CONTRATO DE ADQUISICIÓN DE BIENES Y SERVICIOS No. CGR-BID-028-2022

CONTRATO DE PRÉSTAMO BID 5385/OC-CO *"PROGRAMA PARA LA TRANSFORMACIÓN DIGITAL DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA – CGR"*

Contrato – Método Comparación de Precios

Este CONTRATO, se celebra, una vez suscrito por las partes contractuales el día 30 de junio de 2022, por un parte, la **CONTRALORÍA GENERAL DE LA REPÚBLICA** identificada con el NIT 899.999.067-2, representada por **SANDRA PATRICIA BOHORQUEZ GONZÁLEZ,** identificada con la cédula de ciudadanía No. 52.809.780 en su calidad de Gerente Administrativa y Financiera, nombrada mediante Resolución Ordinaria No 811117-00246-2019 y acta de posesión de fecha 30 de enero de 2019, obrando de acuerdo con las facultades dadas mediante la Ley 1955 de 2019 y la Resolución Organizacional 0191 de 11 de febrero de 2015 quien en adelante se denominará **EL CONTRATANTE** y por la otra, **WEXLER S.A.S.,** identificada con NIT 900.390.198-6, representada por **RAÚL WEXLER PULIDO TÉLLEZ,** identificado con la cédula de ciudadanía No. 79.690.388 de Bogotá en su calidad de representante legal, en adelante denominada el **PROVEEDOR.**

CONSIDERANDO QUE EL CONTRATANTE tiene interés en que el PROVEEDOR preste los servicios que se señalan a continuación,

CONSIDERANDO QUE el PROVEEDOR está dispuesto a prestar dichos servicios,

CONSIDERANDO QUE este contrato se encuentra incluido en el Plan Anual de Adquisiciones aprobado por el BID mediante comunicación No. CCO-536/2022 de fecha 04 de abril de 2022.

Se acuerdan las siguientes cláusulas:

<table>
<tr><td>1. Objeto</td><td>Adquisición de soluciones tecnológicas de ciberseguridad y servicios conexos para la Contraloría General de la República.</td></tr>
<tr><td>2. Alcance del Contrato</td><td>El alcance está dirigido al cumplimiento total de las especificaciones técnicas para lo cual el PROVEEDOR debe entregar a la CGR:
<table>
<tr><th>#</th><th>Descripción</th><th>Cantidad</th><th>Marca/ Referencia</th></tr>
<tr><td>1</td><td>Solución de operaciones de ciberseguridad con enfoque en inteligencia artificial (appliance físico) y el licenciamiento perpetuo de todas sus funcionalidades</td><td>1</td><td>Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331</td></tr>
<tr><td>2</td><td>Servicios conexos de instalación, configuración, puesta en operación, estabilización, transferencia y capacitación de la solución de operaciones de ciberseguridad con enfoque en inteligencia artificial</td><td>N/A</td><td>N/A</td></tr>
</table></td></tr>
</table>

	3	Soporte y garantía para la solución de operaciones de ciberseguridad con enfoque en inteligencia artificial por tres (3) años 7x24x365	N/A	N/A
	4	Solución de ciberseguridad de control de acceso a la red (NAC) (appliance virtual) y el licenciamiento perpetuo de todas sus funcionalidades	1	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO
	5	Servicios conexos de instalación, configuración y puesta en operación, estabilización, transferencia y capacitación de la solución de ciberseguridad de control de acceso a la red (NAC)	N/A	N/A
	6	Soporte y garantía para la solución de ciberseguridad de control de acceso a la red (NAC) por tres (3) años, 7x24x365	N/A	N/A

3. Acuerdos de niveles de servicio (ANS)

Se debe cumplir con los siguientes acuerdos de niveles de servicio para la solución de operaciones de ciberseguridad con enfoque en inteligencia artificial y la solución de ciberseguridad de control de acceso a la red (NAC), así:

Definiciones:

- **Incidente**: Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad de este.
- **Problema**: Evento que se presenta en la operación de las plataformas de seguridad informática, que produce un comportamiento o resultado diferente al esperado. Se debe tener claro que no es error del código del software sino es la falta de parámetros o prototipos no declarados o definidos en las plataformas.
- **Servicio**: Medio para entregar valor a la Entidad con resultados que proporcionen una utilidad y una garantía a las plataformas de seguridad informática (hardware y software).

Se definen las siguientes prioridades para incidentes y problemas, acordes a los niveles de servicio:

Tipo de solicitud de soporte técnico	Asignar responsable o reactivar estado	Horas hábiles para solución		
		Prioridad 1	Prioridad 2	Prioridad 3
Incidente o problema	Una (1) hora	2	4	8

- **Prioridad 1**: Sin acceso al servicio. Afecta la operación del sistema

	• **Prioridad 2**: Caída del servicio con conexión alterna disponible, Intermitencias en el servicio, degradación, servicio lento. • **Prioridad 3**: Impacto leve sobre el servicio que no afecta la operación del sistema. **ANS con cálculo mensual:** Se definen tres niveles de servicio para restablecer servicios o cerrar requerimientos, con los siguientes tiempos de solución: • La CGR registra el incidente o solicitud clasificado con base en la tabla de prioridades establecidas. Una vez la CGR haga el registro en el sistema, el proveedor dispondrá de una (1) hora para atender y analizar el caso y responder sobre la clasificación, solicitud de información y/o aclaraciones. • En el caso en que la CGR reporte incidencias que contengan temas diferentes, el proveedor, dentro de la hora otorgados para dar respuesta e iniciar la atención del soporte, atenderá uno de ellos e informará a la CGR para que se realicen el o los nuevos registros. • Una vez la CGR responda a las inquietudes del proveedor, este dispondrá de otra hora contados a partir de la respuesta dada por la CGR, para reactivar la incidencia y continuar con el proceso. Los tiempos establecidos en los ANS, se suspenden cuando un incidente reportado se encuentre en estado "se necesitan más datos o en verificación cliente". El soporte técnico contratado se prestará en los tiempos establecidos para la solución de fallas y su incumplimiento ameritará la siguiente sanción: • La diferencia que se genere entre el tiempo definido en la tabla de prioridades y el efectivamente utilizado para la atención y/o solución de las fallas, deberá ser compensado por parte del proveedor, de la siguiente manera: o Las horas por incumplimiento de los ANS se penalizarán con horas de acompañamiento en las actividades que defina la CGR, tales como: - transferencia de conocimiento técnico y funcional, parametrizaciones y acompañamiento en la operación. El tiempo de incumplimiento debe constar en los informes mensuales de ejecución del contrato, debidamente aprobadas por las partes, y por cada hora incumplida, el proveedor pagará una (1) hora en cualquiera de las actividades mencionadas en el párrafo anterior, las cuales se pueden acumular, precisando que su cumplimiento se dará durante la ejecución del contrato.
4. Valor y forma de pago	El valor del contrato será la suma de TRES MIL QUINIENTOS SESENTA MILLONES SETECIENTOS TREINTA MIL CUATROCIENTOS NOVENTA Y CINCO PESOS MONEDA LEGAL COLOMBIANA ($3.560.730.495) incluido IVA, dicha suma ha sido establecida en el entendido que incluye todos los costos y utilidades para el PROVEEDOR, así como cualquier obligación tributaria a que este pudiera estar sujeto.

