

CONVOCATORIA ABREVIADA N°012-2026
CRONOGRAMA

OBJETO: Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet.

N°	ETAPA	FECHA Y HORA
1	Envío condiciones de la contratación, vía correo electrónico (Mínimo 3 invitados) y publicación de la convocatoria en plataforma Web (Página Web de la Empresa)	28/04/2026 Hasta las 12:00 horas
2	Presentación de observaciones y/o solicitud de aclaraciones a las condiciones de la contratación.	29/04/2026 Hasta las 18:00 horas
3	Respuesta a las observaciones y/o aclaraciones y/o adendas, según corresponda y publicación en plataforma Web (Página Web de la Empresa).	04/05/2026 Hasta las 17:00 horas.
4	Presentación de propuestas.	06/05/2026 Hasta las 17:00 horas
5	Acta en la que consten los nombres de los oferentes, fecha y hora de presentación de las propuestas y publicación en plataforma Web (Página Web de la Empresa).	07/05/2026 Hasta las 12:00 horas.
6	Evaluación de propuestas y/o solicitudes de subsanación y/o envío de informe preliminar y publicación en plataforma Web (Página Web de la Empresa).	08/05/2026 Hasta las 16:00 horas.
7	Presentación de observaciones al informe de evaluación preliminar y/o aclaraciones y/o subsanaciones de las ofertas.	11/05/2026 Hasta las 18:00 horas
8	Respuesta a las observaciones y publicación del informe de evaluación definitivo en plataforma Web (Página Web de la Empresa).	13/05/2026 Hasta las 16:00 horas.
9	Comunicación de aceptación de la propuesta.	14/05/2026 Hasta las 15:00 horas.

**Versionamiento Formato**

Código: FO33-DE-GDCO
Versión: 1.0
Fecha actualización: 20/10/2023

Medellín, 28 de abril de 2026

Convocatoria Abreviada N° 012-2026

Objeto: *“Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet.”*

VALOR+ S.A.S.

VALOR+ S.A.S – NIT. 900969726-2
Dirección: Carrera 42 # 52-28 piso 3 Avenida Camellón de la Alpujarra – Edificio Edatel
Teléfono: 444-37-47 Ext. 203
Email: recepcion@valormas.gov.co

Contenido:

1. GENERALIDADES	4
1.1 Información General	4
1.1.1 Contexto	4
1.2 Cronograma del Proceso	5
1.3 Comunicaciones del Proceso	6
1.4 Objeto del Contrato	6
1.5 Alcance y Condiciones y/o Especificaciones Técnicas del Bien o Servicio a Contratar	6
1.6 Plazo de Ejecución	10
1.7 Valor (Presupuesto estimado) y Certificado de Disponibilidad Presupuestal (CDP)	10
1.8 Forma de Pago	10
1.9 Monto y Vigencia de las Garantías	11
1.10 Obligaciones Generales:	11
1.10.1 Del Proveedor	12
1.10.2 Del contratante	12
1.11 Obligaciones Específicas	12
2. REQUISITOS DE ADMISIBILIDAD O HABILITANTES	13
2.1 Capacidad Jurídica:	13
2.2 Capacidad Técnica:	14
2.3 Capacidad Financiera:	15
2.4 Capacidad Organizacional:	15
3. CRITERIOS DE SELECCIÓN	16
3.1 Oferta más Favorable	16
3.2 Criterios de Desempate	16
3.3 Procedimiento del sorteo (método aleatorio)	18
3.4 Causales de Rechazo	18
4. EVALUACIÓN DE PROPUESTAS	19
4.1 Fórmula Evaluación Propuesta	20
4.2 Informe de evaluación	21
4.3 Reglas de Subsanción	21
4.4 Suspensión o Cancelación del Proceso de Contratación	21
5. REGLAS PARA LA PRESENTACIÓN DE PROPUESTAS	22
5.1 Propuesta Económica	22
5.2 Estampillas	22



Versionamiento Formato

Código:	FO33-DE-GDCO
Versión:	1.0
Fecha actualización:	20/10/2023

5.3 Validez de la Oferta.....	22
5.4 Rondas de Negociación	22
5.5 Única Oferta.....	23
5.6 Idioma	23
5.7 Anexos.....	23

CONDICIONES DE LA CONTRATACIÓN

1. GENERALIDADES

1.1 Información General

Valor+ S.A.S., es una filial del IDEA, dedicada al desarrollo y ejecución de actividades tendientes a la prestación, comercialización y consultoría para todas aquellas entidades que hacen parte del conglomerado público de la Gobernación de Antioquia, prestando soluciones integrales para la administración y gestión de la información, de recursos y las comunicaciones, mediante la operación de servicios de valor agregado que incluyen: gestión de procesos de soporte, recaudo y facturación, administración de infraestructura tecnológica, BPO (externalización de procesos de negocios), contact center, conectividad, gerenciamiento, diseño, arquitectura, proyectos, infraestructura, construcción, operaciones de alta complejidad logística y tecnológica, diseño de estudios técnicos y/o civiles, entre otras actividades conexas o similares.

Así mismo, Valor+ S.A.S., en virtud de su actividad comercial, objeto y los servicios TIC que presta, se encuentra registrada como empresa de las tecnologías de la información y las telecomunicaciones (TIC), contando con el código de registro N° 960003269 del 28 de junio de 2016 expedido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones, sometida en particular al régimen jurídico especial descrito en la Ley 1341 de 2009.

Por tal motivo, el marco legal del presente proceso y del contrato que de él se derive, está conformado por la Constitución Política, el Manual de Contratación de la entidad, las normas del derecho privado y demás disposiciones legales sobre la materia.

La información que se consigna a continuación contiene las condiciones básicas para la presentación de la oferta, y los interesados deben verificarla completamente.

El hecho de que los posibles oferentes no se informen y documenten debidamente sobre los detalles y condiciones bajo los cuales se contratará, no se considerará como excusa válida para la eventual formulación de posteriores reclamaciones.

La presentación de la oferta se considerará como manifestación expresa de que el o los oferentes han analizado este documento y demás anexos que hacen parte de este, y han obtenido las aclaraciones necesarias sobre los puntos que considere inciertos o dudosos.

1.1.1 Contexto

Valor+ S.A.S., suscribió con el Departamento de Antioquia –Subsecretaría de Servicios Administrativos, el Contrato Interadministrativo N° 4600018598 de 2025, para: *“Servicios para la administración y operación de la mesa de servicios de la Gobernación de Antioquia, servicios de hosting corporativos y servicios de apoyo, para la apropiada operación de la plataforma tecnológica utilizada en la administración departamental”*.

El servicio requerido tiene como finalidad proteger los activos de información, la infraestructura tecnológica y los servicios institucionales ante el incremento de amenazas cibernéticas que pueden



afectar la confidencialidad, integridad y disponibilidad de la información pública administrada. Dicho servicio contempla la monitorización permanente de Internet, Deep Web y Darknet, con el fin de identificar a tiempo filtraciones de información, exposición de credenciales, fuga de datos, venta o intercambio de información institucional, así como cualquier actividad maliciosa o amenaza que pueda comprometer los sistemas de la Gobernación de Antioquia.

A continuación, se exponen los pilares que fundamentan la necesidad del servicio de Vigilancia Tecnológica, Gestión de Vulnerabilidades y Superficie de Ataque, este servicio se ejecutará bajo un enfoque integral, continuo, preventivo y proactivo; los tres (3) ejes fundamentales son los siguientes:

- 1. Vigilancia Tecnológica**
- 2. Gestión de Vulnerabilidades**
- 3. Gestión de Superficie de Ataque**

En resumen, la implementación de este servicio permitirá anticipar, detectar, alertar y mitigar riesgos de ciberseguridad antes de que se materialicen en incidentes, fortaleciendo la capacidad de respuesta y contención del riesgo tecnológico, y contribuyendo al cumplimiento de los lineamientos de seguridad establecidos para las entidades públicas, así como a la adecuada operación de la Mesa de Servicios y los servicios tecnológicos a cargo de VALOR+ S.A.S.

1.2 Cronograma del Proceso

Nº	ETAPA	FECHA Y HORA
1	Envío condiciones de la contratación, vía correo electrónico (Mínimo 3 invitados) y publicación de la convocatoria en plataforma Web (Página Web de la Empresa)	28/04/2026 Hasta las 12:00 horas
2	Presentación de observaciones y/o solicitud de aclaraciones a las condiciones de la contratación.	29/04/2026 Hasta las 18:00 horas
3	Respuesta a las observaciones y/o aclaraciones y/o adendas, según corresponda y publicación en plataforma Web (Página Web de la Empresa).	04/05/2026 Hasta las 17:00 horas.
4	Presentación de propuestas.	06/05/2026 Hasta las 17:00 horas
5	Acta en la que consten los nombres de los oferentes, fecha y hora de presentación de las propuestas y publicación en plataforma Web (Página Web de la Empresa).	07/05/2026 Hasta las 12:00 horas.
6	Evaluación de propuestas y/o solicitudes de subsanación y/o envío de informe preliminar y publicación en plataforma Web (Página Web de la Empresa).	08/05/2026 Hasta las 16:00 horas.
7	Presentación de observaciones al informe de evaluación preliminar y/o aclaraciones y/o subsanaciones de las ofertas.	11/05/2026 Hasta las 18:00 horas
8	Respuesta a las observaciones y publicación del informe de evaluación definitivo en plataforma Web	13/05/2026 Hasta las 16:00 horas.

	(Página Web de la Empresa).	
9	Comunicación de aceptación de la propuesta.	14/05/2026 Hasta las 15:00 horas.

1.3 Comunicaciones del Proceso.

Todas las comunicaciones que los interesados o proponentes pretendan realizar dentro del proceso de contratación se deberán tramitar (Enviar), a través del correo electrónico compras2@valormas.gov.co este será el **único canal de comunicación oficial del proceso**, para recibir observaciones, solicitudes, requerimientos, propuestas, subsanaciones y demás actuaciones.

Las comunicaciones que no sean tramitadas (Enviadas) a través de este medio, **no se tendrán en cuenta dentro del proceso.**

Todas las comunicaciones tramitadas (Enviadas) durante el proceso se deben identificar así: **"Convocatoria Abreviada N° 012-2026 (Vigilancia Tecnológica en Ciberseguridad)"**.

