| El componente antivirus debe permitir la integración con herramientas con el módulo EDR (Endpoint Detection and Response) |
| La consola de administración del componente antivirus debe contar con la capacidad de descargar las actualizaciones desde Internet a través de los protocolos FTP y HTTP, colocándolas en repositorios distribuidos para que los clientes las tomen de estas ubicaciones. |
| La consola de administración del componente antivirus debe contar con la capacidad de administrar, forzar políticas centralizada y directamente a los productos instalados en los equipos, servidores, incluyendo los servidores en la nube. Involucrando configuración, programación de tareas exploración, tareas de actualización, configuración de la exploración en tiempo real, determinación de acciones ante la detección de un virus y alertas de todas la estaciones y servidores. |
| La consola de administración del componente antivirus debe contar con un motor generador de informes que permitan realizar un seguimiento del funcionamiento de las políticas de antivirus en la organización. |

| |
|---|
| La consola de administración del componente antivirus debe permitir a los administradores de seguridad la capacidad de clasificar las máquinas de acuerdo con direcciones IP, creando grupos y asignando rangos de IP a ellos. |
| La consola de administración del componente antivirus debe contar con la capacidad de integrarse al directorio activo y heredar los grupos y esquemas de red de Microsoft Windows. |
| La consola de administración del componente antivirus debe ofrecer mínimo 30 reportes gráficos en tiempo real que reflejen la situación de los equipos incluidos en la consola de administración, los reportes deben incluir información sobre infecciones, cubrimiento y tendencias |
| La consola de administración del componente antivirus debe permitir la generación de reportes de infecciones debe indicar cuáles virus se han detectado, archivos implicados, fecha y hora, en que máquinas y las acciones que tomó el producto (borrado, limpiado, movido, etc.) |
| La consola de administración del componente antivirus debe permitir la generación de reportes de cubrimiento debe indicar la visibilidad del grado de actualización y uso de versiones de productos de toda la red, de tal forma que se minimice la aparición de brotes de virus por máquina sin actualizar o desprotegidas. |
| La consola de administración del componente antivirus debe permitir la generación de reportes de tendencia con datos históricos. |
| La consola de administración del componente antivirus debe permitir la generación de reportes gráficos donde se pueda observar que máquinas no tienen el producto instalado. |
| La consola de administración del componente antivirus debe permitir la generación de reportes de auditoría, en los cuales se pueda observar que inicios de sesión se han realizado, adición, eliminación de equipos, cambios de contraseñas y cambios de política |
| La consola de administración del componente antivirus debe permitir la generación de reportes del inventario de las estaciones que cuentan con el servicio del antivirus. |
| La consola de administración del componente antivirus debe permitir la generación de reportes que indiquen el sistema operativo del equipo y/o servidor, mostrar si se encuentra actualizado |
| La consola de administración del componente antivirus debe indicar qué parches se requieren en el sistema operativo anfitrión antes de aplicar el parche del producto. |
| La consola de administración de antivirus debe permitir que el administrador del sistema pueda crear múltiples perfiles administrativos de acceso a la consola, tales como administradores totales, administradores de sitios definidos o solamente revisores por sitios sin privilegios administrativos. |
| La consola de administración de antivirus debe contar con la capacidad de detectar sistemas no fiables, sistemas no gestionados que se activan en la red, de modo que pueda desplegar un agente en dichos sistemas, distribuirles el componente antivirus y aplicarles directivas. |
| La consola de administración de antivirus debe permitir la identificación en qué punto de la red está ingresando el virus. |
| La consola de administración de antivirus debe permitir la instalación desde ésta los cambios de versión para equipos y servidores. |
| La consola de administración de antivirus debe permitir instalar, desinstalar y programar escaneos de virus a partir de una sola estación o por grupos pudiendo programarlos por fecha y hora. |
| La consola de administración de antivirus debe permitir la generación de políticas de protección por sitios, dominios, grupos, y máquinas específicas. |

| |
|---|
| La consola de administración de antivirus debe tener la capacidad de distribuir automáticamente las actualizaciones de las definiciones de virus, motor de exploración, Service packs, definiciones de emergencia y hotfixes de los productos antivirus |
| La consola de administración de antivirus debe permitir llevar a cuarentena los archivos o adjuntos a una carpeta y generar el tiquete vía correo electrónico al usuario configurado para tal fin para recuperar el archivo. |
| La consola de administración de antivirus debe contar con la opción de administrar las notificaciones para mantener informado a los administradores de todos los eventos con alertas personalizables |
| **Características técnicas del componente Trellix Enterprise EDR for Endpoint** |
| La solución de EDR debe contar con inspección avanzada mediante Inteligencia Artificial (Machine Learning). |
| La solución de EDR debe contar con la funcionalidad específica diseñada para inspeccionar archivos y actividad sospechosa con el fin de detectar patrones maliciosos mediante el uso de técnicas de “Machine Learning”. |
| La solución de EDR debe tener dos modos de análisis: en la nube y en el cliente, dependiendo de la conectividad de los equipos. |
| La solución de EDR debe recolectar información de los atributos de los archivos y su comportamiento para realizar el análisis. |
| La solución de EDR debe tener la capacidad de detectar y tomar acción sobre amenazas "file-less" |
| La solución de EDR debe tener la capacidad de realizar acciones de remediación y rollback ante ataques |
| La solución de EDR debe contar con la capacidad de integrarse y recibir actualizaciones de reputación de un sistema de inteligencia contra amenazas mediante el uso de protocolo abierto de comunicación diseñado específicamente para esta finalidad, con la capacidad de actualizar todas las máquinas del ambiente en tiempo real, sin necesidad de actualizar políticas o comunicarse con la consola de administración. |
| La solución de EDR debe contar con contención dinámica de aplicaciones. |
| La solución de EDR debe permitir seleccionar que aplicaciones con una reputación específica deben ser ejecutadas en modo “contenido”, es decir que esta funcionalidad no le permitirá realizar ciertas acciones que hayan sido consideradas como maliciosas dentro del sistema operativo. |
| La solución de EDR debe permitir la configuración de acciones o de bloqueo o registro según su configuración. |
| La solución de EDR debe contar con la capacidad de integrarse y recibir actualizaciones de reputación de un sistema de inteligencia contra amenazas mediante el uso de protocolo abierto de comunicación diseñado específicamente para esta finalidad, con la capacidad de actualizar todas las máquinas del ambiente en tiempo real, sin necesidad de actualizar políticas o comunicarse con la consola de administración. |
| La solución de EDR debe permitir la ejecución de las aplicaciones potencialmente maliciosas permitiéndoles la ejecución dentro del ambiente (punto final), mientras que limita los cambios en el sistema operativo que esta puede realizar. |
| La solución de EDR debe estar basada en reglas de comportamiento configurables tanto desde la consola cliente como la consola central. |
| La solución de EDR debe permitir la liberación de una aplicación contenida mediante el cambio en la reputación dentro del sistema de inteligencia contra amenazas y la exclusión de las políticas. |
| La solución de EDR debe contar con tecnología de inteligencia de amenazas. |
| La solución de EDR debe permitir la generación una infraestructura colaborativa entre puntos de protección ya sea a nivel perimetral, contenido, virtual o en los equipos de usuario final puedan intercambiar información sobre nuevas amenazas detectadas en tiempo real mediante un protocolo abierto diseñado para este propósito. |