A continuación, el detalle de los precios por ítem:

#	DESCRIPCIÓN	CANT.	VALOR UNITARIO	IVA	VALOR TOTAL
1	Solución de operaciones de ciberseguridad con enfoque en inteligencia artificial (appliance físico) y el licenciamiento perpetuo de todas sus funcionalidades	1	$593.406.300	$112.747.197	$706.153.497
2	Servicios conexos de instalación, configuración, puesta en operación, estabilización, transferencia y capacitación de la solución de operaciones de ciberseguridad con enfoque en inteligencia artificial	N/A	$184.902.100	$35.131.399	$220.033.499
3	Soporte y garantía para la solución de operaciones de ciberseguridad con enfoque en inteligencia artificial por tres (3) años 7x24x365	N/A	$680.698.200	$129.332.658	$810.030.858
4	Solución de ciberseguridad de control de acceso a la red (NAC) (appliance virtual) y el licenciamiento perpetuo de todas sus funcionalidades	1	$634.625.200	$120.578.788	$755.203.988
5	Servicios conexos de instalación, configuración y puesta en operación, estabilización, transferencia y capacitación de la solución de ciberseguridad de control de acceso a la red (NAC)	N/A	$204.786.400	$38.909.416	$243.695.816
6	Soporte y garantía para la solución de ciberseguridad de control de acceso a la red (NAC) por tres (3) años, 7x24x365	N/A	$693.792.300	$131.820.537	$825.612.837
		TOTAL	**$2.992.310.500**	**$568.519.995**	**$3.560.730.495**

	Las tarifas establecidas serán mantenidas a lo largo de la duración del contrato. Este valor se encuentra amparado con el certificado de disponibilidad presupuestal No. 3022 del 28 de abril de 2022 y su adición de fecha 9 de junio de 2022. El valor del contrato, se efectuarán en cuatro (4) pagos en pesos colombianos, así: • Un pago con la entrega de la solución de operaciones de ciberseguridad con enfoque en inteligencia artificial (appliance físico) y el licenciamiento de todas sus funcionalidades por 3 años (Item 1), un valor equivalente al 25% del valor del contrato. • Un pago con la entrega de la solución de ciberseguridad de control de acceso a la red (NAC) (appliance virtual) y el licenciamiento de todas sus funcionalidades por 3 años (Item 4), un valor equivalente al 25% del valor del contrato. • Un pago una vez ejecutado los servicios conexos de instalación, configuración, puesta en marcha y capacitación, documento de soporte y garantía de la solución de operaciones de ciberseguridad con enfoque en inteligencia artificial (appliance físico) de acuerdo con lo descrito en el Anexo de Especificaciones Técnicas y posterior recibo a satisfacción (Items 2 y 3), un valor equivalente al 25% del valor del contrato. • Un pago una vez ejecutado los servicios conexos de instalación, configuración, puesta en marcha y capacitación, documento de soporte y garantía de la solución de operaciones de ciberseguridad de control de acceso a la red (NAC) (appliance virtual) de acuerdo con lo descrito en el Anexo de Especificaciones Técnicas y posterior recibo a satisfacción (Items 5 y 6), un valor equivalente al 25% del valor del contrato. **PARÁGRAFO**: Para la realización del pago se requerirá el recibo a satisfacción por parte de la supervisión del contrato, la presentación de la factura correspondiente y la certificación que acredite el cumplimiento por parte del PROVEEDOR de las obligaciones al Sistema General de Seguridad Social (salud, pensiones y riesgos laborales), aportes parafiscales (Caja de compensación familiar, SENA e ICBF) según corresponda. Los pagos se efectuarán en pesos colombianos en la cuenta que informe por escrito el PROVEEDOR. El plazo para el pago se comenzará a contar a partir del recibo a satisfacción expedido por la supervisión del contrato y la presentación de los documentos, lo último que ocurra.
5. Obligaciones del CONTRATANTE	1. Entregar los insumos requeridos para el cumplimiento del objeto del contrato. 2. Designar formalmente un supervisor que obre como interlocutor directo con el Proveedor. 3. Efectuar los pagos de conformidad con lo acordado en el contrato. 4. Brindar la información requerida para el desarrollo del objeto contractual. 5. Las demás derivadas de la naturaleza del contrato que se requieran para su debida ejecución.

6. Obligaciones del PROVEEDOR	Además de las actividades establecidas en el alcance del contrato el PROVEEDOR deberá: 1. Desarrollar el objeto del contrato, en las condiciones de calidad, oportunidad e idoneidad del personal teniendo en cuenta las especificaciones técnicas. 2. Ejecutar soluciones técnicas sobre incidentes y/o problemas presentados en la plataforma instalada mediante la atención de las solicitudes que se reporten por la CGR, de acuerdo con lo establecido en los acuerdos de niveles de servicio. 3. Reemplazar los dispositivos que se requieran para mejorar capacidad y eficiencia de la plataforma de seguridad. 4. Responder las solicitudes presentadas por la CGR relacionadas con la plataforma instalada de seguridad. 5. Entregar a satisfacción la actualización del licenciamiento e implementación de las plataformas ofertadas de acuerdo con objeto del presente proceso de contratación y sus especificaciones técnicas. 6. Asegurar el soporte técnico y garantía de fabrica en modalidad de 7x24 por tres (3) años. 7. Realizar visitas cada tres (3) meses durante el término de la garantía en las cuales se deben validar las configuraciones de los equipos, hacer los ajustes correspondientes en las reglas de configuración y realizar las recomendaciones pertinentes a la CGR. 8. Entregar un reporte mensual detallado de las actividades desarrolladas e incidentes solucionados durante la vigencia del contrato, y aquellos requeridos por el supervisor del contrato. 9. Documentar de manera técnica lo referente a las actualizaciones y la respectiva transferencia de conocimiento de los cambios realizados, entregando a la supervisión del contrato (o a quien este designe) una copia en medio digital de los documentos de instalación y de control de cambios establecidos por la Oficina de Sistemas e Informática de la Contraloría General de la República. 10. Entregar y cumplir con todos los requerimientos y especificaciones técnicas establecidos y definidos en el presente documento y sus anexos. 11. Salvaguardar la información que obtenga o conozca en el desarrollo de sus actividades, razón por la cual debe tomar las medidas necesarias para garantizar su reserva salvo requerimiento expreso de autoridad competente. 12. Cumplir con las normas generales de protección de datos personales, seguridad de la información y en general la normatividad vigente en Colombia (Ley 1581 de 2012 y Decreto 1377 de 2013), así como con las políticas de seguridad establecidas en la CGR. 13. Responder ante terceros por los daños que se ocasionen y que le sean imputables, en desarrollo del contrato. 14. Reportar en caso de cualquier novedad o anomalía, de manera inmediata la situación al Supervisor del Contrato. 15. Atender los requerimientos que efectúe la entidad relacionados contractualmente. Así mismo, realizar las acciones conducentes a la idónea y oportuna ejecución del contrato.

	16. Asistir a las reuniones que sean convocadas por el Supervisor del contrato para revisar el estado del contrato. 17. Cumplir con todas aquellas obligaciones inherentes al contrato y necesarias para la correcta ejecución del objeto.
7. Responsabilidad	El PROVEEDOR es responsable por el cumplimiento del objeto establecido en la Cláusula 1 del presente Contrato.
8. Plazo de ejecución	Será de **tres (3) meses** a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato y hasta la terminación del objeto contractual.
9. Garantía	El PROVEEDOR deberá constituir una garantía única a favor de la CGR (entidades estatales) consistente en una póliza de cumplimiento a favor de la CGR por el 10% del valor del contrato, la cual estará vigente por el plazo de ejecución del contrato y tres (3) años más considerando la duración de la garantía y el soporte de las soluciones adquiridas.
10. Cesión del contrato	El PROVEEDOR no podrá ceder en todo o en parte la ejecución del contrato sin consentimiento previo del contratante.
11. Indemnidad	El PROVEEDOR se obliga a mantener libre al Contratante de cualquier daño o perjuicio originado en reclamaciones provenientes de terceros, que tenga como causa sus actuaciones.
12. Inhabilidades e Incompatibilidades y conflictos de interés	El PROVEEDOR manifiesta con la firma del presente documento que no se encuentra incurso en inhabilidades o incompatibilidades o conflictos de interés que impidan la entrega de los bienes y la prestación de los servicios contratados.
13. Prácticas prohibidas	El Banco exige a todos los Prestatarios (incluidos los beneficiarios de donaciones), organismos ejecutores y organismos contratantes, al igual que a todas las firmas, entidades o individuos oferentes por participar o participando en actividades financiadas por el Banco incluidos, entre otros, solicitantes, oferentes, proveedores de bienes, contratistas, consultores, miembros del personal, subcontratistas, subconsultores, proveedores de servicios y concesionarios (incluidos sus respectivos funcionarios, empleados y representantes, ya sean sus atribuciones expresas o implícitas) observar los más altos niveles éticos y denunciar al Banco todo acto sospechoso de constituir una Práctica Prohibida del cual tenga conocimiento o sea informado durante el proceso de selección y las negociaciones o la ejecución de un contrato. Las Prácticas Prohibidas comprenden (i) prácticas corruptas; (ii) prácticas fraudulentas; (iii) prácticas coercitivas; (iv) prácticas colusorias; (v) prácticas obstructivas; y (vi) apropiación indebida. A efectos del cumplimiento de esta Política, el Banco define las expresiones que se indican a continuación: (i) *Una práctica corrupta* consiste en ofrecer, dar, recibir, o solicitar, directa o indirectamente, cualquier cosa de valor para influenciar indebidamente las acciones de otra parte; (ii) *Una práctica fraudulenta* es cualquier acto u omisión, incluida la tergiversación de hechos y circunstancias, que deliberada o