Asunto: **"(Observación, Propuesta, subsanación, entre otros)"**, lo que corresponda.

1.4 Objeto del Contrato

Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet.

1.5 Alcance y/o Condiciones y/o Especificaciones Técnicas del Bien o Servicio a Contratar

El objeto del presente contrato comprende la prestación de servicios de vigilancia tecnológica en ciberseguridad, orientados a la identificación, evaluación, monitoreo y mitigación de riesgos asociados a amenazas cibernéticas que puedan comprometer la infraestructura tecnológica y la información de la Gobernación de Antioquia.

Se requiere que el proponente desarrolle y cumpla con lo siguiente:

Descripción / Características	Unidad de medida / Meses
Vigilancia Tecnológica	8
Gestión de Vulnerabilidades	8
Gestión de Superficie de Ataque	8

➤ Servicio de Vigilancia Tecnológica, Gestión de Vulnerabilidades y Superficie de Ataque:

El servicio se ejecutará bajo un enfoque integral, continuo, preventivo y proactivo, estructurado en **(3) ejes fundamentales**, desarrollados de manera articulada, y en cumplimiento de estándares, marcos de referencia y buenas prácticas internacionales en materia de seguridad de la información.

Ejes Fundamentales:

1. **Vigilancia Tecnológica:** Durante la ejecución del contrato, el Proveedor deberá desarrollar actividades de vigilancia tecnológica e inteligencia de amenazas, mediante el monitoreo continuo de fuentes abiertas (OSINT), así como de entornos de Internet, Deep Web y Dark Web. Lo anterior con el propósito de identificar de forma oportuna posibles filtraciones de información, exposición de credenciales institucionales, menciones de la entidad en espacios no autorizados, distribución indebida de información sensible, campañas de ataque y cualquier otra amenaza relevante.

Para el cumplimiento de esta obligación, el Proveedor deberá emplear plataformas especializadas de inteligencia de amenazas (Threat Intelligence), cuya selección deberá estar debidamente sustentada mediante criterios técnicos, funcionales y de cobertura.

Esta actividad deberá complementarse con la entrega periódica de informes ejecutivos y técnicos, los cuales deberán contener como mínimo: los hallazgos identificados, su nivel de criticidad, análisis de riesgo, posibles impactos para la entidad y recomendaciones claras y accionables para la mitigación y gestión de las amenazas detectadas.

2. **Gestión de Vulnerabilidades,** El Proveedor deberá prestar el servicio integral de gestión de vulnerabilidades, el cual comprende la identificación, análisis, clasificación, priorización, tratamiento y seguimiento de vulnerabilidades sobre la infraestructura tecnológica de la entidad, incluyendo: activos internos, activos expuestos en Internet, aplicaciones web y servicios en la nube.

El servicio deberá ejecutarse mediante la **realización de escaneos de seguridad con una periodicidad mínima mensual**, así como la ejecución de análisis extraordinarios bajo demanda, en respuesta a incidentes de seguridad, cambios o solicitud expresa de la entidad. Como resultado, el Proveedor deberá **entregar informes técnicos detallados y reportes ejecutivos que incluyan hallazgos, nivel de criticidad, evidencias, recomendaciones de mitigación y planes de remediación.**

Para la clasificación y priorización de vulnerabilidades, el Proveedor deberá aplicar estándares internacionales, tales como el modelo CVSS (Common Vulnerability Scoring System). En el caso de aplicaciones web, deberá adoptar las buenas prácticas establecidas por OWASP (Open Web Application Security Project), y para la ejecución de pruebas técnicas, deberá alinearse con lo establecido en el marco metodológico NIST SP 800-115. Asimismo, las actividades deberán estar articuladas con el marco MITRE ATT&CK, incorporando enfoques como Adversary Emulation, Red Teaming y Threat Hunting, orientados a fortalecer la capacidad de detección y respuesta ante amenazas avanzadas. **Deberá presentar certificado manifestando que aplica los estándares y buenas prácticas solicitadas en el párrafo anterior.**

El Proveedor deberá disponer de un **componente de personal especializado** para la gestión de vulnerabilidades, el cual será responsable de la operación continua del servicio. Este equipo deberá garantizar la gestión integral del ciclo de vida de las vulnerabilidades, desde su identificación hasta su cierre, incluyendo la validación de la remediación aplicada. De igual forma, deberá coordinar con las áreas técnicas de la entidad la implementación de controles correctivos, realizar seguimiento a los planes de acción y asegurar la trazabilidad de cada hallazgo.

El personal asignado deberá contar con formación profesional en áreas afines a tecnologías de la información y ciberseguridad, así como certificaciones vigentes de reconocimiento internacional, tales como CEH, OSCP, CISA, CISSP o equivalentes. Adicionalmente, deberán acreditar experiencia comprobada en la ejecución de pruebas de seguridad, análisis de vulnerabilidades y gestión de riesgos tecnológicos. **Deberá presentar certificado manifestando que cuenta con el equipo para garantizar la prestación del servicio y que cumple con las certificaciones y experiencia requerida.**

El Proveedor será responsable de garantizar la confidencialidad, integridad y disponibilidad de la información a la que tenga acceso en el desarrollo del contrato, así como del cumplimiento de las políticas de seguridad de la entidad y la normativa vigente aplicable. **Deberá presentar certificado manifestando que garantiza lo anterior.**

3. **La Gestión de Superficie de Ataque:** En desarrollo del objeto contractual, el Proveedor deberá iniciar con el levantamiento, identificación, clasificación y análisis de la infraestructura tecnológica de la entidad, incluyendo los activos de información, plataformas, servicios, aplicaciones y demás componentes que conforman el ecosistema digital institucional. Este ejercicio deberá permitir la identificación de activos críticos, sus dependencias, niveles de exposición y posibles vectores de ataque, constituyéndose como base para la priorización de actividades de vigilancia, análisis y gestión de riesgos.

Con fundamento en lo anterior, el Proveedor deberá implementar un proceso de Gestión de Superficie de Ataque Cibernético, orientado al descubrimiento, inventario, monitoreo y análisis continuo de todos los activos tecnológicos expuestos públicamente por la entidad. Esto incluye, entre otros, dominios y subdominios, direcciones IP públicas, servicios expuestos, certificados digitales y tecnologías web identificadas, con el propósito de minimizar la exposición no intencionada, fortalecer la postura de seguridad y anticipar posibles vectores de ataque mediante la identificación proactiva de riesgos y vulnerabilidades asociadas a dichos activos.

De manera complementaria, el Proveedor deberá realizar una evaluación integral del riesgo cibernético institucional, considerando el contexto actual de amenazas, la probabilidad de ocurrencia de incidentes de seguridad y su impacto potencial a nivel operativo, técnico, legal y reputacional. **Como resultado, se deberá entregar una valoración objetiva y cuantificable del riesgo, que sirva como insumo para la toma de decisiones estratégicas por parte de la entidad.**

El servicio deberá contemplar entre otros los siguientes entregables:

- Generación de alertas tempranas ante la detección de hallazgos críticos o de alto riesgo;
- Elaboración de informes técnicos mensuales que incluyan el análisis de hallazgos, su nivel de criticidad, tendencias identificadas, recomendaciones de mitigación y seguimiento a incidentes detectados;
- Actualización periódica del inventario de activos expuestos y su respectiva clasificación de riesgo.

Además, deberá realizar:

- **Levantamiento y análisis de la infraestructura tecnológica:**

- Realizar el levantamiento, clasificación y documentación de los activos tecnológicos objeto del servicio.
- Identificar los componentes críticos, dependencias, puntos vulnerables y niveles de exposición a amenazas externas e internas.
- Priorizar los activos auditables para determinar el alcance y nivel de profundidad del análisis, con el fin de dimensionar el universo sujeto a vigilancia y gestión de vulnerabilidades.

➤ **Evaluación del riesgo cibernético institucional:**

- Efectuar un análisis técnico y objetivo del nivel de riesgo al que se encuentra expuesta la entidad, considerando el entorno de amenazas actual, incidentes potenciales y el impacto operativo, reputacional, técnico y legal que un ataque podría generar.
- Determinar la probabilidad de ocurrencia de un ciberataque y su severidad, con base en amenazas reales identificadas y verificables.
- Presentar una valoración cuantificable del riesgo cibernético, permitiendo la toma de decisiones informadas por parte de la entidad.

➤ **Vigilancia tecnológica y monitoreo continuo:**

- Realizar monitoreo constante del entorno digital, Internet y Darknet, con el propósito de detectar amenazas emergentes, filtraciones de información, campañas de ataque, vulnerabilidades críticas, exposición de datos, o actos que puedan comprometer los intereses de la entidad.
- Emitir informes semanales detallados, que incluyan:
 - Hallazgos técnicos detectados.
 - Niveles de criticidad.
 - Riesgos asociados.
 - Tendencias o alertas relevantes.
 - Recomendaciones inmediatas de contención o mitigación.

➤ **Gestión y tratamiento de vulnerabilidades:**

- Identificar, analizar y categorizar las vulnerabilidades presentes en los sistemas, plataformas y/o dispositivos objeto del servicio.
- Emitir recomendaciones técnicas específicas, priorizadas según criticidad, para la corrección o mitigación de los riesgos identificados.
- Entregar lineamientos para la mejora continua del ecosistema de ciberseguridad, fortaleciendo los controles existentes y promoviendo prácticas preventivas.

El proveedor deberá ejecutar las actividades descritas, garantizando el cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad (ISO 27001, NIST, MITRE ATT&CK, OWASP, entre otros). Deberá presentar certificado manifestando que garantiza lo anterior.