| |
|---|
| La solución de EDR debe permitir la configuración de la reputación de los archivos localmente (de forma manual o a través de reglas de comportamiento) y mediante distintas fuentes de reputación dentro de la infraestructura de seguridad como: Sandbox y Proxys Web). |
| La solución de EDR debe permitir la asignación diferentes niveles de reputación a aplicaciones y certificados que se ejecutan en un ambiente con un punto de análisis a nivel local, la difusión de esta asignación debe realizarse en tiempo real mediante un protocolo diseñado para este propósito sin requerir que los agentes realicen un proceso de actualización firmas o configuraciones. |
| La solución de EDR debe permitir la asignación de diferentes niveles de reputación de un archivo ejecutable comunicándolo al resto de los equipos de usuarios finales con el objetivo de crear una inteligencia de seguridad en la red. |
| La solución de EDR debe permitir que la comunicación de los eventos se realice en tiempo real mediante el protocolo de comunicación diseñado para este fin, no debe depender de los ciclos de actualización de eventos a la consola central ni del "llamado/despertar de agentes". |
| La solución de EDR debe permitir la integración con el componente antivirus, control de aplicativos y/o control de cambios. |
| La solución de EDR debe ser capaz de utilizar IA generativa para hiper-automatizar las tareas de EDR. |
| La solución de EDR debe ayudar a los analistas de seguridad a gestionar la fatiga por alertas y a cerrar las brechas de talento. |
| La solución de EDR debe mejorar la eficiencia en la triaje, el alcance y el análisis de las alertas de amenazas |
| La solución de EDR debe tener un motor de consulta en lenguaje natural para búsquedas históricas y en tiempo real. |
| La solución de EDR debe incluir un modo interactivo para la búsqueda guiada de amenazas. |
| La solución de EDR debe proporcionar guías de remediación automatizadas. |
| La solución de EDR debe generar resúmenes ejecutivos de incidentes con un solo clic. |
| **Características técnicas del componente Trellix Control de Aplicaciones** |
| Debe ser capaz de evitar que se ejecuten archivos ejecutables no autorizados en los endpoints corporativos |
| Debe tener la capacidad de crear dinámicamente listas blancas (whitelists) de aplicaciones de confianza. |
| Debe tener la capacidad de crear dinámicamente listas blancas (whitelists) de aplicaciones de confianza. |
| Debe poder proteger archivos y entradas de registro críticos para evitar cambios no deseados en el sistema. |
| Debe permitir el monitoreo, detección y bloqueo de scripts sospechosos usando la interfaz AMSI y generar alertas cuando scripts maliciosos son encontrados. |
| Debe soportar los siguientes sistemas operativos de escritorio como mínimo: Windows 11 y Windows 10.<br>○ macOS Sonoma (14.x), mac OS Ventura (13.x) y macOS Monterey (12.x). |
| **Características técnicas del componente Trellix Control de Dispositivos** |
| Debe permitir la aplicación de políticas para controlar la transferencia de datos hacia y desde estos dispositivos. |
| Debe tener la capacidad de clasificar datos y aplicar controles basados en dicha clasificación. |
| Debe poder restringir dispositivos según el tipo, el proveedor o el número de serie. |
| Debe proporcionar un registro detallado de las transferencias de datos. |
| Debe permitir la gestión centralizada de las políticas de control de dispositivos. |

| Características técnicas del componente Trellix Sandbox en la Nube (Cloud Sandbox) incluido: |
|---|
| La solución debe realizar un análisis dinámico y en profundidad de archivos sospechosos utilizando un entorno de sanboxing en la nube para detonar las muestras de forma segura. |
| La solución debe enviar automáticamente las muestras de archivos potencialmente maliciosos al servicio de sandbox en la nube, sin requerir intervención del usuario o administrador. |
| La solución debe ejecutar el análisis de comportamiento de los archivos enviados al sandbox en tiempo real para determinar rápidamente su nivel de amenaza. |
| La solución debe procesar los envíos a sandbox mediante flujos automatizados, no soportando ni dependiendo de la funcionalidad de envío manual de muestras por parte del operador. |
| La solución debe permitir configurar un límite de tamaño máximo de archivo (ej. 5 MB) para las muestras binarias que se envían automáticamente al entorno de sandboxing. |
| La solución debe generar un reporte de análisis de sandbox que incluya una puntuación de riesgo numérica o de severidad y detalles de convicción sobre el archivo detonado. |
| La solución debe permitir la descarga de los Indicadores de Compromiso (IOCs) resultantes de la detonación en el sandbox, condicionado a que la puntuación de riesgo alcance un umbral determinado. |
| La solución debe consultar de forma previa una caché de reputación local en el agente o servidor perimetral antes de enviar una muestra desconocida al sandbox, evitando cargas redundantes de red. |
| **Características técnicas del componente Trellix Inteligencia e Intercambio de Amenazas** |
| Debe proporcionar una biblioteca de inteligencia de amenazas para priorizar las amenazas. |
| Debe ser capaz de correlacionar vulnerabilidades, campañas de amenazas y contramedidas defensivas. |
| Debe ser capaz de correlacionar vulnerabilidades, campañas de amenazas y contramedidas defensivas. |
| Debe poder predecir el impacto de las amenazas y de las contramedidas. |
| Debe sugerir mejoras prescriptivas para cerrar brechas de seguridad. |
| Debe utilizar un motor de análisis de comportamiento para predecir las campañas de amenazas. |
| Debe proporcionar protección proactiva contra amenazas |
| Debe ser capaz de correlacionar datos de inteligencia, información de vulnerabilidades y datos del entorno del cliente |
| Debe ayudar a priorizar las amenazas identificando las que se dirigen activamente a la organización. |
| Debe ofrecer una puntuación de riesgo completa para determinar qué amenazas abordar primero. |
| Debe proporcionar recomendaciones accionables para mitigar las amenazas y cerrar brechas de seguridad |
| Debe proporcionar inteligencia de amenazas a partir de una telemetría de amenazas global. |
| Debe utilizar un motor de análisis de amenazas para identificar actores maliciosos y nuevas campañas de ataque. |
| Debe proporcionar datos contextuales enriquecidos para la toma de decisiones. |
| La inteligencia debe ser actualizada de forma continua. |
| Debe permitir la priorización de las amenazas más críticas |
| Debe ofrecer dashboards personalizables. |
| Debe ser capaz de correlacionar datos de vulnerabilidades, amenazas y riesgos. |
| **Características técnicas del componente Trellix Análisis Forense:** |