	imprudentemente engañen, o intenten engañar, a alguna parte para obtener un beneficio financiero o de otra naturaleza o para evadir una obligación; *(iii)* *Una práctica coercitiva consiste en perjudicar o causar daño, o amenazar con perjudicar o causar daño, directa o indirectamente, a cualquier parte o a sus bienes para influenciar indebidamente las acciones de una parte;* *(iv)* *Una práctica colusoria es un acuerdo entre dos o más partes realizado con la intención de alcanzar un propósito inapropiado, lo que incluye influenciar en forma inapropiada las acciones de otra parte;* *(v)* *Una práctica obstructiva consiste en:* (i) destruir, falsificar, alterar u ocultar evidencia significativa para una investigación del Grupo BID, o realizar declaraciones falsas ante los investigadores con la intención de impedir una investigación del Grupo BID; (ii) amenazar, hostigar, intimidar a cualquier parte para impedir que divulgue su conocimiento de asuntos que son importantes para una investigación; o (iii) actos realizados con la intención de impedir el ejercicio de derechos contractuales de auditoría e inspección del Grupo BID previstos em el párrafo 1.16 (f) de las políticas, o sus derechos de acceso a la información; y (vi) *La apropiación indebida* consiste en el uso de fondos o recursos del Grupo BID para un propósito indebido o para un propósito no autorizado, cometido de forma intencional o por negligencia grave.
14. Solución de controversias	Toda controversia que surja de este contrato deberá someterse a fórmulas de solución directa de conflictos, en caso de no lograr acuerdo podrá someterse a proceso judicial conforme a la ley del país del Contratante.
15. Formas de terminación del contrato	El presente contrato se podrá terminar en los siguientes eventos: **1.** Por vencimiento del plazo de ejecución. **2.** Por mutuo acuerdo entre las partes. **3.** Por cumplimiento del objeto contractual. **4.** Si el CONTRATANTE, a su sola discreción y por cualquier razón, decidiera terminar este Contrato. **5.** Por incumplimiento del CONTRATISTA, en este último caso se procederá de la siguiente forma: En caso de incumplimiento del contrato imputable al CONTRATISTA, éste dispondrá de cinco (5) días contados a partir de la notificación de la Entidad para justificar o enmendar el incumplimiento de cualquiera de las estipulaciones contractuales. Si no lo hiciese, o no justificare o enmendare adecuadamente el incumplimiento, la Entidad declarará anticipada y unilateralmente terminado el contrato. Será también causa para que la Entidad proceda a declarar la terminación anticipada y unilateral del contrato, cuando el CONTRATISTA incurriere en prácticas corruptivas (soborno, extorsión o coerción, fraude, colusión, apropiación indebida).
16. Supervisión	La Supervisión y Control estarán a cargo del Director de la Oficina de Sistemas e Informática - OSEI o quien designe por escrito el ordenador del gasto. El supervisor deberá autorizar con su firma los pagos que deban hacerse al PROVEEDOR. Para el efecto, además del cumplimiento de las obligaciones, verificará como requisito para cada pago, el cumplimiento de las obligaciones relacionadas con la seguridad social en cumplimiento de la normatividad vigente.

17. Documentos del contrato	Hacen parte integral del presente contrato (i) La solicitud de cotización y sus anexos. (ii) la cotización presentada por el PROVEEDOR el 23 de mayo de 2022 (iii) el CDP y (iv) cualquier otro documento que llegue a generarse para la correcta ejecución del objeto contractual.
18. Perfeccionamiento y requisitos de ejecución	El presente contrato se entiende perfeccionado en la fecha de suscripción por las partes y efectuado el registro presupuestal por parte del Contratante. Para su ejecución requiere del cumplimiento de los anteriores requisitos y la presentación de la garantía establecida en la cláusula 9 del presente acuerdo.
19. Inspección y auditorías	El PROVEEDOR deberá conservar los documentos y registros relacionados con actividades del contrato por un periodo de siete (7) años después de la expiración de este contrato, de tal forma que el Contratante, o su representante designado y/o el Banco los inspeccione, obtenga copias de ellos, y los haga verificar por los auditores nombrados por el Contratante o el Banco, si así lo exigiera el Contratante o el Banco según sea el caso.
20. Modificaciones y cambios	Sólo podrán modificarse los términos y condiciones de este Contrato, incluido el alcance de los Servicios, mediante acuerdo por escrito entre las Partes. Cada una de las Partes deberá dar la debida consideración a cualquier modificación propuesta por la otra Parte.
21. Fuente de financiación y domicilio contractual	El Contrato que se pretende suscribir se financiará con recursos de crédito externo del Programa para la Transformación Digital de la Contraloría General de la República – Contrato de Préstamo BID 5385/OC-CO, y el domicilio será la ciudad de Bogotá D.C.
22. Dirección para notificaciones	El CONTRATANTE recibe notificaciones en la Carrera 69 No. 44 - 35 y EL PROVEEDOR en la Calle 24 C # 44 A - 26, ambas en la ciudad de Bogotá, D.C., correo electrónico andres.tabares@wexler.com.co

Para constancia se firma en Bogotá, D. C, a los treinta (30) días del mes de junio de dos mil veintidós (2022).

EL CONTRATANTE,

SANDRA PATRICIA BOHORQUEZ GONZÁLEZ
Gerente Administrativa y Financiera
Contraloría General de la República

EL PROVEEDOR,

RAÚL WEXLER PULIDO TÉLLEZ
Representante legal
WEXLER S.A.S.

CONTRATO DE ADQUISICIÓN DE BIENES Y SERVICIOS No. CGR-BID-028-2022

ESPECIFICACIONES TÉCNICAS

1. ANTECEDENTES Y JUSTIFICACIÓN

Para el cumplimiento de las funciones establecidas en la Constitución Política de Colombia en especial lo consignado en los Artículos 267 y 268, dentro de estándares de calidad y eficiencia, la Contraloría General de la República - CGR debe generar constantemente medidas para optimizar y fortalecer sus procesos, de tal forma que los resultados redunden en el buen gobierno, en la transparencia de la gestión pública y en el control de la corrupción, generando confianza y credibilidad para el ciudadano.

Es así como el Gobierno Nacional a través del documento CONPES No. 4045 de 2021 autorizó a la Nación para contratar un empréstito externo con la Banca Multilateral hasta por 30 millones de dólares estadunidenses, destinados al financiamiento del Programa para la Transformación Digital de la Contraloría General de la República. En este contexto, la República de Colombia y el Banco Interamericano de Desarrollo – BID celebraron el Contrato de Préstamo No. 5385/OC-CO el 13 de diciembre de 2021. El objetivo del Programa es incrementar la efectividad del control fiscal de la Entidad a través del incremento de la productividad y de los niveles de eficacia en el ejercicio de vigilancia y control aumentando las oportunidades para la participación ciudadana. Para cumplir con este objetivo, en el programa se propusieron tres componentes: i) Fortalecimiento de las capacidades institucionales para la transformación digital; ii) Fortalecimiento de las herramientas digitales para el control fiscal; y iii) Enfoque ciudadano e integridad.

La CGR ha realizado esfuerzos para el aseguramiento de su infraestructura y servicios tecnológicos, especialmente en el ámbito de la ciberseguridad, los cuales han permitido el desarrollo y ejecución de su función misional en un ambiente seguro y confiable. Asimismo, la pandemia modificó la manera de trabajar y entregar servicios a través del teletrabajo, el trabajo remoto y la virtualidad lo cual incrementa el riesgo, tal y como señala el informe escrito por la Cámara Colombiana de Informática y Telecomunicaciones "*TENDENCIAS CIBERCRIMEN COLOMBIA 2019 – 2020"*. (INFORME TENDENCIAS CIBERCRIMEN (ccit.org.co) "*Los incidentes más reportados en Colombia siguen siendo los casos de Phishing con un 42%, la Suplantación de Identidad 28%, el envío de malware 14% y los fraudes en medios de pago en línea con 16%"*. Así las cosas, es importante continuar reforzando el modelo de seguridad informática con soluciones integrales que permitan habilitar y consolidar un ecosistema de aseguramiento y monitoreo de ciberseguridad.