Deberá ejecutar la gestión integral de vulnerabilidades, que comprende la identificación, análisis, clasificación, priorización y seguimiento de vulnerabilidades presentes en la infraestructura interna, activos expuestos en Internet, aplicaciones web y servicios en la nube. Estas actividades deberán realizarse con una periodicidad mínima mensual y de manera adicional cuando se presenten eventos

1.10.1 Del Proveedor

1. Cumplir con el objeto del contrato y sus especificaciones técnicas en los términos señalados en el mismo, así como en los estudios de conveniencia y la propuesta presentada.
2. Ejecutar el objeto del contrato en forma adecuada y eficiente, poniendo todo su conocimiento, experiencia y capacidad.
3. Cumplir a satisfacción las actividades u obligaciones específicas establecidas en objeto y alcance del contrato.
4. Cancelar los gastos de perfeccionamiento, ejecución, e impuestos que se generen debido al contrato.
5. Reportar a El Contratante y/o al supervisor del contrato toda la información que se requiera con el fin de que estos puedan verificar tanto el cumplimiento de los requisitos y compromisos contractuales como los legales a que haya lugar y cualquier novedad que se suscite.
6. Acatar las recomendaciones emanadas de los informes de supervisión e implementar inmediatamente los planes de acción y de mejoramiento que se requieran.
7. Mantener comunicación permanente con el supervisor del contrato, a fin de recibir orientaciones, evaluar el proceso y velar por el cumplimiento del objeto del contrato.
8. Presentar los informes que se le requieran sobre la ejecución y desarrollo del contrato.
9. Facilitar la labor al supervisor dando respuesta oportuna a las observaciones o requerimientos que se realicen y atender todos los requerimientos de la supervisión del contrato.
10. Participar en las reuniones de trabajo necesarias para la ejecución del contrato (programadas con antelación)
11. Informar oportunamente a El Contratante cuando exista o sobrevenga alguna de las inhabilidades e incompatibilidades previstas en la constitución y la ley.
12. Manifiestar bajo la gravedad de juramento, que se entiende prestado con la firma del presente contrato, estar a paz y salvo con El Contratante. Adicionalmente, autoriza a El Contratante para que, en el momento de un pago, automáticamente, sin previo aviso y siempre y cuando no exista Acuerdo de Pago vigente entre El Proveedor y El Contratante, hagan cruce de cuentas, para compensar los valores que tenga en mora por cualquier concepto.
13. Las demás que se requieran para el cumplimiento del contrato, de acuerdo con los lineamientos del objeto y alcance contractual.

1.10.2 Del contratante

1. Realizar el pago de acuerdo con lo establecido en la forma de pago.
2. Facilitar el acceso a la información que sea necesaria, de manera oportuna, para la debida ejecución del objeto del contrato.
3. Acompañar y vigilar el desarrollo de todo el proceso objeto del contrato.
Elaborar y suscribir el acta de inicio, liquidación y los demás documentos que se presenten con ocasión de la ejecución del contrato.
4. Las demás que se requieran para el cumplimiento del objeto y alcance contractual.

1.11 Obligaciones Específicas

N/A


Versionamiento Formato

Código: FO33-DE-GDCO
 Versión: 1.0
 Fecha actualización: 20/10/2023

2. REQUISITOS DE ADMISIBILIDAD O HABILITANTES

Los requisitos habilitantes son aquellos que miden la aptitud del proponente para participar en un proceso de contratación como oferente y eventualmente, para ejecutar el objeto y las obligaciones contractuales. El propósito de Valor+ S.A.S., al establecer los requisitos habilitantes es determinar unas condiciones mínimas que deben cumplir el o los oferentes y la forma cómo el interesado debe acreditarlas.

Los requisitos habilitantes serán objeto de verificación, por lo tanto, únicamente se consideran habilitados aquellos oferentes que cumplan con todos los requisitos solicitados. Se evaluarán como "Cumple". En caso contrario, se evaluarán como "No cumple" y, por tanto, no será objeto de evaluación en los requisitos de calificación, sin perjuicio de la subsanación que el o los oferentes puedan realizar en el término que otorgue Valor+ S.A.S.

A su vez, se revisará que los proponentes no se encuentren en causales de inhabilidad o incompatibilidad para presentar la oferta, celebrar o ejecutar el contrato. Para ello, revisará entre otros, el boletín de responsables fiscales, el certificado de antecedentes disciplinarios, el certificado de antecedentes judiciales, entre otros.

Igualmente, todos los oferentes deben diligenciar y firmar los siguientes formatos anexos:

- Inhabilidades e Incompatibilidades
- Habeas Data - Autorización tratamiento de datos personales
- SARLAFT - Certificado lavado de activos y financiación del terrorismo

2.1 Capacidad Jurídica:

En el presente proceso de contratación, pueden participar personas jurídicas cuyo objeto social les permita participar de acuerdo con el objeto del proceso, y acrediten los requisitos de admisibilidad o habilitantes solicitados y demuestren su capacidad jurídica, mediante la presentación de los siguientes documentos:

N°	DOCUMENTO
1	Carta de presentación de la propuesta debidamente diligenciada.
2	Certificado de existencia y representación legal del proponente, con fecha de expedición no mayor a treinta (30) días anteriores a la fecha de presentación de la oferta.
3	Acta de la Junta o Asamblea que autoriza al representante legal del Proponente a presentar la oferta, cuando se trate de persona jurídica (Si aplica).
4	Certificado de estar a paz y salvo con el sistema de seguridad social integral (salud, pensión, riesgos profesionales y ARL) y aportes parafiscales (ICBF, Sena y Cajas de Compensación Familiar), expedido por el representante legal y/o contador o revisor fiscal (adjuntando copia de la cédula, copia de la tarjeta profesional y certificado de antecedentes disciplinarios expedido por la junta central de contadores del contador) o Planilla integrada de autoliquidación de aportes a la seguridad social integral y aportes parafiscales.
5	Copia del documento de identidad del representante legal o apoderado.
6	Copia del registro único tributario – RUT

VALOR+ S.A.S – NIT. 900969726-2

Dirección: Carrera 42 # 52-28 piso 3 Avenida Camellón de la Alpujarra – Edificio Edatel

Teléfono: 444-37-47 Ext. 203

Email: recepcion@valormas.gov.co

7	Certificado Registro de Deudores Alimentarios Morosos – REDAM, la consulta del certificado deberá atender al nombre e identificación del representante legal.
8	Certificado de la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST, emitido por la ARL o el Ministerio del Trabajo, con vigencia no mayor a noventa (90) días antes de la presentación de la oferta.
9	Boletín de responsabilidad fiscal (Contraloría) del Proponente y su representante legal (Cuando se trate de personas jurídicas).
10	Certificado de antecedentes disciplinarios (Procuraduría) del Proponente y su representante legal (Cuando se trate de personas jurídicas).
11	Certificado de antecedentes judiciales (Policía Nacional) del Representante Legal.
12	Certificado de Registro de Medidas Correctivas (Policía Nacional) del Representante Legal.
13	Certificado Antecedentes de delitos sexuales (Policía Nacional) cometidos contra menores de 18 años del Representante legal.
14	Certificación Bancaria.
15	Formato Inhabilidades e Incompatibilidades Persona Jurídica diligenciado.
16	Formato Autorización tratamiento de datos personales diligenciado.
17	Formato Certificación de lavado de activos y financiación del Terrorismo diligenciado.
18	Garantía de seriedad de la propuesta.
19	Registro Único de Proponentes – RUP renovado y en firme. Los proponentes deberán estar inscritos y clasificados en el Registro Único de Proponentes de la Cámara de Comercio de su jurisdicción, de acuerdo con las condiciones establecidas en el Título VI Registro Único de Proponentes –RUP del Decreto 1082 de 2015. La expedición de dicho certificado no podrá tener una anterioridad superior a treinta (30) días calendario, contado a partir de la fecha de cierre del proceso. En caso de no contar con el RUP renovado en firme, se deberán aportar Balances o Estados Financieros aprobados del año inmediatamente anterior.
20	Manifestación Juramentada de Ausencia de Multas y/o Sanciones: El proponente deberá hacer manifestación juramentada de ausencia o presencia de multas y/o sanciones impuestas por entidades públicas en los cinco (5) últimos años anteriores al cierre de esta convocatoria. En caso de que el proponente haya sido multado o sancionado, deberá allegar con su oferta una certificación expedida por el representante legal en donde informe la ocurrencia del hecho y la Entidad que la hizo efectiva o la impuso según el caso, o en su defecto, copia del acto administrativo por medio del cual se impuso la sanción o multa, con el fin de verificar su alcance.

La expedición de los certificados no podrá tener una anterioridad superior a treinta (30) días calendario, contado a partir de la fecha de cierre del proceso.

En caso de que la persona jurídica tenga menos de tres (3) años de constitución, podrá aportar experiencia de los socios, siempre y cuando guarde relación con el objeto del presente proceso. Para esto, deberá aportar certificado donde conste la conformación de la sociedad, con el fin de validar dicha experiencia.

2.2 Capacidad Técnica:

Para la verificación de la experiencia se tomarán los contratos ejecutados por el proponente, que

registren en el (Formato anexo de Experiencia Técnica), con los cuales pretende acreditar las condiciones mínimas exigidas.

La evaluación de la propuesta incluirá un análisis de la capacidad técnica del oferente, de tal manera que la ejecución del contrato sea coherente con su propuesta, de acuerdo con los requisitos establecidos en este documento:

Para ser considerado hábil, el proponente deberá acreditar la cuantía en máximo dos (2) contratos relacionados con el objeto del presente proceso, en ejecución, ejecutados o terminados a la fecha de cierre de la convocatoria y cuya sumatoria sea igual o superior al presupuesto oficial establecido para esta contratación.

Las certificaciones deberán contener por lo menos la siguiente información:

- Contratante.
- Proveedor.
- Objeto.
- Valor.
- Plazo.
- Estado: (en ejecución, ejecutado o terminado)

Los certificados de experiencia deben ser en idioma español.

Para los contratos en ejecución, adicionalmente se deberá certificar cual es el valor ejecutado a la fecha.

2.3 Capacidad Financiera:

Los requisitos financieros para participar en el presente proceso serán verificados a partir de la información que deberá aportar el proponente en el correspondiente Registro Único de Proponentes (RUP) debidamente actualizado y renovado y/o aportar Balances o Estados Financieros aprobados del año inmediatamente anterior.