| |
|---|
| La solución debe proporcionar la capacidad de obtener una imagen cruda (Raw Disk) completa o parcial del disco físico del endpoint remoto para análisis pericial en profundidad. |
| La solución debe permitir solicitar el volcado completo de la memoria física del endpoint remoto (Full Memory) para investigaciones avanzadas de malware residente. |
| La solución debe ser capaz de adquirir el volcado de memoria exclusivamente de un proceso en ejecución específico, referenciado por su Identificador (PID) o nombre. |
| La solución debe permitir la recolección de porciones de memoria específicas correspondientes a un controlador (driver) del sistema para investigar amenazas a nivel del kernel (Rootkits). |
| La solución debe proveer una función para recopilar un paquete de Triage estándar que incluya información del sistema, actividad de procesos, archivos, conexiones de red y registros (registry) en el momento del incidente. |
| La solución debe permitir focalizar la recolección de datos de Triage especificando una marca de tiempo temporal (Timestamp), capturando eventos ocurridos momentos antes y después de dicho evento. |
| La solución debe permitir la recolección masiva o múltiple de archivos forenses utilizando filtros de expresiones regulares (Regex) sobre rutas específicas del disco. |
| La solución debe permitir realizar recolecciones de archivos en modo crudo (RAW Mode) saltando las APIs del sistema operativo para capturar archivos bloqueados o eliminados. |
| La solución debe incorporar herramientas para crear y editar scripts de Triage personalizados, permitiendo incluir o excluir módulos de auditoría según los requerimientos de la investigación para reducir el volumen de datos. |
| La solución debe posibilitar la ejecución de consultas y barridos distribuidos en tiempo real sobre los endpoints conectados para localizar procesos activos, conexiones o valores de registro. |
| La solución debe poseer la capacidad de interrogar bases de datos periciales históricas almacenadas para rastrear la actividad pasada de un archivo o proceso, sin depender de la conectividad actual del endpoint. |
| La solución debe permitir una búsqueda profunda o "Exhaustiva" a través de todo el entorno corporativo forzando el escaneo completo de archivos o registros saltándose optimizaciones rápidas. |
| La solución debe reconstruir cadenas de ataque mediante el rastreo y graficado de las relaciones jerárquicas padre-hijo desde un proceso sospechoso hacia su origen. |
| La solución debe capturar, reconstruir y correlacionar los eventos de autenticación y uso de cuentas para detectar movimientos laterales e inicios de sesión anómalos. |
| La solución debe integrar visores analíticos internos (Audit/Triage Viewer) para procesar y presentar la telemetría adquirida organizándola por líneas de tiempo, procesos, servicios y modificaciones al sistema. |
| La solución debe proveer un gráfico de trazabilidad secuencial (Trace/Story Graph) que represente cronológica y visualmente los eventos de la alerta, mostrando nodos de archivos, procesos, conexiones de inyecciones de memoria. |
| La solución debe posibilitar la exportación del paquete de evidencia recolectado (Triage o volcado de memoria) en un formato pericial estructurado (ej. .mans o .zip) para su escrutinio detallado en herramientas especializadas de análisis offline. |
| La solución debe proveer un software instalable y administrable íntegramente dentro de los servidores e infraestructura física o virtual del cliente (on-premise) para orquestar agentes y adquirir evidencias sin depender de consolas en la nube. |
| La solución debe facultar a los administradores para borrar remotamente los datos y cachés forenses adquiridos almacenados en la consola, a fin de liberar espacio de almacenamiento. |
| La solución debe permitir la configuración de un límite máximo de almacenamiento en el disco local del agente (en Megabytes) utilizado para alojar la telemetría histórica del endpoint; reciclando registros antiguos cuando se alcance el tope. |