Como parte de la estrategia de ciberseguridad la entidad cuenta con un servicio gestionado de Centro de Operaciones de Seguridad (SOC por sus siglas en inglés) que cuenta con especialistas en ciberseguridad, administración, gestión, monitoreo, control y mitigación de ataques cibernéticos que se puedan presentar. Este servicio ha permitido brindar seguridad, disponibilidad y desempeño de la plataforma tecnológica de la CGR, con operación ininterrumpida 7x24x365. Sin embargo, no todos los riesgos y ataques cibernéticos son cubiertos y mitigados por este centro, y por ello se requiere fortalecer los controles que minimicen el riesgo de materialización de algún tipo de ataque informático que impacte la normal operación de los procesos misionales y de apoyo de la CGR dado que para sus ataques los hackers utilizan cada vez más métodos sofisticados, en la medida que usan más inteligencia artificial, por ejemplo, acuden a ingeniería social a escala, rastreo de documentos, evasión del reconocimiento de imágenes y voz, contaminación de datos, entre otros.

Así las cosas, se deben incorporar soluciones novedosas que consideren buenas prácticas de industria (seguridad informática), fortalezcan la arquitectura de ciberseguridad y le permitan a la CGR aumentar su capacidad de protección y control, tanto de la infraestructura física como virtual, incluyendo los equipos y dispositivos utilizados por los funcionarios y contratistas dentro de la Entidad. Considerando lo antes mencionado, se requiere de una solución que permita un control y monitoreo continuo de la red (NAC por sus siglas en inglés), que analice el comportamiento de ataque y la contención de las operaciones de ciberseguridad con enfoque en inteligencia artificial las cuales se incorporarían e integrarían con el servicio gestionado del SOC para tener visibilidad y control centralizado de los diferentes componentes que permitan actuar de manera proactiva y lograr un aseguramiento mayor a la plataforma tecnológica de la entidad.

CONTRATO DE ADQUISICIÓN DE BIENES Y SERVICIOS No. CGR-BID-028-2022

Por lo anterior, la CGR requiere la adquisición de soluciones de operaciones de ciberseguridad con enfoque en inteligencia artificial y de seguridad en el acceso a la red (NAC), que incluya servicios conexos de instalación, configuración, puesta en marcha, capacitación, garantía y soporte.

1. OBJETO

Adquisición de soluciones tecnológicas de ciberseguridad y servicios conexos para la Contraloría General de la República.

2. ALCANCE DEL OBJETO

El alcance está dirigido cumplimiento total de las especificaciones técnicas que se encuentran descritas en el Anexo 3.

3. OBLIGACIONES DEL PROVEEDOR

a. Desarrollar el objeto del contrato, en las condiciones de calidad, oportunidad e idoneidad del personal teniendo en cuenta las especificaciones técnicas.
b. Ejecutar soluciones técnicas sobre incidentes y/o problemas presentados en la plataforma instalada mediante la atención de las solicitudes que se reporten por la CGR, de acuerdo con lo establecido en los acuerdos de niveles de servicio.
c. Reemplazar los dispositivos que se requieran para mejorar capacidad y eficiencia de la plataforma de seguridad.
d. Responder las solicitudes presentadas por la CGR relacionadas con la plataforma instalada de seguridad.
e. Entregar a satisfacción la actualización del licenciamiento e implementación de las plataformas ofertadas de acuerdo con objeto del presente proceso de contratación y sus especificaciones técnicas.
f. Asegurar el soporte técnico y garantía de fabrica en modalidad de 7x24 por tres (3) años.
g. Realizar visitas cada tres (3) meses durante el término de la garantía en las cuales se deben validar las configuraciones de los equipos, hacer los ajustes correspondientes en las reglas de configuración y realizar las recomendaciones pertinentes a la CGR.
h. Entregar un reporte mensual detallado de las actividades desarrolladas e incidentes solucionados durante la vigencia del contrato, y aquellos requeridos por el supervisor del contrato.
i. Documentar de manera técnica lo referente a las actualizaciones y la respectiva transferencia de conocimiento de los cambios realizados, entregando a la supervisión del contrato (o a quien este designe) una copia en medio digital de los documentos de instalación y de control de cambios establecidos por la Oficina de Sistemas e Informática de la Contraloría General de la República.
j. Entregar y cumplir con todos los requerimientos y especificaciones técnicas establecidos y definidos en el presente documento y sus anexos.
k. Salvaguardar la información que obtenga o conozca en el desarrollo de sus actividades, razón por la cual debe tomar las medidas necesarias para garantizar su reserva salvo requerimiento expreso de autoridad competente.
l. Cumplir con las normas generales de protección de datos personales, seguridad de la información y en general la normatividad vigente en Colombia (Ley 1581 de 2012 y Decreto 1377 de 2013), así como con las políticas de seguridad establecidas en la CGR.
m. Responder ante terceros por los daños que se ocasionen y que le sean imputables, en desarrollo del contrato.
n. Reportar en caso de cualquier novedad o anomalía, de manera inmediata la situación al Supervisor del Contrato.
o. Atender los requerimientos que efectúe la entidad relacionados contractualmente. Así mismo, realizar las acciones conducentes a la idónea y oportuna ejecución del contrato.
p. Asistir a las reuniones que sean convocadas por el Supervisor del contrato para revisar el estado del

contrato.

q. Cumplir con todas aquellas obligaciones inherentes al contrato y necesarias para la correcta ejecución del objeto.

4. OBLIGACIONES DEL CONTRATANTE

a. Entregar los insumos requeridos para el cumplimiento del objeto del contrato.
b. Designar formalmente un supervisor que obre como interlocutor directo con el Proveedor.
c. Efectuar los pagos de conformidad con lo acordado en el contrato.
d. Brindar la información requerida para el desarrollo del objeto contractual.

CONTRATO DE ADQUISICIÓN DE BIENES Y SERVICIOS No. CGR-BID-028-2022

#	DESCRIPCIÓN	OFRECIMIENTO	DOCUMENTO SOPORTE Y FOLIO
GENERALIDADAES			
1	Suministro de appliance físico.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FORTINDR - HOJA DE DATOS - PAG. 4
2	Los componentes que integran la solución no deben aparecer en listas End-Of-Life ó End-of-Sale del fabricante.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
CARACTERÍSTICAS MÍNIMAS DE DESEMPEÑO			
3	Almacenamiento: 4 TB SSD	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FORTINDR - HOJA DE DATOS - PAG. 4
4	2 interfaces de 10 Gbps RJ-45 y 1 de 1 Gbps RJ45	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FORTINDR - HOJA DE DATOS - PAG. 4
5	Capacidad de análisis de tráfico con un desempeño mínimo de 10 Gbps.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FORTINDR - HOJA DE DATOS - PAG. 4
6	Fuente de poder redundante	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FORTINDR - HOJA DE DATOS - PAG. 4
FUNCIONALIDADES DE SEGURIDAD			
7	La plataforma debe utilizar mecanismos de inteligencia artificial y redes neuronales para el análisis de tráfico y muestras, usando modelos entrenados y maduros.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FORTINDR - HOJA DE DATOS - PAG. 1
8	La plataforma debe estar en capacidad de hacer análisis de tráfico en tiempo real.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 45 a 47