Para validar la capacidad financiera, el oferente deberá aportar los siguientes indicadores:

INDICADOR	FÓRMULA	INDICADOR
Índice de Liquidez	$\frac{\text{Activo corriente}}{\text{Pasivo Corriente}}$	Mayor o igual a 1.3
Índice de endeudamiento	$\frac{\text{Activo Total}}{\text{Pasivo Total}}$	Menor o igual al 60%
Razón de Cobertura de Intereses	$\frac{\text{Utilidad operacional}}{\text{Gasto de Intereses}}$	Mayor o igual a 2.0

2.4 Capacidad Organizacional:

Para validar la capacidad organizacional se tomará la información que aparezca en el Registro Único de Proponentes (RUP) y/o Balances o Estados Financieros aprobados del año inmediatamente anterior, según las mismas indicaciones dadas en el numeral anterior, es decir que, el o los oferentes deberán aportar los siguientes indicadores:

FACTOR EVALUACIÓN	FORMULA	CRITERIO
Indicadores de Rentabilidad		
ROE	$\frac{\text{Utilidad Operacional}}{\text{Patrimonio}}$	Mayor o igual al 5%
ROA	$\frac{\text{Utilidad Operacional}}{\text{Activo Total}}$	Mayor o igual al 2%

3. CRITERIOS DE SELECCIÓN

3.1 Oferta más Favorable

Las ofertas que se reciban en virtud del presente proceso de selección serán, en todo caso, objeto de verificación de las condiciones establecidas para la escogencia del Proveedor. **Las propuestas presentadas deben ser económicas y técnicas respecto del desarrollo a ejecutar.**

Los criterios de selección que permitan identificar la oferta más favorable para Valor+ S.A.S., serán: Valor o precio del ofrecimiento, especificaciones técnicas, experiencia, apoyo a la industria nacional y emprendimiento y empresas de mujeres y la forma de ponderación o de evaluación de dichos factores.

3.2 Criterios de Desempate

En caso de presentarse empate en el puntaje total de dos o más ofertas, Valor+ S.A.S., dará aplicación a los criterios de desempate establecidos en el artículo 35 de la Ley 2069 de 2020 de forma sucesiva y excluyente para seleccionar al aferente favorecido.

Si persiste el empate, Valor+ S.A.S., debe utilizar las siguientes reglas de forma sucesiva y excluyente para seleccionar el oferente favorecido.

Lo anterior, de conformidad con los criterios de desempate establecidos en el artículo 35 de la Ley 2069 de 2020 Factores de desempate.

En caso de empate en el puntaje total de dos o más ofertas en los Procesos de Contratación realizados con cargo a recursos públicos, los Procesos de Contratación realizados por las Entidades Estatales indistintamente de su régimen de contratación, así como los celebrados por los Procesos de Contratación de los patrimonios autónomos constituidos por Entidades Estatales, el contratante deberá utilizar las siguientes reglas de forma sucesiva y excluyente para seleccionar al oferente favorecido, respetando en todo caso los compromisos internacionales vigentes.

1. Preferir la oferta de bienes o servicios nacionales frente a la oferta de bienes o servicios extranjeros.
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.
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. Si la oferta es presentada por un proponente plural, el integrante del oferente que acredite que el diez por ciento (10%) de su nómina está en condición de discapacidad en los términos del presente numeral, debe tener una participación de por lo menos el veinticinco por ciento (25%) en el consorcio, unión temporal o promesa de sociedad futura y aportar mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta.
 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.
 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.
 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.
 7. Preferir la oferta presentada por un proponente plural siempre que:
 - a) esté conformado por al menos una madre cabeza de familia y/o una persona en proceso de reincorporación o reintegración, o una persona jurídica en la cual participe o participen mayoritariamente, y, que tenga una participación de por lo menos el veinticinco por ciento (25%) en el proponente plural; la madre cabeza de familia, la persona en proceso de reincorporación o reintegración, o la persona jurídica aporte mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta; y
 - b) ni la madre cabeza de familia o persona en proceso de reincorporación o reintegración, ni la persona jurídica, ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural.
 8. Preferir la oferta presentada por una MiPymes o cooperativas o asociaciones mutuales; o un proponente plural constituido por Mipymes, cooperativas o asociaciones mutuales.
 9. Preferir la oferta presentada por el proponente plural constituido por micro y/o pequeñas empresas, cooperativas o asociaciones mutuales.
 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; o, la oferta presentada por un proponente plural siempre que:
 - a) esté conformado por al menos una MIPYME, cooperativa o asociación mutual que tenga una participación de por lo menos el veinticinco por ciento (25%);
 - b) la MIPYME, cooperativa o asociación mutual aporte mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta; y
 - c) ni la MIPYME, cooperativa o asociación mutual ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural.
 11. Preferir las empresas reconocidas y establecidas como Sociedad de Beneficio e Interés Colectivo o Sociedad BIC, del segmento MIPYMES.
 12. Utilizar un método aleatorio (sorteo) para seleccionar el oferente, método que deberá haber sido previsto previamente en los Documentos del Proceso.

PARÁGRAFO 1. Los factores de desempate serán aplicables en el caso de las cooperativas y asociaciones mutuales que cumplan con los criterios de clasificación empresarial, definidos por el Decreto 957 de 2019, priorizando aquellas que sean micro, pequeñas o medianas.

PARÁGRAFO 2. Para los criterios enunciados que involucren la vinculación de capital humano, el oferente deberá acreditar una antigüedad igual o mayor a un año. Para los casos de constitución inferior a un año se tendrá en cuenta a aquellos trabajadores que hayan estado vinculados desde el momento de constitución de la misma.

PARÁGRAFO 3. El Gobierno Nacional podrá reglamentar la aplicación de factores de desempate en casos en que concurran dos o más de los factores aquí previstos.

3.3 Procedimiento del sorteo (método aleatorio)

Se realizarán dos sorteos, así:

El primero, para definir el orden mediante el cual los proponentes seleccionarán las balotas que dirimirán el empate.

- a) Revisión estado balotas. Se pondrá en evidencia, a viva voz, la numeración de las balotas la cual debe guardar relación directa con la cantidad de proponentes habilitados para el desempate.
- b) Se depositan las balotas previamente revisadas, una a una, en sobre no traslucido.
- c) Indicación a los proponentes del número de oportunidades que tendrán para escoger balotas. Para todos los efectos esta será una única vez.
- d) Cada proponente selecciona en su oportunidad una balota, el número que esta refleje, le dará el orden en que podrá seleccionar la balota que dirima el empate.

Realizado el primer sorteo, y definido el orden de selección; los proponentes procederán a escoger la balota que dirima el empate, en el orden que se haya determinado.

1. Se aceptará la oferta al proponente que saque la balota con el mayor número, o bien la balota de diferente color a las demás.
2. El resultado será aceptado de antemano por los proponentes involucrados en el empate sin lugar a reclamación alguna.

3.4 Causales de Rechazo

Definición de eliminación: se entiende por "eliminación" la decisión de excluir del proceso de convocatoria, una oferta cuando dentro de su análisis se detectan errores, faltas, incoherencias, o en general información no admisible, o cuando se presente alguna(s) de las causales descritas a continuación:

Serán causales para rechazar la oferta el incumplimiento de cualquiera de los requisitos mínimos de participación solicitados en este documento o por incumplimiento de requisitos legales.

- a) Cuando la oferta o sus aclaraciones contengan información inexacta o contradictoria.
- b) Cuando la oferta se modifique por el oferente de manera unilateral o ante una solicitud de aclaración.



Versionamiento Formato

Código: FO33-DE-GDCO
 Versión: 1.0
 Fecha actualización: 20/10/2023

- c) Cuando el oferente no haya respondido requerimientos de información- subsanación de Valor+ S.A.S., en el plazo otorgado para ello, o los responda de manera insatisfactoria o inconsistente, o lo haga modificando la oferta.
- d) Cuando la información requerida en los formularios para la evaluación de la oferta, de acuerdo con lo previsto en las condiciones particulares sea consignada en forma indebida, incorrecta o parcial.
- e) Cuando su presentación sea extemporánea; es decir, se presente luego de la fecha y hora fijadas para el cierre de la convocatoria.
- f) Cuando el objeto social o actividad mercantil del proponente no corresponda a lo requerido por Valor+ S.A.S.
- g) Cuando no se diligencie la totalidad de los ítems requeridos en el formato de oferta económica, o cuando éste sea modificado u alterado por el proveedor.
- h) Cuando el proponente no aporte o reúna los requisitos habilitantes o condiciones de participación indicados en el presente documento condiciones de la contratación y las demás previstas en la ley.
- i) Cuando la oferta económica presentada, supere el valor del presupuesto oficial establecido por la Empresa.
- j) Cuando con la oferta económica no se presente la póliza de seriedad de la oferta y el comprobante de pago de esta.

4. EVALUACIÓN DE PROPUESTAS

La o las ofertas que se reciban en virtud del procedimiento de contratación que se adelante por parte de Valor+ serán, en todo caso, objeto de verificación jurídica y de las condiciones de mercado para su adquisición. Adicionalmente, en los procedimientos de convocatoria pública y abreviada, se verificarán además las condiciones habilitantes financieras y técnicas aplicables, que podrán ser objeto de subsanación en las condiciones que el documento de condiciones de la contratación determine.

Los responsables de la recepción de las ofertas deberán detallar por escrito el número de propuestas recibidas, indicando el nombre, identificación del oferente, valor de la propuesta (cuando aplique), hora y fecha de recepción de esta y el número de folios de esta.

Todas las propuestas deberán evaluarse teniendo en cuenta los criterios y factores de selección. No podrán introducirse o utilizarse criterios para evaluar las ofertas, diferentes a los establecidos en los documentos de la contratación.

En el documento de condiciones de la contratación, Valor+ podrá abrogarse la facultad de hacer adjudicaciones parciales del objeto contractual, siempre que se considere técnicamente viable y sea conveniente para la Empresa, lo cual deberá ser materia de autorización por parte del Comité de Contratación.

No se tendrán en cuenta en ninguno de los criterios establecidos para el procedimiento y asignación de puntaje, las propuestas que no estén habilitadas y las que se encuentren incursas en las causales de "Rechazo de Propuestas", las demás serán consideradas ofertas válidas para el procedimiento de asignación de puntaje.