| |
|---|
| La solución debe soportar la adquisición remota de diagnósticos de estado y registros del agente de seguridad desplegado para propósitos de soporte técnico o solución de problemas periciales. |
| La solución debe considerar las tareas de aislamiento de host o contención como máxima prioridad en el encolamiento de acciones en el servidor, sobreponiéndose y pausando extracciones masivas forenses en progreso. |
| **Características técnicas del componente Trellix Mobile Security Advanced** |
| El componente de protección avanzada para dispositivos móviles debe permitir la protección de dispositivos móviles sin necesidad de desplegar componentes on-premises. |
| El componente de protección avanzada para dispositivos móviles debe integrarse como un módulo de la consola de administración de la solución de protección de Endpoint de la Entidad. |
| El componente de protección avanzada para dispositivos móviles debe entregar la siguiente información sobre los dispositivos móviles: vulnerabilidades, riesgo de aplicaciones, usuario asociado al dispositivo, sistema operativo, estado de configuración, estado de sistema operativo (actualizable y/o vulnerable). |
| El componente de protección avanzada para dispositivos móviles debe colectar la siguiente información en sus eventos: vector (dispositivo, red, aplicación), usuario, ubicación en donde ocurrió el evento, detalle de amenaza de red (wifi conectado, direcciones IP asociadas, redes wifi-cercanas), detalle de amenaza de aplicación (riesgos de privacidad y seguridad) |
| El componente de protección avanzada para dispositivos móviles debe ser compatible con sistemas operativos Android y Apple iOS, incluyendo teléfonos y tabletas de ambos sistemas operativos. |
| El componente de protección avanzada para dispositivos móviles debe permitir la protección de sistemas operativos Chromebooks |
| El componente de protección avanzada para dispositivos móviles debe permitir la integración con soluciones de SIEM vía Syslog |
| El componente de protección avanzada para dispositivos móviles debe permitir controlar la información colectada sobre los eventos de amenazas, con el propósito de gestionar el nivel de privacidad de los usuarios finales de acuerdo con las políticas BYOD definidas en la Entidad. |
| El componente de protección avanzada para dispositivos móviles debe permitir la gestión centralizada desde una misma consola |
| El componente de protección avanzada para dispositivos móviles debe detectar amenazas |
| El componente de protección avanzada para dispositivos móviles debe analizar las amenazas en el dispositivo, garantizando que el mismo esté protegido aun estando offline o en modo avión |
| El componente de protección avanzada para dispositivos móviles debe utilizar mecanismos de inteligencia artificial para la detección de amenazas |
| El componente de protección avanzada para dispositivos móviles debe tomar acción en cuanto a amenazas basadas en el – dispositivo, red y aplicaciones |
| El componente de protección avanzada para dispositivos móviles debe tener la capacidad de crear políticas de aplicaciones, desde la cual permita perfilar las aplicaciones de acuerdo con los permisos y accesos que tienen en el dispositivo móvil, para luego marcarlas fuera de cumplimiento o definir una lista blanca/lista negra. |
| El componente de protección avanzada para dispositivos móviles debe tener la capacidad de detectar la navegación a sitios web maliciosos y phishing. |
| El componente de protección avanzada para dispositivos móviles debe entregar funcionalidades de sandboxing en la nube, la cual entrega resultados sobre los riesgos de privacidad y seguridad que pueden tener las aplicaciones móviles. |

| |
|---|
| El componente de protección avanzada para dispositivos móviles debe contar con funcionalidades de sandboxing para permitir que el usuario administrador pueda someter aplicaciones de manera manual, y entregar reportes ejecutivos y técnicos con los hallazgos. |
| El componente de protección avanzada para dispositivos móviles debe permitir tomar las siguientes acciones en torno a las amenazas detectadas como bloqueo y desconexión de bluetooth o wifi, bloqueo de conexiones de red (sinkhole), terminar un proceso |
| El componente de protección avanzada para dispositivos móviles debe permitir la configuración de reglas de comportamiento desde la consola central |
| El componente de protección avanzada para dispositivos móviles debe incluir análisis de amenazas avanzadas, incluyendo análisis con algoritmos de Machine Learning identificando indicadores de compromiso en el dispositivo, aplicaciones y por conexiones de red. |
| El componente de protección avanzada para dispositivos móviles debe permitir detectar amenazas basadas en la red, cono ataques tipo man-in-the-middle (mitm). |
| El componente de protección avanzada para dispositivos móviles debe detectar y tomar acciones de actualización para dispositivos con sistemas operativos desactualizados. |
| El componente de protección avanzada para dispositivos móviles debe contar con la capacidad de detectar vulnerabilidades del sistema operativo |
| El componente de protección avanzada para dispositivos móviles debe ofrecer análisis avanzado de aplicaciones para evaluar el riesgo de privacidad y seguridad de las aplicaciones iOS y Android, esta evaluación de riesgos móviles deberá estar basada en la nube, diseñada para analizar rigurosamente aplicaciones utilizando al menos 20 motores únicos y altamente analíticos, que incluyan análisis estático y dinámico. |
| El componente de protección avanzada para dispositivos móviles debe contar con la capacidad de configurar reacciones a las amenazas detectadas (amenaza por amenaza y por grupo de dispositivos), tanto directamente en el dispositivo como a través de la consola de administración. |
| El componente de protección avanzada para dispositivos móviles debe contar con la capacidad de modificar la forma en que se abordan amenazas específicas para distintos grupos de dispositivos, lo que brinda la flexibilidad de responder adecuadamente dada la postura de riesgo asociada con un dispositivo. Por ejemplo, las amenazas detectadas en el dispositivo de un ejecutivo y aquellas detectadas en un dispositivo de administrador de TI pueden abordarse de manera diferente |
| El componente de protección avanzada para dispositivos móviles debe ser una aplicación disponible en Apple App Store y Google Play Store. El componente de protección avanzada para dispositivos móviles se instala como una aplicación normal y no debe requerir privilegios de administrador. El componente de protección avanzada para dispositivos móviles no debe realizar cambios de configuración en el dispositivo para brindar su protección. |
| El componente de protección avanzada para dispositivos móviles debe contar con una consola de la solución móvil permite personalizar y configurar las alertas de usuario de la solución en varios idiomas para que, cuando se detecte una amenaza en el dispositivo, los mensajes de detección de amenazas se presenten al usuario en su propio idioma. |
| El componente de protección avanzada para dispositivos móviles debe permitir a los administradores recibir notificaciones por correo electrónico sobre cualquier detección de amenaza en el momento de la detección a través de la consola central |
| El componente de protección avanzada para dispositivos móviles debe contar con la capacidad de configuración de la consola para que no contenga datos que permitan al administrador remitir los eventos de amenaza a un usuario físico o a una persona física, ya que los datos pueden ofuscarse cuando se sincronizan desde la consola de la solución y solo se utilizan los ID de los dispositivos de la solución móvil para identificar un dispositivo. |