9	El equipo que conforma la solución debe ser instalado fuera de línea, es decir, la recepción del tráfico de red debe hacerse a través de puertos pasivos (puertos mirror /SPAN), de tal manera de no causar retardos en el desempeño de la red	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 8 y 15
10	La plataforma debe poder hacer aprendizaje de nuevas características de malware del entorno de la Contraloría General de la República, en adición a los modelos que traiga de fábrica.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 75 y 92
11	La solución debe integrarse con el Firewall de Nueva Generación que tiene la entidad (FortiGate), para la generación de acciones automáticas de bloqueo o cuarentena ante la detección de un ataque.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 23 a 24
12	La solución debe estar en capacidad de hacer análisis de tráfico cifrado sin realizar desencripción del mismo y recibir tráfico SSL Decryption mirroring	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 8, 24 y 49
13	La solución debe integrarse con la plataforma de SIEM del SOC de la entidad (FortiSIEM)	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FORTINDR - HOJA DE DATOS - PAG. 3
14	La solución debe integrarse con la plataforma de SOAR del SOC de la entidad (FortiSOAR)	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 15 a 16
15	La solución debe estar en capacidad de brindar resultados del análisis en menos de un segundo.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 8 a 10
16	La solución debe suministrar visibilidad de dispositivos, usuarios, aplicaciones en la red.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 41
17	Además del modelo de inteligencia artificial pre-entrenado, la solución debe estar en capacidad de hacer aprendizaje del tráfico observado en el escenario real de la entidad.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 133
18	La solución debe estar en capacidad de identificar y clasificar al menos los siguientes escenarios generales diferentes de malware: Gusanos, Ransomware, Troyanos bancarios, Minería de Bitcoin, Robo de credenciales, DDoS emtre otros.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 30

19	La solución debe estar en capacidad de hacer investigación del malware detectado usando sus modelos de inteligencia artificial.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FORTINDR - HOJA DE DATOS - PAG. 1
20	La solución debe estar en capacidad de hacer detección del paciente cero de un ataque o infección.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FORTINDR - HOJA DE DATOS - PAG. 2
21	La solución debe estar en capacidad de analizar tráfico proveniente de un puerto mirror / SPAN en la red, con un desempeño mínimo de 10 Gbps.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 8
22	La solución debe integrarse con la plataforma de protección de amenazas avanzadas, para la remisión de muestras sospechosas y la generación de indicadores de compromiso con base en la respuesta de análisis realizado.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FORTINDR - HOJA DE DATOS - PAG. 3
23	La solución debe estar en capacidad de hacer búsqueda de brotes de malware basados en variantes de detecciones conocidas.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FORTINDR - HOJA DE DATOS - PAG. 1
24	La solución debe mostrar las amenazas que se van identificando en la red en tiempo real, con la investigación de la fuente de la amenaza y su avance en el tiempo.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 46
25	La solución debe integrarse con la plataforma de SIEM ofertada, para la correlación de eventos de detecciones realizadas.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 123
26	La solución debe mostrar en su dashboard información general acerca del estado de CPU, memoria y licenciamiento.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 121
27	La solución debe poder hacer actualización de los modelos de inteligencia artificial o redes neuronales,	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 10
28	La solución no debe requerir la instalación de agentes en activos de la entidad para cumplir con sus funcionalidades.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 8

29	La administración de la herramienta deberá realizarse tipo web y CLI, en el caso que la solución de administración sea cliente servidor el licenciamiento debe ser ilimitado.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 8
30	La solución debe mostrar en su dashboard características aprendidas a partir del tráfico de la entidad.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	FortiNDR-7.0.0-Administration_Guide - PAG. 20
IMPLEMENTACIÓN			
31	La solución deberá incluir el diseño de la arquitectura y políticas de acuerdo con las necesidades de la entidad y su implementación y puesta en funcionamiento.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
32	Implementación de la solución de acuerdo con las mejores prácticas del fabricante, teniendo en cuenta una arquitectura de red segura.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
33	El proveedor deberá realizar un análisis de la arquitectura de red actual, con el fin de aplicar las mejores prácticas para la implementación	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
34	Planeación de cada una de las actividades, validadas en conjunto con los ingenieros designados por el supervisor del contrato, el entregable es el plan de trabajo a ejecutar.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
35	Realizar las actividades necesarias para la configuración y puesta en marcha de plataforma de seguridad y estabilización de la plataforma.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
36	Configuración y alistamiento del software y de la máquina virtual a la última versión estable aprobada por el fabricante.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
37	La solución será responsabilidad del proveedor hasta el recibo a satisfacción por parte del supervisor del contrato.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos

38	Se deben contemplar todos los servicios profesionales necesarios para la implementación e integración con los elementos de seguridad de la Entidad. El personal que ejecute los servicios de implementación, configuración y soporte de la solución debe ser certificado por el respectivo fabricante.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
39	Configuración y alistamiento del software y máquina virtual a la última versión estable aprobada por el fabricante	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
40	Se debe elaborar plan de pruebas de la solución para su ejecución y documentar los resultados.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
LICENCIAMIENTO			
41	La solución debe incluir el licenciamiento perpetuo para todas las funcionalidades.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
SOPORTE Y GARANTÍA			
42	Entregar el documento en el cual conste el soporte y garantía de la solución implementada, por parte del proveedor, durante un periodo de tres (3) años, posterior al recibo a satisfacción	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
43	Prestar los servicios de soporte, entrega de licenciamiento, hardware y software en las instalaciones de la entidad ubicada en el nivel central.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
44	La solución debe tener garantía y soporte técnico de fábrica en esquema 7x24x365 durante tres (3) años.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
45	La solución debe contar con soporte técnico y retorno de hardware por parte del fabricante por un periodo de 3 años en un esquema 7x24x365, incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
46	El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario hábil y no hábil por el tiempo contratado	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos

47	Se deben incluir actividades de mantenimiento, las cuales se realizarán como mínimo un (1) mantenimiento preventivo al año para minimizar problemas y mantener los sistemas actualizados, cuando este sea requerido por la entidad, durante el periodo de garantía y soporte que es de tres (3) años. En cuanto a los mantenimientos correctivos se deben realizar los que sean necesarios con el fin de garantizar la disponibilidad del servicio, durante el periodo de garantía y soporte que es de tres (3) años.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
48	Se deben incluir las actividades necesarias para atender las solicitudes de la CGR durante el contrato, que podrán incluir las siguientes actividades:	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
	• Cambios de Configuraciones.		
	• Acompañamiento en migraciones.		
	• Consultas e implementación de nuevas funcionalidades		
49	Realizar visitas cada tres (3) meses durante la vigencia del contrato en las cuales se deben validar las configuraciones de los equipos y realizar los ajustes correspondientes en las reglas de configuración y realizar las recomendaciones que se requieran a los administradores de las plataformas.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
50	Mantener actualizados los niveles de firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
51	Al finalizar cada visita correctiva y/o preventiva el proveedor deberá generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones, y si hubo cambio de software y/o en la configuración.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
52	El horario de atención para el mantenimiento correctivo y preventivo deberá ser de 7x24 en sitio, sin costo adicional para la entidad.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
DOCUMENTACIÓN			
53	Realizar y documentar entre otras, las siguientes actividades:	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
	• Nuevas configuraciones y migraciones solicitadas por la Entidad.		
	• Configuración e implementación de la solución, con el resultado de las pruebas incluyendo evidencias (captura de pantallas, fotos)		
CAPACITACIONES Y TRANSFERENCIA DE CONOCIMIENTO			

54	Realizar transferencia de conocimientos para cinco (5) funcionarios de la entidad, la cual debe incluir por lo menos temas de administración, configuración y afinamiento de la solución implementada.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
55	El proveedor debe brindar capacitación oficial de fabricante para cinco (5) funcionarios de la entidad sobre la operación y administración de la solución.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos
ACUERDOS DE NIVELES DE SERVICIO		Se detallan en la cláusula 3.	
CERTIFICADO DE FABRICANTE			
57	El oferente debe contar con el máximo nivel de membresía del fabricante, para lo cual debe adjuntar el certificado de distribuidor autorizado del fabricante con fecha no mayor a 60 días anteriores al cierre del proceso, donde se evidencie el nivel de membresía. Las certificaciones deben dirigirse a la Contraloría General de la República.	Appliance físico + Licencias (NDR+ANN): FAI-3500F-BDL-331	Enterados, aceptamos y cumplimos

SOLUCIÓN DE CONTROL DE ACCESO A LA RED (NAC)