Las ofertas que se reciban en virtud del presente proceso serán, en todo caso, objeto de verificación de las condiciones establecidas para las escogencias del Proveedor.

El criterio de selección que permita identificar la oferta más favorable para Valor+ S.A.S., será la

ponderación de los siguientes criterios, siempre que haya cumplido con las especificaciones técnicas y requisitos habilitantes del proceso.

Lo anterior, de acuerdo con lo siguiente:

ÍTEM DE EVALUACIÓN	PUNTOS
PRECIO: Oferta de menor valor	85
APOYO A LA INDUSTRIA NACIONAL	10
EMPRENDIMIENTO Y EMPRESAS DE MUJERES	5
TOTAL	100

4.1. Fórmula Evaluación Propuesta

PRECIO: 85 puntos

PP=65*Pm/Pi	PP:	Puntaje factor Precio
	Pm:	Valor propuesta menor precio
	Pi:	Valor propuesta a comparar
	65	Puntaje máximo asignado al factor

Se otorgará **85 puntos** a la propuesta que oferte el menor valor. En todo caso, ninguna propuesta podrá superar el valor del presupuesto oficial establecido para esta contratación, siendo causal de rechazo la propuesta que supere dicho valor.

Se asignará el máximo puntaje del ítem respectivo (precio ítems) al proponente cuya oferta sea la más económica, el porcentaje de los demás oferentes se asignarán en proporción, por regla de tres simple, de conformidad con los precios ofertados.

APOYO A LA INDUSTRIA NACIONAL: 10 puntos

Este puntaje lo obtendrá el proponente que oferte bienes y servicios nacionales, entendiéndose como tales, aquellos prestados por empresas constituidas de acuerdo con la legislación nacional, por personas naturales colombianas o por residentes en Colombia

El artículo 1 en su parágrafo, de la Ley 816 de 2003, modificado por el artículo 51 del Decreto Nacional 019 de 2012 establece: *“Se otorgará tratamiento de bienes y servicios nacionales a aquellos bienes y servicios originarios de los países con los que Colombia ha negociado trato nacional en materia de compras estatales y de aquellos países en los cuales a las ofertas de bienes y servicios colombianos se les conceda el mismo tratamiento otorgado a sus bienes y servicios nacionales.”*

EMPRENDIMIENTO Y EMPRESAS DE MUJERES: 5 puntos

Se entenderán como emprendimientos y empresas de mujeres aquellas que cumplan con alguna de las siguientes condiciones:

- a. Cuando más del cincuenta por ciento (50%) de las acciones, partes de interés o cuotas de



Versionamiento Formato

Código: FO33-DE-GDCO
 Versión: 1.0
 Fecha actualización: 20/10/2023

participación de la persona jurídica pertenezcan a mujeres 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. 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 conste la distribución de los derechos en la sociedad y el tiempo en el que las mujeres han mantenido su participación.

- b. Cuando por lo menos el cincuenta por ciento (50%) de los empleos del nivel directivo de la persona jurídica sean ejercidos por mujeres y éstas hayan estado vinculadas laboralmente a 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.

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 todas las personas que conforman los cargos de nivel directivo del proponente, el número de mujeres y el tiempo de vinculación.

La certificación deberá relacionar el nombre completo y el número de documento de identidad de cada una de las personas que conforman el 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.

4.2 Informe de evaluación

El informe de evaluación será enviado a él o los oferentes, teniendo en cuenta el cronograma establecido en el presente documento.

4.3 Reglas de Subsanabilidad

En el proceso de selección y en general en la actividad contractual que adelante Valor+ S.A.S., prevalecerá lo sustancial sobre lo formal. Lo anterior implica que la ausencia de requisitos o la falta de documentos habilitantes o de admisibilidad, y que no constituyan factores de evaluación o de asignación de puntaje, no servirán de título suficiente para el rechazo de las ofertas y podrán ser subsanados dentro del término que se establezca.

En ejercicio de la facultad de subsanación de la oferta, los oferentes no podrán modificar o mejorar la oferta.

4.4 Suspensión o Cancelación del Proceso de Contratación

Valor+ S.A.S., podrá suspender o terminar, previa decisión debidamente justificada, el proceso de selección en cualquiera de sus etapas, cuando aparezcan circunstancias técnicas, operativas, económicas, de mercado, de fuerza mayor, orden de autoridad competente, acto irresistible de terceros o razones de utilidad o conveniencia corporativa, o cualquier otra que haga inconveniente la contratación.

3. REGLAS PARA LA PRESENTACIÓN DE PROPUESTAS

5.1 Propuesta Económica

Para elaborar la propuesta económica, esta debe realizarse en el formato adjunto (Formato Propuesta Económica), este es un requisito habilitante, deben ser firmado por la persona que acredita capacidad para presentar la oferta; estar diligenciado por completo, sin alterar, modificar o adicionar los ítems solicitados.

Para efectos de facilitar la verificación y evaluación de la propuesta que realizará, Valor+ S.A.S, lo invitamos a presentar los demás archivos en PDF y el (Formato Propuesta Económica) diligenciado en formato Excel.

5.2 Estampillas

Por la naturaleza jurídica de Valor+ S.A.S. se aplican las siguientes retenciones por concepto de estampillas, las cuales deben estar contempladas dentro de la propuesta económica:

ESTAMPILLAS	
Universidad de Envigado	0.4%
Politécnico	0.4%
Pro-Desarrollo	0.6%
Pro-Hospital	1 %
Pro-Deporte y Recreación	2.5%
Adulto Mayor	2 %
Universidad Digital	0.4%
Total	7.3%

5.3 Validez de la Oferta

La oferta tendrá una validez de Treinta (30) días calendario, contados a partir de la fecha límite para su presentación.

5.4 Rondas de Negociación

En las modalidades de selección mediante convocatoria que adelante Valor+ S.A.S., y previo a la formalización de la contratación, con la finalidad de mejorar las condiciones comerciales o técnicas, Valor+ S.A.S., podrá realizar rondas de negociación con los oferentes habilitados.

**Versionamiento Formato**

Código: FO33-DE-GDCO
Versión: 1.0
Fecha actualización: 20/10/2023

5.5 Única Oferta

En el evento de recibirse una sola oferta en el desarrollo de la convocatoria abreviada, podrá aceptarse siempre y cuando se ajuste a las condiciones de la contratación y sea conveniente para la Empresa.

En caso de que no se presente ninguna oferta o que las recibidas no cumplan con lo exigido en los términos de la convocatoria, se declarará terminado el proceso.

5.6 Idioma

La oferta y sus anexos, así como toda comunicación que se origine dentro de este proceso de contratación, deberán presentarse en idioma castellano. Los documentos que no estén en idioma Castellano deberán presentarse acompañados de una traducción oficial a dicho idioma.

Se deberá tener en cuenta que la capacidad máxima de cada correo a enviar no deberá superar la capacidad de 15 MB, si los documentos adjuntos la superan, deben separarse en varios mensajes, los archivos deben nombrarse con máximo 10 caracteres.

5.7 Anexos de los proponentes

- Propuesta Económica
- Documentos (Capacidad jurídica y experiencia)
- Formatos diligenciados y firmados:
 - Inhabilidades e Incompatibilidades.
 - Autorización tratamiento de datos personales.
 - Certificación lavado de activos y financiación del terrorismo.
- Los demás anexos que hagan parte de la convocatoria y que los proponentes deban diligenciar y firmar.



RE: Convocatoria Abreviada N°012-2026

Desde Victor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

Fecha Mar 28/04/2026 11:31

Para Compras Valor + 2 <compras2@valormas.gov.co>

CC Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

Buenos días.

Dando respuesta a lo solicitado se carga documentos al sitio web de la entidad referente a la Convocatoria Abreviada N°012-2026.

Convocatoria Abreviada N°012-2026

Convocatoria Abreviada N°012-2026.

1. Condicionales de la contratación
2. Cronograma Convocatoria Abreviada
3. CDP
4. Relación Experiencia Técnica
5. Formato Autorización de tratamiento de datos personales
6. Anexo Resolución de Incapacidades
7. Formato Inhabilidades e Incompatibilidades
8. Formato Certificación de lavado de activos y financiación del Terrorismo - SARLAFI
9. Formato Propuesta Económica

Gracias por la atención prestada
Saludos,



Victor Rodrigo Galvis Zuleta

Contratista

victor.galvis@valormas.gov.co

Carrera 53A #42 161, Torre B, Piso 6

Ed. Plaza de la Libertad

Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le avisará que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos avisar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

De: Compras Valor + 2 <compras2@valormas.gov.co>

Enviado el: martes, 28 de abril de 2026 11:15 a. m.

Para: Victor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

CC: Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres

<gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

Asunto: Convocatoria Abreviada N°012-2026

Cordial saludo,

Amablemente solicito tu ayuda por favor, para publicar la siguiente convocatoria en la página web de la entidad.

Convocatoria Abreviada N°012-2026.

Objeto: "Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."

1. Condiciones de la contratación
2. Cronograma Convocatoria Abreviada
3. CDP
4. Relación Experiencia Técnica.
5. Formato Autorización de tratamiento de datos personales
6. Anexo Resolución de Inquietudes
7. Formato Inhabilidades e Incompatibilidades
8. Formato Certificación de lavado de activos y financiación del Terrorismo - SARLAFT.
9. Formato Propuesta Económica

Quedo atenta.

Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edetel, Piso 3 Sector Alpujarra,

Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.



Convocatoria Abreviada N°012-2026- Intrust Security

Desde Compras Valor + 2 <compras2@valormas.gov.co>

Fecha Mar 28/04/2026 11:38

Para sbaron@intrustsecurity.co <sbaron@intrustsecurity.co>

CC Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

9 archivos adjuntos (756 KB)

1.Condiciones Contratación Convocatoria Abreviada N° 012-2026.docx; 2.Cronograma Convocatoria 012-2026.docx; 3.CDP 738.pdf; 4. Relación Experiencia Técnica_v1.0.docx; 5.Autorización tratamiento de datos personales_v2.0.docx; 6. Resolución Inquietudes_v1.0.xlsx; 7. Inhabilidades e incompatibilidades_v1.0.docx; 8.Certificación lavado de activos y financiación del terrorismo_v2.0.docx; 9. Oferta Económica.xlsx;

Cordial saludo,

Actualmente la empresa Valor+ S.A.S., está adelantando la Convocatoria Abreviada N°012-2026, cuyo objeto es **“Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet.”**

Lo invitamos a presentar su propuesta para la prestación de dichos servicios, adjunto encontrara las Condiciones de Contratación del proceso y sus anexos se encuentran adjuntos en el presente correo, cualquier inquietud y comunicación oficial el correo electrónico: compras2@valormas.gov.co.