| Características técnicas del componente de antivirus para servidores (Cloud Workload Security CWSE-S, Trellix Enterprise EDR for Endpoint) |
|---|
| El componente antivirus para servidores debe proteger servidores Windows y Linux, con agente personalizable, y configuración de excepciones propias del ambiente de servidor |
| El componente antivirus para servidores debe contar con la capacidad de gestión desde la consola centralizada, así el servidor se encuentre en ambiente de virtualización, on-premise o nube (Azure, AWS) |
| El componente antivirus para servidores debe permitir la configuración de políticas de seguridad que incluyen configuración de puertos de Firewall no seguros. |
| El componente antivirus para servidores debe contar con la capacidad de optimización del escaneo en ambientes virtuales en Microsoft Hyper-V, teniendo como opción el uso con o sin agente en cada servidor |
| El componente antivirus para servidores debe contar con la capacidad de administración de políticas de grupos dando visibilidad del ambiente físico, virtual y en nube. |
| **Características técnicas del componente Trellix Data Loss Prevention (DLP)** |
| El componente DLP para Endpoint debe ser proporcionado por el fabricante Trellix, asegurando que el soporte y la funcionalidad estén completamente integrados y administrados a través de mínimo una consola a máximo cuatro consolas. |
| El componente DLP debe ofrecer capacidades de clasificación de datos, cifrado, monitoreo y bloqueo para proteger la información crítica. |
| El componente DLP debe contar con una interfaz de monitoreo y un panel para el manejo de incidentes, separado de un panel para eventos operacionales, donde se muestren eventos administrativos. |
| El componente DLP debe monitorear el contenido que atraviese el Endpoint a través de puertos de entrada/salida como: Bluetooth, LPT, USB, etc. |
| El componente DLP debe identificar contenidos basados en tipo de contenido/documento. |
| El componente DLP debe colocar etiquetas(taggeo) de la información para su posterior rastreo y comparación, usando mecanismos que no incrementen la latencia en la inspección. Por ejemplo, usando GUIDs asociados a la metadata de los archivos. |
| El componente DLP debe monitorear el contenido que atraviese el Endpoint, por dirección IP y protocolo. |
| El componente DLP debe permitir la clasificación y orden se los documentos para que los usuarios realicen la clasificación manual de los documentos de manera fácil desde las aplicaciones de Office, como Word, Excel y PowerPoint, de acuerdo con las marcas definidas a través de la consola de administración central. La clasificación manual debe ser parte integral de la solución, sin depender de complementos o software de terceros. |
| El componente DLP debe permitir el etiquetado y protección de documentos según su origen, evitando la copia y filtración de información desde aplicaciones web, aplicaciones de red y recursos compartidos de red. |
| El componente DLP debe proporcionar informes y paneles de control que permitan verificar el cumplimiento de normas y políticas de seguridad |
| El componente DLP debe permitir la concienciación del usuario a través de alertas basadas en políticas institucionales |

| |
|---|
| El componente DLP debe permitir la personalización de mensajes de notificación al usuario, incluyendo el logotipo institucional y texto personalizado, para cada regla aplicada. |
| El componente DLP debe permitir la aplicación de estándares de cumplimiento que aborden las acciones cotidianas de los usuarios, como enviar correos electrónicos, publicar en la web o en la nube, y copiar archivos en dispositivos extraíbles. |
| El componente DLP debe utilizar técnicas avanzadas marcar y clasificar los documentos no públicos |
| El componente DLP debe tener integración con herramientas de administración de derechos, como Microsoft Windows Rights Management Service. |
| El componente DLP debe permitir el control de los datos en uso, a través de agentes instalados, para controlar acciones del usuario relacionadas con copiar información, imprimir archivos clasificados y captura de pantalla basada en datos sensibles, permitiendo la realización de la captura de pantalla de la aplicación si no contiene información clasificada |
| El componente DLP debe poder identificar contenido usando expresiones regulares, palabras clave, las funciones hash, y la coincidencia de patrones. |
| El componente DLP debe poder identificar el contenido basado en localización y usando la huella digital de documentos (fingerprint) |
| El componente DLP debe permitir la creación de políticas basadas en usuarios y grupos LDAP |
| El componente DLP debe hacer cumplir las políticas, mientras que el Endpoint se desconecta de la red corporativa |
| El componente DLP debe presentar un flujo de trabajo que incluya con una fase de clasificación o definición, una fase de identificación y registro, una fase de protección y una fase de monitoreo. |
| El componente DLP 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. |
| El componente DLP 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. |
| El componente DLP debe contar con una consola a nivel de Endpoint para aumenta la conciencia de los empleados de la protección de datos, permitiendo auto remediar cualquier violación a regulaciones de cumplimiento protección información de identificación personal (PII), seguridad de la información (ISO 27001) y similares para reducir las tareas manuales realizadas por los administradores DLP. |
| El componente DLP debe permitir la configuración de propiedades a los incidentes, para su posterior revisión. Las propiedades deben ser como mínimo: Severidad, Estatus, Resolución, Revisor |
| El agente del componente DLP debe registrar todas las violaciones, incumplimiento de políticas e informar a la base de datos central de la consola, cuando se establece una conexión a la red corporativa |
| El componente DLP debe contar con mecanismos que prevengan la vista no autorizada de información no pública a través del módulo de manejo de incidentes, limitando adicionalmente la vista de incidentes sólo a los roles cuyos privilegios se lo permitan. |
| El componente DLP debe contar con la posibilidad de hacer control de acceso basado en roles. |
| El componente DLP debe permitir la definición de reglas de protección basadas en: tipo de archivo, extensiones de archivo, propiedades de documento, tipos de encripción y asignación de usuarios o grupos. |

| |
|---|
| El componente DLP debe contar con un listado de reglas de acción amplio para realizar como mínimo las siguientes acciones: sólo lectura, reportar a la consola central, aplicar tag, aplicar políticas de RM (Right Management), poner en cuarentena, encriptar, guardar la evidencia, solicitar justificación, notificar al usuario, monitorear y bloquear |
| El componente DLP debe controlar la impresión usando impresoras locales, en red, print screen e impresión en pdf. |
| El componente DLP debe controlar la carga de información sensible a aplicaciones cloud como Box.inc, SkyDrive, Syncplicity, Dropbox, Google Drive, One Drive y similares |
| El componente DLP debe tener la capacidad de administrar, configurar, instalar, desinstalar, actualizar, asignar políticas para el control de dispositivos y prevención de fuga de Información |
| El componente DLP debe estar en capacidad de administrar desde la consola HTTPS otras soluciones de protección del Endpoint, gerencia de riesgo y seguridad web/email |
| El componente DLP debe permitir la creación de repositorios remotos para la distribución del software del software y actualizaciones en sitios remotos y minimizar el ancho de banda. |
| El componente DLP de permitir la replicación manual o automática a través de tareas el software para las actualizaciones e instalaciones. |
| El componente DLP debe permitir el acceso a las políticas por cada producto y generar una copia a la política de cada producto para generar una nueva sin afectar la política predeterminada. |
| El componente DLP debe permitir que los roles autorizados consulten los reportes de auditoría de entrada al servidor de administración, cambio de perfiles o roles, cambio de contraseñas, desinstalación de los agentes por eliminación, cambios de políticas, cambios ocurridos en el servidor de administración, acciones que incluyen agregar o borrar sitios, grupos, computadoras o cuentas, renombrar sitios o grupos |
| El componente DLP debe permitir la protección de las reglas de protección de datos a grupos de usuarios de Active Directory |
| El agente del componente DLP debe emplear reglas para proteger los datos clasificados como no públicos para la copia de software (Portapapeles), en aplicaciones en la nube, en el correo electrónico, compartidos en la red, enviado a impresión, que deben ser protegidos de la captura de pantalla, en aplicaciones y navegadores específicos, en publicaciones Web |
| El componente DLP debe restringir las normas de protección de datos a grupos de maquinaria o equipo que formen parte del mismo rango de direcciones IP. |
| El componente DLP debe restringir las reglas de protección de datos en función del sistema operativo en ejecución |
| El componente DLP debe permitir la ejecución de acciones diferenciadas si el usuario está fuera de la red local |
| La solución debe emplear técnicas de reconocimiento de patrones de texto predefinidos y diccionarios |
| El componente DLP debe contener de forma predeterminada al menos 150 objetos predefinidos entre diccionarios y definiciones de texto. |
| El componente DLP debe permitir la integración con herramientas de clasificación de información de terceros |
| El componente DLP debe tener la capacidad de crear reglas para la identificación de contenido clasificado y la toma de una determinada acción. |
| El componente DLP debe permitir la creación de reglas que permitan el control de la distribución no autorizada de datos clasificados |