#	DESCRIPCIÓN REQUERIMIENTO		
GENERALIDADES			
1	Suministro de appliance virtual.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 11
2	Capacidad de instalación sobre hipervisores: Microsoft Hyper-V, VMWare	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 11
3	Los componentes que integran la solución no deben aparecer en listas End-Of-Life ó End-of-Sale del fabricante.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumnplimos
CARACTERISTICAS MÍNIMAS DE DESEMPEÑO			
4	Capacidad de gestión de al menos 15000 dispositivos conectados concurrentes	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 11
5	En caso de requerirse múltiples Appliances o VMs para la implementación de la solución, esta deberá permitir la administración centralizada del conjunto desde un Appliance o VM de administración	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 11
6	En caso de requerirse múltiples Appliances o VMs para la implementación de la solución, las licencias deben poder aplicarse individualmente a cada dispositivo o ser manejadas de manera centralizada, distribuyéndose dinámicamente según las necesidades de cada dispositivo de control	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 11

7	La solución debe ser licenciable por dispositivo. Estas licencias deben ser perpetuas deben permitir distintos niveles de operación (visibilidad, control, compliance)	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 7
CARACTERÍSTICAS DE CÓMPUTO			
A continuación, se describen las máximas capacidades de cómputo que puede asignar la Contraloría General de la República en su plataforma de virtualización (VMWare) para la solución, en caso de que la solución ofertada requiera mayor cantidad de recursos, el oferente podrá entregar el hardware sobre el cual virtualizará la solución.			
El oferente debe adjuntar a la oferta documento de fabricante de la solución en el cual certifique las capacidades optimas de recursos requeridas de la solución para el cumplimiento del adecuado desempeño de los 15.000 dispositivos incluidos en el requerimiento.			
8	La entidad asignará un máximo de 6 vCPU a la máquina virtual	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumnplimos
9	La entidad asignará un máximo de 32 GB en RAM a la máquina virtual	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumnplimos
10	La entidad asignará un máximo de 480 GB en disco a la máquina virtual	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumnplimos
FUNCIONALIDADES DE VISIBILIDAD			
11	Debe contar con un proceso continuo de detección y categorización de dispositivos, que permita detectar y controlar dispositivos desconocidos o no autorizados de manera automática, sin requerir de agentes instalados en los dispositivos.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 1
12	Debe permitir determinar el perfil de los dispositivos descubiertos mediante métodos que no requieran la instalación de agentes incluyendo, al menos, los siguientes: DHCP fingerprint, HTTP/HTTPS, Ubicación, SSH, Telnet, TCP, UDP, OUI, WMI, WinRM, NMAP.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 232 a 235
13	Debe permitir el uso de Agentes Persistentes para el perfilamiento de dispositivos	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 421 a 31
14	La solución debe poder reconocer, al menos, los siguientes sistemas operativos sin necesidad de agentes: Android, Apple iOS for iPhone/iPad7/iPod, Chrome OS, Free BSD, Kindle/Kindle Fire, Linux, Mac OS X, Open BSD, Solaris, Symbian, Web OS.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 462 a 463

15	La plataforma de control de acceso debe tener plantillas o perfiles predefinidos para diferentes tipos de dispositivos de usuario final tales como: Sistema de Alarma, Android, Apple iOS, Cámara, Lector de Tarjetas, Control Ambiental, Sistema genérico de monitoreo, switches, Hub, Teléfono IP, Linux, Mac OS X, Dispositivo Móvil, PBX, Impresora, Servidor, UPS, Access point wireless, VPN, IPS/IDS.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 181 a 204
16	Debe recordar el perfil asignado a cada dispositivo, y verificar que sigue siendo válido en cada conexión del dispositivo. Si el perfil cambiara, dependiendo del cambio observado, deberá permitir o impedir su conexión. En este último caso, deberá notificar inmediatamente sobre el hecho.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 2
17	Debe permitir la categorización manual o automática de dispositivos.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 7
18	Debe soportar la identificación de dispositivos y sistemas operativos, con clasificación automática, y permitir la visualización de esta información.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 7
19	Debe permitir la designación de un Sponsor que autorice la categorización del dispositivo o el acceso de un invitado.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 555
20	Debe permitir la recategorización periódica de los dispositivos.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 218 a 226
21	Debe permitir la fijación de períodos de tiempo en los que el dispositivo está autorizado a operar, y evaluarlos periódicamente.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 219
22	Debe permitir la importación de un archivo .CSV conteniendo información sobre los dispositivos a registrar.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 78
23	Debe permitir el registro manual de dispositivos no SNMP.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 14
24	Debe permitir la identificación de usuarios mediante Active Directory o Portal Cautivo.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 163 y 555
25	La solución debe operar indistintamente para entornos cableados o inalámbricos, locales o remotos.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 1
26	Debe permitir la identificación de dispositivos mediante Portal Cautivo, Perfilamiento y clasificación automáticos, Autorización mediante Radius, Active Directory y OpenLDAP,e integración	Appliance virtual: FNC-CAVM	FortiNAC-920-AdminGuide - PAG. 349 a 358

	con plataformas MDM (al menos Air Watch, Google Gsuite, MaaS360, Mobile Iron y XenMobile).	Licenciamiento: LIC-FNACPRO	
CARACTERÍSTICAS MÍNIMAS DE VISIBILIDAD DE RED			
27	La solución debe permitir un despliegue centralizado, en una arquitectura fuera de banda, y brindar control de acceso en Capa 2 sobre una infraestructura cableada e inalámbrica.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 17
28	Debe permitir crear una estructura jerárquica que permita ordenar los dispositivos de infraestructura de la red de manera lógica o geográfica.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 1181
29	Debe permitir crear, modificar y borrar dispositivos y sus características.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 1
30	Debe contar con un proceso continuo de detección y categorización de dispositivos de infraestructura de red, que permita detectar y controlar los switches, routers y otros dispositivos de la red.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 14
31	Debe permitir mover fácilmente los dispositivos dentro de la estructura jerárquica generada.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 181 a 204
32	Debe permitir realizar polling de los dispositivos en Capa 2.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 376
CARACTERÍSTICAS MÍNIMAS DE VISIBILIDAD DE ENDPOINT			
33	Debe permitir la detección de hosts desconocidos (rogue).	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 180
34	Debe permitir la identificación de hosts mediante Portal Cautivo.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 554 a 656
35	Debe permitir la categorización automática de hosts.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 218 a 226
36	Debe permitir la recategorización periódica de los hosts desconocidos.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 218 a 226
37	Debe recordar el perfil asignado a cada host, y verificar que sigue siendo válido en cada nueva conexión del host. Si el perfil variara, deberá impedir su conexión y notificar inmediatamente sobre el hecho.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 393

38	Debe permitir la fijación de períodos de tiempo en los que el host está autorizado a operar, y evaluarlos periódicamente.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 398
39	Debe permitir la importación de un archivo .CSV conteniendo información sobre los hosts a registrar.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 78
40	Debe permitir la integración con plataformas MDM	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 345 a 358
41	La solución no debe requerir obligatoriamente el uso de 802.1x para permitir el descubrimiento de hosts en la infraestructura cableada.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 343
42	Debe permitir determinar el perfil de los hosts descubiertos mediante métodos que no requieran la instalación de agentes incluyendo, al menos, los siguientes: DHCP Fingerprinting, HTTP/HTTPS, Ubicación, SNMP, SSH, Telnet, TCP, UDP, OUI, WMI, WinRM.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 232 a 235
CARACTERÍSTICAS MÍNIMAS DE VISIBILIDAD DE USUARIOS			
43	Debe permitir el uso de Agentes Persistentes para el perfilamiento de hosts.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 421 a 431
44	Debe permitir la identificación de usuarios mediante Active Directory.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 163 y 555
45	Debe permitir la identificación de usuarios mediante Portal Cautivo.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 555
46	La solución debe incluir opciones de análisis flexibles para plataformas Windows, MacOS y Linux. La tecnología de agentes desvanecibles no debe requerir la instalación de software de terceros, tales como Java.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 419
47	Debe permitir la designación de un Sponsor que autorice el acceso de un invitado.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 555
48	Debe permitir la designación de un Sponsor que autorice la categorización de un host.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 555
CARACTERÍSTICAS MÍNIMAS DE AUTOMATIZACIÓN Y CONTROL			