1. Condiciones de la contratación
2. Cronograma Convocatoria Abreviada
3. CDP
4. Relación Experiencia Técnica.
5. Formato Autorización de tratamiento de datos personales
6. Anexo Resolución de Inquietudes
7. Formato Inhabilidades e Incompatibilidades
8. Formato Certificación de lavado de activos y financiación del Terrorismo - SARLAFT.
9. Formato Propuesta Económica

Quedamos atentos y esperamos pronta respuesta,

Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatei, Piso 3 Sector Aloujarra,

Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.



Observaciones - Convocatoria Abreviada N°012-2026

Desde Compras Valor + 2 <compras2@valormas.gov.co>

Fecha Jue 30/04/2026 9:55

Para Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

CC Compras Valor + <compras@valormas.gov.co>

📎 1 archivo adjunto (35 KB)

6. Resolución Inquietudes_v1.0 HDC.xlsx;

Cordial saludo,

Relaciono el consolidado de observaciones recibidas para la Convocatoria N° 012, cuyo objeto es **"Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."**, Lo anterior, con el fin de que se brinde una respuesta oportuna, de acuerdo con el cronograma establecido.

N°	ETAPA	FECHA Y HORA
1	Envío condiciones de la contratación, vía correo electrónico (Mínimo 3 invitados) y publicación de la convocatoria en plataforma Web (Página Web de la Empresa)	28/04/2026 Hasta las 12:00 horas
2	Presentación de observaciones y/o solicitud de aclaraciones a las condiciones de la contratación.	29/04/2026 Hasta las 18:00 horas
3	Respuesta a las observaciones y/o aclaraciones y/o adendas, según corresponda y publicación en plataforma Web (Página Web de la Empresa).	04/05/2026 Hasta las 17:00 horas.
4	Presentación de propuestas.	06/05/2026 Hasta las 17:00 horas
5	Acta en la que consten los nombres de los oferentes, fecha y hora de presentación de las propuestas y publicación en plataforma Web (Página Web de la Empresa).	07/05/2026 Hasta las 12:00 horas.
6	Evaluación de propuestas y/o solicitudes de subsanación y/o envío de informe preliminar y publicación en plataforma Web (Página Web de la Empresa).	08/05/2026 Hasta las 16:00 horas.
7	Presentación de observaciones al informe de evaluación preliminar y/o aclaraciones y/o subsanaciones de las ofertas.	11/05/2026 Hasta las 18:00 horas
8	Respuesta a las observaciones y publicación del informe de evaluación definitivo en plataforma Web (Página Web de la Empresa).	13/05/2026 Hasta las 16:00 horas.
9	Comunicación de aceptación de la propuesta.	14/05/2026 Hasta las 15:00 horas.

Quedo atenta,
Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige.
Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución
o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos
notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

Resolución de inquietudes



Versionamiento Formato
Código: E013-DE-GCYN
Versión: 1.0
Fecha actualización: 28/09/2023

Medellín, 04 de mayo de 2026

Objeto: "Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet"

Agradecemos a los futuros oferentes su participación activa en el presente proceso y la presentación de sus observaciones. Damos respuesta en los siguientes términos:

	Fecha (DD/MM/AA)	Pregunta o inquietud formulada	Respuesta por parte de Valor+ S.A.S.								
1	29/04/2026	En el punto (Se requiere que el proponente desarrolle y cumpla con lo siguiente:) se encuentra una tabla donde dice unidad de medida 8 meses. Se solicita amablemente a la entidad confirmar si lo esperado en este contrato es por los 8 meses en cada característica según la tabla.	De acuerdo con lo establecido en el documento "Condiciones de la Contratación Convocatoria Abreviada N° 012-2026", en el numeral "1.5. Alcance y/o Condiciones y/o Especificaciones Técnicas del Bien o Servicio a Contratar", se estipuló que el proponente debe desarrollar lo siguiente: 1.5 Alcance y/o Condiciones y/o Especificaciones Técnicas del Bien o Servicio a Contratar El objeto del presente contrato comprende la prestación de servicios de vigilancia tecnológica en ciberseguridad, orientados a la identificación, evaluación, monitoreo y mitigación de riesgos asociados a amenazas cibernéticas que pueden comprometer la infraestructura tecnológica y la información de la Gobernación de Antioquia. Se requiere que el proponente identifique y cumpla con lo siguiente: <table><tr><th>Desarrollos / Componentes</th><th>Unidad de medida / Meses</th></tr><tr><td>Vigilancia Tecnológica</td><td>A</td></tr><tr><td>Gestión de Vulnerabilidades</td><td>B</td></tr><tr><td>Gestión de Seguridad de la Información</td><td>C</td></tr></table> Adicional y según lo indicado en el numeral "1.6 Plazo de ejecución", se señaló que el plazo es: 1.6 Plazo de Ejecución Será desde la suscripción del acta de inicio hasta el 31 de diciembre del 2026.	Desarrollos / Componentes	Unidad de medida / Meses	Vigilancia Tecnológica	A	Gestión de Vulnerabilidades	B	Gestión de Seguridad de la Información	C
Desarrollos / Componentes	Unidad de medida / Meses										
Vigilancia Tecnológica	A										
Gestión de Vulnerabilidades	B										
Gestión de Seguridad de la Información	C										
2	29/04/2026	para el punto 1 VIGILANCIA TECNOLÓGICA, se solicita amablemente a la entidad compartir los dominios a monitorear y las marcas.	El alcance del servicio comprende los dominios, plataformas y ambientes tecnológicos asociados a Antioquia, Salud, Vehículos, Tasa de Seguridad, Educación, Hacienda, Seguridad Ciudadana, Catastro, Sede Electrónica, así como cualquier otro dominio, sistema o activo digital perteneciente o administrado por la Gobernación de Antioquia, de acuerdo con las necesidades y prioridades definidas por la entidad. En cumplimiento de los lineamientos de seguridad de la información, la Entidad se abstiene de divulgar marcas, fabricantes o versiones específicas de las tecnologías que conforman su infraestructura, dado que esta información es clasificada como sensible y su exposición podría incrementar la superficie de riesgo frente a amenazas cibernéticas externas. En consecuencia, el alcance del servicio de Vigilancia Tecnológica requerido por la Entidad comprende, de manera general, los siguientes componentes: -Infraestructura de red y mecanismos de seguridad perimetral (incluyendo firewalls de nueva generación). -Aplicaciones web y APIs. -Servicios en la nube y plataformas colaborativas -Sistemas de información misionales y administrativos. -Gestión de identidades y accesos. -Estaciones de trabajo y servidores. -Activos expuestos en internet, incluyendo aquellos presentes en espacios no indexados o de acceso restringido (Deep Web y Dark Web). El servicio de vigilancia tecnológica deberá cubrir tanto las tecnologías actualmente implementadas como aquellas que se incorporen durante la vigencia del contrato, garantizando un monitoreo continuo y actualizado frente a la evolución del entorno tecnológico y las amenazas emergentes. En caso de requerirse un mayor nivel de detalle técnico para asegurar la correcta prestación del servicio, la Entidad suministrará dicha información únicamente al proveedor adjudicatario, bajo la firma de acuerdos de confidencialidad y no divulgación de información y conforme a los procedimientos establecidos en su política de seguridad de la información.								
3	29/04/2026	Punto 2 GESTION DE VULNERABILIDADES: se aclara a la entidad que es necesario saber las cantidades y tipo de activos, por ejemplo cuantos activos de infraestructura son y cuantas paginas o sitios web, como tambien cuales son los servicios en nube, si es IaaS o se refiere a plataformas de proveedores publicos y si es Infraestructura en nube cuantos activos son.	La Entidad cuenta con un entorno tecnológico híbrido que integra componentes on-premise y servicios en la nube. Se disponen ambientes web y sistemas de información desplegados tanto en infraestructura local (on-premise) como en múltiples proveedores de servicios en la nube, incluyendo Microsoft Azure, Google Cloud Platform y Oracle Cloud, entre otros. Se tiene una infraestructura tecnológica aproximada de 300 servidores, alrededor de 50 ambientes web y múltiples dispositivos de red, operando bajo un entorno híbrido que integra componentes locales y servicios en la nube, lo cual demanda una gestión integral, continua y especializada en materia de seguridad de la información y ciberseguridad.								
4	29/04/2026	Punto 2 GESTION DE VULNERABILIDADES: se solicita amablemente aclarar el alcance, debido a que en el 3er parrafo de este punto, se habla de Adversary Emulation, red teaming y threat Hunting, estos puntos son ejercicios totalmente diferentes a la gestión de vulnerabilidades, igualmente se requiere incluirlo?.	En relación con el Punto 2 – Gestión de Vulnerabilidades, se aclara que el alcance del servicio sí incluye Adversary Emulation, Red Teaming y Threat Hunting, integrados de manera transversal al proceso de gestión de vulnerabilidades y no como ejercicios independientes. Estas capacidades se incorporan para contextualizar los hallazgos técnicos frente a escenarios reales de amenaza, correlando las vulnerabilidades identificadas con tácticas, técnicas y procedimientos utilizados por actores de amenaza, bajo la alineación conceptual del marco MITRE ATT&CK y la referencia metodológica del NIST SP 800-115, fortaleciendo la priorización del riesgo, la validación de la explotabilidad y la toma de decisiones de remediación, en complemento a los estándares CVSS y OWASP.								
5	29/04/2026	Punto 2 componente especializado, Se aclara a la entidad que podemos brindar acompañamiento en el ciclo de vida de las vulnerabilidades, sin embargo, la ejecución de la remediación es responsabilidad de Valor +.	La ejecución de las acciones de mitigación y remediación corresponde directamente a la entidad. Sin embargo, en múltiples ocasiones se requiere el acompañamiento de la empresa del Servicio de Vigilancia Tecnológica para brindar apoyo técnico especializado y estratégico a los responsables de la plataforma tecnológica, facilitando el proceso de mitigación de las brechas de seguridad informática derivadas de las vulnerabilidades identificadas. Este acompañamiento deberá incluir la realización de sesiones técnicas, orientados a explicar los vectores de explotación, recomendaciones para su adecuada mitigación y remediación. Contribuyendo de manera efectiva al proceso de gestión y cierre de vulnerabilidades.								