| |
|---|
| El componente DLP debe permitir el control del uso máximo de RAM localmente |
| El componente DLP debe permitir que los módulos específicos de la solución se deshabiliten si no se utilizan en las reglas de protección. |
| El componente DLP debe tener clasificaciones definidas por protección de información de identificación personal (PII), y la clasificación definida por la Entidad. |
| El componente DLP debe contar con la capacidad de identificar información no pública basada en estándares avanzados (expresión regular) y los que correspondan a Colombia y otros países |
| El componente DLP debe permitir el uso de las propiedades del documento de Office para clasificarlo y ordenarlo |
| El componente DLP debe permitir la clasificación sobre la base del origen o el destino |
| El componente DLP debe soportar sistemas operativos Windows y MacOS |
| El componente DLP debe permitir el monitoreo o bloqueo total de los dispositivos conectados |
| El componente DLP debe permitir la creación de políticas unificadas para sistemas operativos Windows y MacOS. |
| El componente DLP debe gestionar los dispositivos de manera unificada en la misma consola de administración de antivirus |
| El componente DLP debe permitir la extensión de sus funcionalidades hacia prevención de fuga de datos, con el propósito de evitar despliegues adicionales |
| El componente DLP debe permitir la configuración de reglas basada en localización del usuario, de tal forma que permita tomar distintas acciones cuando el usuario está dentro o fuera de la Entidad |
| El componente DLP debe permitir la desactivación de una regla o un conjunto de reglas |
| El componente DLP debe permitir el control de los dispositivos de Almacenamiento Removible, Bluetooth, Multimedia, Smartphones, Plug and Play, CDs/DVDs |
| El componente DLP debe permitir el bloqueo de ejecución de aplicaciones desde dispositivos removibles, permitiendo también configurar excepciones. |
| La solución debe permitir el control de dispositivos bajo los siguientes criterios: clase de dispositivo, medio de conexión, fabricante, modelo y número mero de serie |
| El componente DLP debe permitir la creación de políticas de bloqueo, monitoreo o solo lectura para dispositivos de almacenamiento removible. |
| La solución debe permitir la configuración de definiciones de dispositivos bajo las siguientes categorías lista negra, lista Blanca, permitido, no permitido |
| El componente DLP debe permitir el agrupamiento de dispositivos por medio de propiedades comunes con al menos las siguientes categorías: ID de fabricante (Vendor ID), ID de producto (Product ID), clase de dispositivo (Device Class) |
| El componente DLP debe identificar los dispositivos Plug and Play bajo al menos una de las siguientes propiedades: Tipo de Bus, Clase de Dispositivo (Device Class), ID de fabricante (Vendor ID), ID de producto (Product ID) |
| El componente DLP debe identificar los dispositivos removibles bajo las siguientes propiedades: Tipo de Bus, Sistema de Archivo, Número de Serie, Permisos de lectura/escritura |
| El componente DLP debe reconocer las siguientes clases de dispositivos de manera nativa y todos los dispositivos posibles en el mercado: Batería, Lectores de huella y dispositivos biométricos, Bluetooth, Drives de CD/DVD, Impresoras, scanner, Adaptadores de video, Disco Duro, Controladoras y drives de diskette, GPS, Infrarrojo, dispositivos que usen el protocolo de conexión IEEE 1394, Mouse, Modem, Fax, Adaptadores de Red, PCMCIA, dispositivos Apple, dispositivos Android, almacenamiento removible, Lectores de tarjetas SD, Dispositivos Windows Portable, Dispositivos Plug and Play |