49	La solución no debe requerir obligatoriamente el uso de 802.1x para brindar control de acceso a nivel de Puerto en la infraestructura cableada.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 404
50	Debe permitir el ingreso de credenciales mediante Mac Auth, MAB, 802.1x o Portal Cautivo.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 404
51	Debe soportar la validación de credenciales: Con servidor RADIUS y con servidor LDAP.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 579
52	Debe soportar la validación automática de credenciales mediante agentes persistentes o volátiles.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 421 a 431
53	La solución debe tener la capacidad de aprovechar la combinación de informaciones sobre la identidad del usuario y el tipo de dispositivo para aprovisionar dinámicamente permisos de acceso basados en roles y distintos niveles de acceso.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 316
54	Debe permitir la generación de políticas de control, agrupadas jerárquicamente, y determinar la política a aplicar a cada dispositivo en función de una serie de reglas de asignación.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 163 y 555
55	Debe soportar, al menos, los siguientes tipos de información para determinar la política a aplicar: Ubicación, Grupo de Pertenencia, Atributo, Fecha y Hora.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 169
56	La solución debe incluir funcionalidades de Guest Management, permitiendo la creación de perfiles de invitados y contratistas.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 44
57	Debe permitir la creación de plantillas que agrupen a los invitados o contratistas en grupos que tengan distintos permisos de acceso, o períodos de tiempo de acceso permitido.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 144
58	Debe contar con herramientas que permitan la generación y mantenimiento de este tipo de usuarios y sus claves de acceso.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 144
59	Debe permitir la creación de Portales de Auto-Registro.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 151
60	Debe soportar el envío de claves de acceso mediante SMS.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 151

61	Debe permitir la existencia de Sponsors que aprueben el ingreso de invitados o contratistas a la red, o que eleven los permisos de acceso de ciertos individuos.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 555
62	La solución debe incluir funcionalidades de IoT que permita su gestión y autorización de manera manual y automática para incorporarse a la red de la Entidad.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 555
63	La solución debe incluir funcionalidades de Endpoint Compliance. Antes de permitir el acceso de los dispositivos a la red, debe asegurarse de que estos cumplen con una serie de requisitos de seguridad, integridad y configuración, que hagan seguro su acceso a la red.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 130
64	La solución debe permitir que se comprueben los servicios en ejecución para computadoras Windows.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 514
65	La solución debe permitir que se compruebe información sobre certificado digital en computadoras Windows.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 514
66	La solución debe permitir que se compruebe registro o clave del registro para computadoras Windows.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 514
67	La solución debe permitir que se comprueben procesos en ejecución para estaciones Windows, Linux y MacOS.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 514
68	La solución debe permitir que se compruebe la existencia de un archivo almacenado en un directorio determinado para las computadoras Windows, Linux y MacOS.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 514
69	La solución debe permitir que se compruebe la existencia de ciertos paquetes instalados en computadoras Linux y MacOS.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 425
70	Debe permitir el uso de agentes persistentes, evanescentes (desaparecen luego de realizado en análisis) o pasivos.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 65
71	Si un dispositivo no pasa los tests de Compliance, debe ser posible no forzar la remediación, forzar la remediación inmediatamente, enviando al dispositivo a una red de cuarentena o permitir la remediación retardada, dando un período de tiempo desde la detección inicial de problemas, para la solución de estos. Pasado el período de tolerancia, de persistir los problemas, el dispositivo debe ser puesto en cuarentena inmediatamente.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 539
Características Mínimas de Respuesta Incidentes			

72	Debe permitir la construcción de reglas de seguridad que se activen ante eventos de seguridad definidos por el administrador, para generar alarmas de seguridad.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 719
73	Ante una alarma de seguridad debe permitir el bloqueo o aislamiento automático de los hosts comprometidos.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 721
74	Debe permitir homogeneizar los niveles de severidad de los mensajes de syslog de múltiples dispositivos externos.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 721
75	Debe permitir la creación, modificación y borrado de acciones que puedan ser asociadas a una alarma.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 721
76	Las acciones por ejecutar deben incluir, al menos: Ejecución de un script de comandos, enviar una alarma a un log externo, enviar un mensaje de correo electrónico al usuario o a los administradores, cambiar el rol del host involucrado, deshabilitar el host, deshabilitar el puerto de conexión, revalidar el estado de compliance del host, marcar el host como En Riesgo, marcar el host como Seguro.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 733
77	Debe poder integrarse con Firewalls, Scanners de Vulnerabilidad y otras soluciones de seguridad de terceros, incluyendo: Checkpoint, Fortinet, Palo Alto. Ante la detección de una amenaza, estos dispositivos enviarán a la solución un reporte que le permita tomar acción.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 738
INTEGRACIÓN			
78	La solución debe poder interoperar con dispositivos de conexión cableada e inalámbrica de los principales fabricantes, incluyendo, como mínimo: HP/HP Procurve/H3C/Aruba, Cisco, Extreme, Huawei	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 307
79	La solución debe permitir la integración de dispositivos de infraestructura de seguridad de terceras partes, incluyendo: CheckPoint, , Cisco FireEye, Fortinet, Juniper, Palo Alto, Qualys, SonicWall, Tenable, MobileIron, MaaS360, Citrix XenMobile,	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 307
80	La solución debe permitir la integración de Servicios de Directorios y Sistemas Operativos, incluyendo: RADIUS: Microsoft IAS, LDAP: Microsoft Active Directory, Microsoft Windows, Linux, Android.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 307
81	La solución debe permitir la integración de Aplicaciones de Seguridad de Endpoints, incluyendo: Kaspersky	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 488
82	La solución debe contar con un método genérico de integración de dispositivos, mediante la recepción, análisis e interpretación de mensajes de Syslog.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 693

83	La solución debe incluir una REST API que permita: Obtener información detallada sobre un elemento en particular, tal como un usuario o un host; Interrogar a la base de datos para obtener información sobre un conjunto de dispositivos; Actualizar los registros de usuarios o dispositivos; Bloquear o desbloquear el acceso de un usuario o dispositivo a la red.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 12
CARACTERÍSTICAS MÍNIMAS DE ADMINISTRACIÓN			
84	La solución debe permitir distintos roles administrativos, incluyendo la capacidad de limitar y controlar la cantidad de acceso permitido a las funcionalidades disponibles, dependiendo del grupo administrativo de la organización al que pertenezca el usuario. Por ejemplo: Help Desk, Operaciones de Red, Operaciones de Seguridad.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 88
85	La solución debe proveer información de auditoría de todas las conexiones de la red, tanto cableadas como inalámbricas. Esto debe incluir una interfaz amigable, que permita buscar y generar consultas en la información almacenada.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 661
86	La solución debe incluir información de auditoría de todas las acciones y cambios realizados al sistema por los usuarios administradores, incluyendo qué se cambió, cuándo se cambió y quién lo cambió.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 661
CARACTERÍSTICAS MÍNIMAS DE REPORTES			
87	Debe contar con un Tablero de Control que presente información relevante de manera resumida.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 822
88	El Tablero de Control debe poder ser modificable para permitir el despliegue de la información que el Administrador considere más relevante.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 822
89	Debe contar con reportes predefinidos que incluyan resultados sobre: Registro de Invitados; Registro de dispositivos; Escaneo de Dispositivos.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 822
90	Debe permitir la generación de reportes a medida entre otros: Registro de usuarios y Dispositivos; Falla en los Registros; Logs de Conexión.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 828
91	Debe permitir la generación y archivado de reportes periódicos.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 854
92	Debe permitir el envío automatizado de reportes mediante correo electrónico.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 822
93	Debe contar con reportes de Compliance	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 865

94	La información de los reportes debe poder ser exportada en formato HTML, CSV, Excel, XML, RTF o PDF.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 831
95	El log de alarmas debe poder ser ordenado por severidad.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 835
96	Debe permitir la aceptación y eliminación de alarmas del log de forma manual y automática.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 888
97	Debe poder integrarse con la plataforma de reportería con la que cuenta la entidad, para el envío de logs y generación de reportes.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 822
98	Debe poder enviar logs a la plataforma de SIEM del SOC de la entidad.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FORTINAC - HOJA DE DATOS - PAG. 1
99	Debe permitir la definición de alarmas en función de la ocurrencia de determinados eventos.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	FortiNAC-920-AdminGuide - PAG. 822
IMPLEMENTACIÓN			
100	La solución deberá incluir el diseño de la arquitectura y políticas de acuerdo con las necesidades de la entidad y su implementación y puesta en funcionamiento.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
101	Implementación de la solución de acuerdo con las mejores prácticas del fabricante, teniendo en cuenta una arquitectura de red segura.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
102	El proveedor deberá realizar un análisis de la arquitectura de red actual, con el fin de aplicar las mejores prácticas para la implementación	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
103	Planeación de cada una de las actividades, validadas en conjunto con los ingenieros designados por el supervisor del contrato, el entregable es el plan de trabajo a ejecutar.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
104	Realizar las actividades necesarias para la configuración y puesta en marcha de plataforma de seguridad y estabilización de la plataforma.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos

105	Configuración y alistamiento del software y de la máquina virtual a la última versión estable aprobada por el fabricante.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
106	La solución será responsabilidad del proveedor hasta el recibo a satisfacción por parte del supervisor del contrato.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
107	Se deben contemplar todos los servicios profesionales necesarios para la implementación e integración con los elementos de seguridad de la Entidad. El personal que ejecute los servicios de implementación, configuración y soporte de la solución debe ser certificado por el respectivo fabricante.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
108	Configuración y alistamiento del software y máquina virtual a la última versión estable aprobada por el fabricante	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
109	Se debe elaborar plan de pruebas de la solución para su ejecución y documentar los resultados.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
LICENCIAMIENTO			
110	La solución debe incluir el licenciamiento perpetuo para todas las funcionalidades.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
SOPORTE Y GARANTÍA			
111	Entregar el documento en el cual conste el soporte y garantía de la solución implementada, por parte del proveedor, durante un periodo de tres (3) años, posterior al recibo a satisfacción	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
112	Prestar los servicios de soporte, entrega de licenciamiento, hardware y software en las instalaciones de la entidad ubicada en el nivel central.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
113	La solución debe tener garantía y soporte técnico de fábrica en esquema 7x24x365, durante tres (3) años	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
114	La solución debe contar con soporte técnico y retorno de hardware por parte del fabricante por un periodo de 3 años en un esquema 7x24x365, incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
115	El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario hábil y no hábil por el tiempo contratado	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos

116	Se deben incluir actividades de mantenimiento, las cuales se realizarán como mínimo un (1) mantenimiento preventivo al año para minimizar problemas y mantener los sistemas actualizados, cuando este sea requerido por la entidad, durante el periodo de garantía y soporte que es de tres (3) años. En cuanto a los mantenimientos correctivos se deben realizar los que sean necesarios con el fin de garantizar la disponibilidad del servicio, durante el periodo de garantía y soporte que es de tres (3) años.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
117	Se deben incluir las actividades necesarias para atender las solicitudes de la CGR durante el contrato, que podrán incluir las siguientes actividades:	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
	• Cambios de Configuraciones.		
	• Acompañamiento en migraciones.		
	• Consultas e implementación de nuevas funcionalidades		
118	Realizar visitas cada tres (3) meses durante la vigencia del contrato en las cuales se deben validar las configuraciones de los equipos y realizar los ajustes correspondientes en las reglas de configuración y realizar las recomendaciones que se requieran a los administradores de las plataformas.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
119	Mantener actualizados los niveles de firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
120	Al finalizar cada visita correctiva y/o preventiva el proveedor deberá generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones, y si hubo cambio de software y/o en la configuración.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
121	El horario de atención para el mantenimiento correctivo y preventivo deberá ser de 7x24 en sitio, sin costo adicional para la entidad.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
DOCUMENTACIÓN			
122	Realizar y documentar entre otras, las siguientes actividades:	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
	• Nuevas configuraciones y migraciones solicitadas por la Entidad.		
	• Configuración e implementación de la solución, con el resultado de las pruebas incluyendo evidencias (captura de pantallas, fotos)		
CAPACITACIONES Y TRANSFERENCIA DE CONOCIMIENTO			
123	Realizar transferencia de conocimientos para seis (6) funcionarios de la entidad, la cual debe incluir por lo menos temas de administración, configuración y afinamiento de la solución implementada.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos

124	El proveedor debe brindar capacitación oficial de fabricante para cinco (5) funcionarios de la entidad sobre la operación y administración de la solución.	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos
ACUERDOS DE NIVELES DE SERVICIO		Se detallan en la cláusula 3	
CERTIFICADO DE FABRICANTE			
126	El oferente debe contar con el máximo nivel de membresía del fabricante, para lo cual debe adjuntar el certificado de distribuidor autorizado del fabricante con fecha no mayor a 60 días anteriores al cierre del proceso, donde se evidencie el nivel de membresía. Las certificaciones deben dirigirse a la Contraloría General de la República	Appliance virtual: FNC-CAVM Licenciamiento: LIC-FNACPRO	Enterados, aceptamos y cumplimos

CONTRATO DE ADQUISICIÓN DE BIENES Y SERVICIOS No. CGR-BID-028-2022

Países Elegibles

1) Países Miembros

Alemania, Argentina, Austria, Bahamas, Barbados, Bélgica, Belice, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Croacia, Dinamarca, Ecuador, El Salvador, Eslovenia, España, Estados Unidos, Finlandia, Francia, Guatemala, Guyana, Haití, Honduras, Israel, Italia, Jamaica, Japón, México, Nicaragua, Noruega, Países Bajos, Panamá, Paraguay, Perú, Portugal, Reino Unido, República de Corea, República Dominicana, República Popular de China, Suecia, Suiza, Surinam, Trinidad y Tobago, Uruguay, y Venezuela.

2) Criterios para determinar Nacionalidad y el país de origen de los bienes y servicios

Para efectuar la determinación sobre: a) la nacionalidad de las firmas e individuos elegibles para participar en contratos financiados por el Banco y b) el país de origen de los bienes y servicios, se utilizarán los siguientes criterios:

A) Nacionalidad

a) **Un individuo** tiene la nacionalidad de un país miembro del Banco si él o ella satisface uno de los siguientes requisitos:

   (i) es ciudadano de un país miembro; o
   (ii) ha establecido su domicilio en un país miembro como residente "bona fide" y está legalmente autorizado para trabajar en dicho país.

b) **Una firma** tiene la nacionalidad de un país miembro si satisface los dos siguientes requisitos:

   (i) esta legalmente constituida o incorporada conforme a las leyes de un país miembro del Banco; y
   (ii) más del cincuenta por ciento (50%) del capital de la firma es de propiedad de individuos o firmas de países miembros del Banco.

Todos los socios de una asociación en participación, consorcio o asociación (APCA) con responsabilidad mancomunada y solidaria y todos los subcontratistas deben cumplir con los requisitos arriba establecidos.

B) Origen de los Bienes

Los bienes se originan en un país miembro del Banco si han sido extraídos, cultivados, cosechados o producidos en un país miembro del Banco. Un bien es producido cuando mediante manufactura, procesamiento o ensamblaje el resultado es un artículo comercialmente reconocido cuyas características básicas, su función o propósito de uso son substancialmente diferentes de sus partes o componentes.

En el caso de un bien que consiste de varios componentes individuales que requieren interconectarse (lo que puede ser ejecutado por el suministrador, el comprador o un tercero) para lograr que el bien pueda operar, y sin importar la complejidad de la interconexión, el Banco considera que dicho bien es elegible para su financiación si el ensamblaje de los componentes individuales se hizo en un país miembro. Cuando el bien es una combinación de varios bienes individuales que normalmente se empacan y venden comercialmente como una sola unidad, el bien se considera que proviene del país en donde este fue empacado y embarcado con destino al comprador.

Para efectos de determinación del origen de los bienes identificados como "hecho en la Unión Europea", estos serán elegibles sin necesidad de identificar el correspondiente país específico de la Unión Europea.

El origen de los materiales, partes o componentes de los bienes o la nacionalidad de la firma productora, ensambladora, distribuidora o vendedora de los bienes no determina el origen de los mismos

C) Origen de los Servicios

El país de origen de los servicios es el mismo del individuo o firma que presta los servicios conforme a los criterios de nacionalidad arriba establecidos. Este criterio se aplica a los servicios conexos al suministro de bienes (tales como transporte, aseguramiento, montaje, ensamblaje, etc.), a los servicios de construcción y a los servicios de consultoría.