Fecha (DD/MM/AA)	Pregunta o inquietud formulada	Respuesta por parte de Valor+ S.A.S.																											
6 29/04/2026	se solicita a la entidad aclarar el alcance en la gestión de vulnerabilidades debido a que en el documento Pag 10, solicitan servicios de ethical haking caja negra y/o gris, esto significa que tambien se debe aplicar ethical haking a todos los activos de la entidad y de manera mensual ? si es así, por favor indicar la catidad y tipo de activos.	En el alcance del servicio se expresa lo siguiente: "Realización de pruebas de penetración mensuales (caja negra y/o caja gris) sobre la plataforma tecnológica de la entidad, priorizando los activos críticos y aquellos que la organización considere estratégicos, con el fin de identificar y mitigar oportunamente vulnerabilidades de seguridad informática". La entidad cuenta con una infraestructura tecnológica aproximada de 300 servidores, alrededor de 50 ambientes web y múltiples dispositivos de red, operando bajo un entorno híbrido que integra componentes locales y servicios en la nube. Lo anterior incluye tecnologías actuales y futuras que sean incorporadas durante la ejecución del contrato. El servicio se presta de manera continua bajo un enfoque de ciberseguridad preventiva y proactiva, orientado a la identificación temprana, gestión oportuna y mitigación efectiva de riesgos y vulnerabilidades, fortaleciendo de forma permanente la postura de seguridad de la entidad.																											
7 29/04/2026	Punto 3 La gestión de superficie de ataque, para este punto se solicita aclarar si lo requerido es una consultoría basada en la ISO/IEC 27001.	Se aclara que el servicio no corresponde a una consultoría específica para la implementación o certificación de la Norma ISO/IEC 27001, sino que está orientado a la prestación de servicios especializados en seguridad de la información y ciberseguridad, los cuales serán ejecutados conforme a las necesidades, requerimientos y prioridades definidas por la entidad durante la vigencia contractual. Es un servicio de Vigilancia Tecnológica (Deep Web y Dark Web). El servicio contempla la operación continua de un esquema de ciberseguridad preventiva y proactiva, estructurado en tres (3) ejes fundamentales: (1) Vigilancia Tecnológica, (2) Gestión de Vulnerabilidades y (3) Gestión de la Superficie de Ataque. Estos componentes permiten identificar, analizar y mitigar riesgos asociados a la exposición de activos digitales. Estos componentes permiten identificar, analizar y mitigar riesgos asociados a la exposición de activos digitales. Adicionalmente, incluye la realización de pruebas de penetración mensuales (caja negra y/o caja gris), así como la disponibilidad de una aplicación web para la visualización, seguimiento y control de las vulnerabilidades identificadas, tanto por el servicio de vigilancia como por otras herramientas de la entidad. Es de señalar, que en el documento "Condiciones de la contratación Convocatoria Abreviada N°012-2026", en el numeral "1.5. Alcance y/o Especificaciones Técnicas del Bien o Servicio a Contratar, en la Gestión tratamiento de vulnerabilidades" señala: <u>El proveedor deberá ejecutar las actividades descritas, garantizando el cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad (ISO 27001, NIST, MITRE ATTACK, OWASP, entre otros). Deberá presentar certificado manifestando que garantiza lo anterior.</u>																											
8 29/04/2026	se solicita amablemente a la entidad ampliar el plazo de entrega, esto con el fin de validar de acuerdo a las respuestas a las observaciones los diferentes escenarios del proyecto. Se sugiere el 12 de mayo del 2026	No se acepta la observación, considerando la alta criticidad, prioridad y urgencia que demanda la prestación del servicio, dado que su ejecución oportuna es fundamental para garantizar la continuidad, fortalecimiento y protección de la seguridad de la información y la infraestructura tecnológica de la entidad. En el documento "Condiciones de la Contratación Convocatoria Abreviada N° 012-2026", en el numeral "1.2. Cronograma del Proceso" se tienen establecido los plazos para cada etapa. <table border="1"> <caption>1.2 Cronograma del Proceso</caption> <thead> <tr> <th>N°</th> <th>ETAPA</th> <th>FECHA Y HORA</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Unión consorcios de la comunidad, vía correo electrónico (Máximo 3 invitadas) y publicación de la convocatoria en plataforma Web (Página Web de la Entidad).</td> <td>Hasta las 12:00 horas.</td> </tr> <tr> <td>2</td> <td>Presentación de observaciones y/o solicitudes de aclaración a las condiciones de la contratación.</td> <td>04/05/2026 Hasta las 16:00 horas.</td> </tr> <tr> <td>3</td> <td>Respuesta a las observaciones y/o solicitudes por correo electrónico y publicación en plataforma Web (Página Web de la Entidad).</td> <td>04/05/2026 Hasta las 17:00 horas.</td> </tr> <tr> <td>4</td> <td>Presentación de propuestas.</td> <td>04/05/2026 Hasta las 17:00 horas.</td> </tr> <tr> <td>5</td> <td>Acta en la que constan los nombres de los observadores, fecha y hora de presentación de las propuestas y publicación en plataforma Web (Página Web de la Entidad).</td> <td>07/05/2026 Hasta las 12:00 horas.</td> </tr> <tr> <td>6</td> <td>Evaluación de propuestas y/o solicitudes de subsanación y/o nota de informe preliminar y publicación en plataforma Web (Página Web de la Entidad).</td> <td>08/05/2026 Hasta las 16:00 horas.</td> </tr> <tr> <td>7</td> <td>Presentación de observaciones e informe de evaluación preliminar y/o subsanación de las observaciones.</td> <td>11/05/2026 Hasta las 16:00 horas.</td> </tr> <tr> <td>8</td> <td>Respuesta a las observaciones y publicación del informe de evaluación definitivo en plataforma Web.</td> <td>13/05/2026 Hasta las 16:00 horas.</td> </tr> </tbody> </table>	N°	ETAPA	FECHA Y HORA	1	Unión consorcios de la comunidad, vía correo electrónico (Máximo 3 invitadas) y publicación de la convocatoria en plataforma Web (Página Web de la Entidad).	Hasta las 12:00 horas.	2	Presentación de observaciones y/o solicitudes de aclaración a las condiciones de la contratación.	04/05/2026 Hasta las 16:00 horas.	3	Respuesta a las observaciones y/o solicitudes por correo electrónico y publicación en plataforma Web (Página Web de la Entidad).	04/05/2026 Hasta las 17:00 horas.	4	Presentación de propuestas.	04/05/2026 Hasta las 17:00 horas.	5	Acta en la que constan los nombres de los observadores, fecha y hora de presentación de las propuestas y publicación en plataforma Web (Página Web de la Entidad).	07/05/2026 Hasta las 12:00 horas.	6	Evaluación de propuestas y/o solicitudes de subsanación y/o nota de informe preliminar y publicación en plataforma Web (Página Web de la Entidad).	08/05/2026 Hasta las 16:00 horas.	7	Presentación de observaciones e informe de evaluación preliminar y/o subsanación de las observaciones.	11/05/2026 Hasta las 16:00 horas.	8	Respuesta a las observaciones y publicación del informe de evaluación definitivo en plataforma Web.	13/05/2026 Hasta las 16:00 horas.
N°	ETAPA	FECHA Y HORA																											
1	Unión consorcios de la comunidad, vía correo electrónico (Máximo 3 invitadas) y publicación de la convocatoria en plataforma Web (Página Web de la Entidad).	Hasta las 12:00 horas.																											
2	Presentación de observaciones y/o solicitudes de aclaración a las condiciones de la contratación.	04/05/2026 Hasta las 16:00 horas.																											
3	Respuesta a las observaciones y/o solicitudes por correo electrónico y publicación en plataforma Web (Página Web de la Entidad).	04/05/2026 Hasta las 17:00 horas.																											
4	Presentación de propuestas.	04/05/2026 Hasta las 17:00 horas.																											
5	Acta en la que constan los nombres de los observadores, fecha y hora de presentación de las propuestas y publicación en plataforma Web (Página Web de la Entidad).	07/05/2026 Hasta las 12:00 horas.																											
6	Evaluación de propuestas y/o solicitudes de subsanación y/o nota de informe preliminar y publicación en plataforma Web (Página Web de la Entidad).	08/05/2026 Hasta las 16:00 horas.																											
7	Presentación de observaciones e informe de evaluación preliminar y/o subsanación de las observaciones.	11/05/2026 Hasta las 16:00 horas.																											
8	Respuesta a las observaciones y publicación del informe de evaluación definitivo en plataforma Web.	13/05/2026 Hasta las 16:00 horas.																											
9 29/04/2026	Con relación a la convocatoria en asunto solicitamos aclaración sobre los activos que requieren gestionar ya que en el punto N°2 hacen referencia a los activos internos. Vigilancia tecnológica ¿Cuántos dominios, marcas o activos digitales se deben monitorear? ¿El alcance incluye únicamente la entidad principal o también filiales? ¿Se requiere monitoreo en Deep y Dark Web con alertas en tiempo real? ¿Frecuencia esperada de reportes (semanal, mensual, ambos)? Se quiere cotizar takedowns, cuantos?	El alcance del servicio comprende los dominios, plataformas, sistemas y ambientes tecnológicos asociados a Antioquia, Salud, Vehículos, Tasa de Seguridad, Educación, Hacienda, Seguridad Ciudadana, Catastro, Sede Electrónica, así como cualquier otro dominio, activo digital o componente tecnológico perteneciente o administrado por la Gobernación de Antioquia, conforme a las necesidades, prioridades y criticidad definidas por la entidad. Adicionalmente, todo nuevo desarrollo, implementación tecnológica, aplicación, sistema o servicio digital que sea incorporado a la infraestructura institucional deberá ser objeto de un análisis de seguridad detallado, incluyendo evaluaciones técnicas especializadas, identificación de vulnerabilidades, validación de controles de seguridad y pruebas que permitan detectar riesgos potenciales antes de su salida a producción, garantizando así la protección integral de la plataforma tecnológica y el fortalecimiento continuo de la postura de ciberseguridad institucional. La Entidad cuenta con activos digitales expuestos a internet como portales web, aplicaciones, APIs y servicios en la nube. Se requiere que el servicio contemple capacidades de monitoreo en Deep Web y Dark Web, orientadas a la identificación de posibles filtraciones de información, credenciales comprometidas, suplantaciones de marca, dominios fraudulentos u otras amenazas asociadas a la Entidad. Se espera un esquema combinado de reportes que incluya: Reportes semanales y Mensuales con el consolidado de lo identificado. Adicionalmente, se deberán generar reportes extraordinarios en caso de hallazgos críticos o incidentes relevantes. El servicio de takedowns no se tiene incluido en el alcance del proyecto																											
10 29/04/2026	Gestión de vulnerabilidades ¿Cuántos activos se van a evaluar? () ¿Que tipo de activos son y cuantos por cada uno? (IPs, servidores, endpoints, aplicaciones web, servicios en la nube, etc) ¿Se requiere escaneo continuo o únicamente mensual? ¿Se espera incluir validación de remediación (retest)?	La entidad cuenta con una infraestructura tecnológica aproximada de 300 servidores, alrededor de 50 ambientes web y múltiples dispositivos de red, operando bajo un entorno híbrido que integra componentes locales y servicios en la nube, lo cual demanda una gestión integral, continua y especializada en materia de seguridad de la información y ciberseguridad. Se requiere escaneo continuo y un informe mensual En caso de requerirse la validación de remediación (retest), el proveedor deberá realizarlo.																											