| |
|---|
| El componente DLP debe permitir habilitar o deshabilitar una determinada regla de protección de acuerdo con la localización del equipo (ej. Dentro o fuera de la red de la Entidad) |
| El componente DLP debe permitir la creación de clases y tipos de dispositivos personalizados, utilizando, como mínimo, los siguientes criterios: Clase de Dispositivo, Tipo de Bus, Número de Serie, ID de fabricante, ID de producto, Sistema de Archivo |
| El componente DLP debe contar con la capacidad de identificar un nuevo dispositivo conectado a las estaciones de trabajo, cuyo hardware es desconocido y enviar una alerta a la consola centralizada indicando una nueva clase de dispositivo encontrada |
| El componente DLP debe permitir el control de dispositivos mediante su globally unique identifier (GUID) que es un número pseudoaleatorio empleado en aplicaciones de software |
| El componente DLP debe permitir la creación de los siguientes tipos de controles y reglas: control de dispositivo, control de discos duros, reglas para dispositivos Plug and Play, almacenamiento removible, regla de acceso de archivos a dispositivos de almacenamiento removible, regla de dispositivo TrueCrypt que es un programa de cifrado gratuito que permite ocultar el contenido de un archivo o de un dispositivo de almacenamiento completo con datos aleatorios. |
| El componente DLP debe permitir que cada regla sea aplicada a: cualquier usuario, un usuario que pertenece a un grupo específico (OR), un usuario que pertenezca a todos los grupos (AND), un usuario local o usuario fuera del dominio |
| El componente DLP de permitir la definición de las reglas con creación de objetos LDAP en base a: SID de Objeto, Nombre de Objeto, Dominio de Objeto |
| El componente DLP debe permitir que para cada regla se configuren exclusiones como mínimo para: usuarios y dispositivos |
| El componente DLP de permitir que cada regla tenga la asignación de los siguientes niveles de severidad: Informativa (Information), advertencia (Warning), menor(minor), mayor(major), critica(crítical) |
| El contratista debe diseñar, estructurar y ejecutar un plan de trabajo en al menos las siguientes ocho (8) fases |
| FASE I: El contratista debe realizar levantamiento de información y entendimiento de la misión y estructura organizacional de la Entidad. El Contratista debe realizar la instalación, despliegue y configuración inicial del componente DLP |
| FASE II: El contratista debe validar el tipo de información que compone la información clasificada y reservada del DNP identificando los datos personales (sensibles, semiprivados y privados), identificando donde esta alojada la información y cuáles son los niveles de acceso que deberían tener los usuarios. El contratista puede recolectar la información mediante entrevistas y reuniones con el personal del DNP. |
| FASE III: El contratista debe realizar la instalación, despliegue y configuración de la herramienta, así como su integración con las demás soluciones de ciberseguridad de Trellix y otras si aplica. |
| FASE IV: El contratista debe realizar las configuraciones en el componente DLP con relación a los perfiles roles y permisos de los grupos de usuarios para el acceso a la información y data de la Entidad |
| FASE V: El contratista debe realizar las configuraciones de las reglas y políticas de El componente DLP |
| FASE VI: El contratista debe implementar tableros de control y reportes de seguimiento y monitoreo. |
| FASE VII: El contratista debe realizar unas recomendaciones de mejora para ajustes y afinamiento de las políticas del DLP. Realizar reuniones de seguimiento, entendimiento, mejora, afinamiento, análisis de los reportes, evaluación de la evolución de la implementación, asesoría en la configuración y administración de El componente DLP, estas revisiones deben ser entregadas DNP en un informe |

FASE VIII: El contratista debe realizar una transferencia de conocimiento y evaluación (assesment) inicial y en relación con el flujo de trabajo a seguir en caso de un incidente de seguridad relacionado con fuga de información

**Servicios técnicos y certificaciones requeridos por parte del oferente**

- El oferente deberá entregar todas las soluciones / equipos en los sitios/sedes indicadas por la entidad.
- Instalación, Implementación, configuración y puesta en marcha de las soluciones de seguridad y conectividad ofertadas.
- El oferente deberá realizar la instalación y configuración de los equipos con personal certificado por el fabricante con el cual se esté presentando.
- Todas las plataformas deberán ser de propósito específico, no se aceptan soluciones genéricas.
- El servicio de soporte del oferente debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas en horario Hábil y No Hábil por el tiempo contratado.
- El oferente seleccionado deberá entregar implementada y funcionando las soluciones completas, de acuerdo con los requerimientos y políticas.
- Planeación de cada una de las actividades, validadas en conjunto con el DNP.
- Configuración y alistamiento del software a la última versión estable aprobada por el fabricante para la plataforma.
- Afinamiento y estabilización de las plataformas.
- Pruebas de Servicio de las plataformas.
- Entrega de las plataformas a satisfacción al DNP.
- Las actividades de afinamiento de las plataformas deberán ser realizadas por personal certificado por el fabricante.
- La entidad requiere que se realicen pruebas / muestras de las plataformas donde se evidencie la correcta configuración y afinamiento de cada plataforma.
- El oferente deberá garantizar soporte y garantía para las plataformas ofertadas en un esquema 7x24 por un (1) año, con soporte remoto por parte del fabricante
- El servicio de soporte debe incluir atención de incidentes sobre las plataformas ofertadas.
- Consultas a través de llamadas telefónicas, correo electrónico.
- Sesiones remotas en horario Hábil y No Hábil. Todo con respecto a las plataformas ofertadas y objeto del presente contrato.
- El oferente deberá contar con certificación vigente del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022, expedida por un organismo de certificación acreditado. La certificación deberá estar vigente a la fecha de cierre del proceso y cubrir los servicios asociados a la solución ofertada.
- El oferente deberá contar con certificación vigente del Sistema de Gestión de Servicios de TI conforme a la norma ISO/IEC 20000-1:2018, expedida por un organismo de certificación acreditado. La certificación deberá estar vigente a la fecha de cierre del proceso y cubrir la prestación y gestión de los servicios de tecnología de la información relacionados con la solución ofertada.

**Experiencia del proponente**

El proponente deberá acreditar experiencia con la ejecución de HASTA TRES (3) CONTRATOS que cumplan con los siguientes requisitos:

Certificaciones: Adjuntar los certificados de experiencia expedidos por el contratante donde se evidencie que el proponente en calidad de contratista ha ejecutado contratos cuyo objeto esté relacionado con la adquisición y/o renovación de soluciones de ciberseguridad, y al menos un contrato debe cumplir con alguno de los siguientes ítems:

- Adquisición o renovación de licenciamiento/servicios de DLP.
- Adquisición o renovación de licenciamiento/servicios de EDR.

Valor: Las sumatoria de las certificaciones allegadas de los contratos acreditados deberá ser igual o superior al (100 %) del presupuesto oficial expresado en SMLMV.

**Servicios requeridos del fabricante:**
Servicios consultivos para las soluciones incluidas en este documento, considerando las siguientes actividades:

- Actualización a versión más reciente estable del producto (esquema N-1) en un ambiente piloto, según aplique
- Habilitación de nuevas funciones conforme a nueva versión disponible implementada, según aplique
- Revisión y corrección de errores conocidos, según aplique
- Implementación de buenas prácticas actualizadas, según aplique
- Implementación y optimización de tareas programadas, según aplique
- Revisión casos de soporte activos y entrega de recomendaciones, según aplique
- Integración con tecnologías de terceros o Trellix compatibles según aplique
- Desarrollo de casos de su adicionales según aplique.
- Transferencia de conocimientos sobre nuevas funciones disponibles, según aplique Los servicios consultivos deben programarse de manera mensual, trimestral o semestral, según disponibilidad de la entidad y con una persona responsable directa de fabrica (PM) con quién se coordinarán las actividades, entregables y documentación general. Para la programación de las actividades propuestas se debe contar con 280 horas durante el año. Para requerimientos en sitio, se solicitarán 40 horas continuas.

Operación y Personal en LTAM: El fabricante debe contar con operación y personal propio en LTAM. No se aceptará personal tercerizado para la operación o soporte principal. En caso de no contar con el personal necesario en LTAM, el fabricante deberá comprometerse a contratar de forma permanente al menos 30 personas en la región.

**Equipo mínimo requerido para el fabricante:**

Equipo mínimo de trabajo requerido.

**Un (1) Ingeniero - Gerente del Proyecto**

Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones, industrial o carreras afines. Tarjeta Profesional con expedición mínima de diez (10) años.
Posgrado en Gerencia de Proyectos y/o Certificación PMP vigente.
● Certificación vigente en ITIL Foundation v3 o superior.
● Certificación vigente en ITIL Strategist Direct, Plan and Improve
● Certificación vigente en ITIL Managing Professional
Experiencia mínima 5 proyectos gerenciando y/o coordinando proyectos
de TI y/o Seguridad Informática.
Tarjeta Profesional con exposición mínima de diez (10) años

**Un (1) Ingeniero - Líder Técnico**

Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.
● Especialización o maestría en Seguridad de la Información o informática o Ciberseguridad.
● Certificación vigente en SCRUM Foundations Professional (SFPC).
● Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC
20000-1:2018.
● Certificación vigente en AUDITOR LÍDER en la norma ISO/IEC
27001:2022.
● Certificación vigente en LÍDER GESTOR CIBERSEGURIDAD en la
norma ISO/IEC 27032:2023.
Experiencia general de diez (10) años a partir de la expedición de la tarjeta profesional, de los cuales mínimo de cinco (5)
años como líder o coordinador o gerente de servicios de TI.
Certificaciones de Experiencia específica de mínimo años (5) años en liderar equipo de operaciones y servicios de seguridad.

**Un (1) Ingeniero – Implementador**

Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.
● Especialización o maestría en Seguridad de la Información o informática o Ciberseguridad.
● Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018.
● Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 27001:2022.
Experiencia general de diez (10) años a partir de la expedición de la tarjeta profesional, de los cuales mínimo de cinco (5)
años en implementación, soporte y/o monitoreo de soluciones de seguridad.
La experiencia se cuenta a partir de la expedición de la tarjeta profesional

**Un (01) Ingeniero – Soporte**

Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.
• Especialización en seguridad de la Información o informática Ciberseguridad.
• Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 27001:2022.
EXPERIENCIA: Mínimo cinco (5) años de experiencia general todas contadas a partir de la expedición de la T.P., y mínimo tres (3) años en implementación, soporte y/o monitoreo de soluciones de seguridad.

NOTA 1: Cada uno de los perfiles deberá presentarse por separado (ninguno podrá repetir cargo o rol El contratista debe aportar en la fase de inicio del contrato las hojas de vida actualizadas las hojas de vida actualizadas, certificaciones y contrato laborales de vinculación a la empresa o proponente participante (evitando figuras de tercerización) (a la fecha del proceso) evidenciando el cumplimiento de cada especificación solicitada.

## ANEXO 2 OFERTA ECONÓMICA

(ESTE FORMATO DEBERÁ SER DILIGENCIADO EN LA PLATAFORMA DE SECOP II)

| Ítem | Descripción | Cantidad | VALOR UNITARIO INCLUIDO IVA | VALOR TOTAL INCLUIDO IVA |
|---|---|---|---|---|
| 1 | Renovación y actualización (upgrade) del licenciamiento por suscripción de Trellix EDR for Endpoint en su edición Enterprise, con Business Software Support por un (1) año. La suscripción cubre hasta cinco (5) dispositivos asigna$dos por usuario, incluyendo funcionalidades avanzadas de detección, investigación y respuesta extendida ante amenazas. | 2655 | $185.071 | $491.363.505 |
| 2 | Renovación de la licencia por suscripción Trellix Cloud Workload Security CWSE-S con Business Software Support por un (1) año en su edición Enterprise | 127 | $726.483.00 | $92.263.341 |
| 3 | Renovación de la licencia por suscripción Trellix Mobile Security Advanced con Business Software Support por un (1) año. Cubre hasta 5 dispositivos asignados por usuario en su edición Enterprise | 55 | $391,541 | $21.534.755 |
| 4 | Renovación de la licencia por suscripción Trellix Data Loss Prevention (DLP) con Business Software Support por un (1) año en su edición Enterprise | 2212 | $70.422 | $155.773.464 |
| 5 | Soporte, transferencia de conocimiento de acuerdo con lo requerido en el anexo técnico y con nivel Gold. | 1 | $138.090.120 | $138.090.120 |
| **TOTAL CON IVA** | | | | **$899.025.185** |

**Nota 1**: Los valores ofertados no podrán superar el presupuesto oficial ni se podrá superar el valor ofertado por ítem, asignados para el presente proceso de selección, incluido IVA y demás tributos a que haya lugar, ***so pena de rechazo*** de esta. Por lo anterior, el proveedor debe construir su oferta económica partiendo del análisis pertinente que arrojó el estudio de mercado del presente proceso.

**Nota** 2: Los valores ofertados no debe utilizar centavos; por lo tanto, el valor total de la propuesta económica y el valor de los impuestos a que hubiere lugar, deben presentarse en números enteros, es decir, el proponente deberá aproximar al peso, ya sea por exceso, si la suma es mayor a 0.50, o por defecto, si la suma es menor o igual a 0.49, en todo caso los valores ofertados deberán ser consignados en la plataforma SECOP II, formulario “oferta económica”.

**Nota 3:** Se entiende que en el valor total de la oferta se encuentran incluidos todos los tributos y gastos en que incurra el contratista para dar cumplimiento al objeto del presente proceso.

**Nota 4**: Igualmente, al momento de determinar el valor de su propuesta, tenga en cuenta que asumirá el riesgo cambiario y los posibles incrementos que puedan presentar los costos directos e indirectos para el cumplimiento del contrato, por ello el plazo de validez de su oferta debe ser igual o superior a noventa (90) días.

**Nota 5:** El valor del contrato a adjudicar será el resultante del evento de subasta.