Fecha (DD/MM/AA)	Pregunta o inquietud formulada	Respuesta por parte de Valor+ S.A.S.
11 29/04/2026	Pruebas de seguridad (Pentesting / Red Team) ¿Cuántos activos críticos desean evaluar? ¿Qué tipo de pruebas requieren (caja negra, gris, Red Team completo)? ¿Desean incluir ejercicios de ingeniería social? ¿Tienen definida una duración estimada para estos ejercicios?	La entidad cuenta con una infraestructura tecnológica aproximada de 300 servidores, cerca de 50 ambientes web y múltiples dispositivos de red en un entorno híbrido. En este contexto, se prioriza la evaluación continua de los activos críticos y de aquellos componentes estratégicos que la entidad determine según su nivel de riesgo e impacto operativo. Respecto a los activos críticos: Dentro de la cantidad de ambientes se podría decir que la cantidad no es exacta ya que al tener alrededor de 50 y múltiples dispositivos estos serían los activos a tener en cuenta para ser evaluados en los momentos que se requieran. Se requiere la realización de pruebas de penetración mensuales bajo metodologías de caja negra y/o caja gris sobre la plataforma tecnológica institucional, enfocadas en identificar, evaluar y contribuir a la mitigación oportuna de vulnerabilidades de seguridad informática. No se contempla dentro del alcance la ejecución de ejercicios de ingeniería social. La prestación del servicio se establece bajo un esquema continuo, con un enfoque preventivo, proactivo y de mejora permanente, orientado al fortalecimiento constante de la postura de ciberseguridad de la entidad. Es importante aclarar que el servicio de Vigilancia Tecnológica no se limita exclusivamente a los activos clasificados como críticos, sino que está orientado a la plataforma tecnológica de la Entidad.
12 29/04/2026	Gestión de superficie de ataque ¿Cuentan actualmente con un inventario de activos o debe construirse desde cero? ¿Cuántos dominios, subdominios e IPs públicas manejan? ¿Qué tan dinámico es su entorno (on-premise, nube, híbrido)?	La entidad cuenta con una infraestructura tecnológica aproximada de 300 servidores, alrededor de 50 ambientes web y múltiples dispositivos de red, operando bajo un entorno híbrido que integra componentes locales y servicios en la nube, lo cual demanda una gestión integral, continua y especializada en materia de seguridad de la información y ciberseguridad. La Entidad dispone de un esquema de direccionamiento IP público con un bloque aproximado de 128 direcciones IP. No obstante, es importante precisar que la infraestructura tecnológica también incluye activos desplegados en servicios de hosting externo y entornos en la nube, particularmente en Microsoft Azure, así como otros proveedores, lo que puede incrementar la cantidad de direcciones IP públicas y recursos expuestos. El proveedor deberá contemplar mecanismos de descubrimiento y monitoreo continuo de la superficie de ataque externa, incluyendo dominios, subdominios e IPs públicas, tanto en infraestructura propia como en servicios de terceros, garantizando una cobertura integral y actualizada durante la ejecución del servicio. De acuerdo con lo señalado en el documento "Condiciones de la Contratación Convocatoria Abreviada N° 012-2026" en el numeral "1.5 Alcance y/o Condiciones y/o Especificaciones Técnicas del Bien o Servicio a Contratar", se establece que deberá entregar: Realizar el levantamiento, clasificación y documentación de los activos tecnológicos objeto del servicio.
13 29/04/2026	Evaluación de riesgo cibernético ¿Requieren una evaluación puntual o un seguimiento continuo? ¿Qué nivel de profundidad esperan (alto nivel o análisis cuantitativo detallado)?	La entidad requiere un servicio de evaluación y seguimiento continuo, ejecutado conforme a las necesidades institucionales, prioridades estratégicas y eventos de ciberseguridad que se presenten durante la vigencia contractual, garantizando una gestión permanente, preventiva y proactiva de la seguridad informática. Se espera un análisis cuantitativo detallado, orientado a identificar, validar y documentar técnicamente las vulnerabilidades detectadas, demostrando de manera clara su nivel de explotación, impacto potencial y criticidad sobre la infraestructura tecnológica. Cada hallazgo deberá estar debidamente soportado con evidencia técnica, análisis de riesgo y documentación precisa que facilite la toma de decisiones y la implementación efectiva de acciones de mitigación.
14 29/04/2026	Modelo de servicio y equipo ¿Se espera un servicio gestionado continuo o bajo demanda? ¿Horario requerido (8x5, 24x7)? ¿Nivel de especialización esperado del equipo?	La entidad requiere un servicio gestionado continuo, orientado a brindar apoyo permanente al área de ciberseguridad, bajo un enfoque preventivo, proactivo y estratégico que permita fortalecer de manera constante la postura de seguridad de la infraestructura tecnológica institucional. El servicio deberá prestarse bajo un esquema de disponibilidad 24/7, garantizando capacidad de atención, monitoreo, respuesta y acompañamiento oportuno ante vulnerabilidades, riesgos o eventos de ciberseguridad que puedan afectar la operación de la entidad. Se exige un alto nivel de especialización del equipo de trabajo, conformado por profesionales con perfil experto en ciberseguridad, experiencia comprobada y certificaciones especializadas en identificación, análisis, explotación ética y gestión de vulnerabilidades, asegurando así la calidad técnica, profundidad y efectividad de los servicios prestados. De acuerdo con lo señalado en el documento "Condiciones de la Contratación Convocatoria Abreviada N° 012-2026" en el numeral "1.5 Alcance y/o Condiciones y/o Especificaciones Técnicas del Bien o Servicio a Contratar", se establece: El proveedor deberá disponer de un componente de personal especializado para la gestión de vulnerabilidades, el cual será responsable de la operación continua del servicio. Este equipo deberá garantizar la gestión integral del ciclo de vida de las vulnerabilidades, desde su identificación hasta su cierre, incluyendo la validación de la remediación aplicada. De igual forma, deberá soportar con los flujos técnicos de la entidad la implementación de controles correctivos, realizar seguimiento a los planes de acción y asegurar la efectividad de los hallazgos. VALOR+ S.A.S. - NIT. 900007744 Dirección: Carrera 42 a 43 Sur 3 Avenida, Centro de la Alameda - Edificio Valero Teléfono: +57 (313) 454 7811 Email: info@valorplus.com.co El personal asignado deberá contar con formación profesional en áreas afines a tecnologías de la información y ciberseguridad, así como certificaciones vigentes de reconocimiento internacional, tales como CEH, OSCP, CISA, CISSP o equivalentes. Adicionalmente, deberán acreditar experiencia comprobada en la ejecución de pruebas de seguridad, análisis de vulnerabilidades y gestión de riesgos tecnológicos. Deberá presentar certificaciones reconocidas que acredite el dominio para sustentar la prestación del servicio y sus planes de acción, reportes de vulnerabilidades y vulnerabilidades remediadas. Valor+ S.A.S. - NIT. 900007744 Dirección: Carrera 42 a 43 Sur 3 Avenida, Centro de la Alameda - Edificio Valero Teléfono: +57 (313) 454 7811 Email: info@valorplus.com.co

Equipo estructurador:

ORIGINAL FIRMADO
 Carlos Arturo Correa Correa
 Rol Técnico

ORIGINAL FIRMADO
 Daniela María López Angulo
 Rol Logístico

ORIGINAL FIRMADO
 Verónica Restrepo Álvarez
 Rol Financiero

ORIGINAL FIRMADO
 Paula Andrea Toro Torres
 Rol Financiero

ORIGINAL FIRMADO
 Paula Cristina Parra Carmona
 Rol Jurídico

Resolución de inquietudes



Versionamiento Formato
Código: 0013-05-007N
Versión: 1.0
Fecha actualización: 28/08/2023

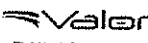
Medellín, 04 de mayo de 2026

Objeto: "Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de Internet y Darknet"

Agradecemos a los futuros oferentes su participación activa en el presente proceso y la presentación de sus observaciones. Damos respuesta en los siguientes términos:

	Fecha (DD/MM/AA)	Pregunta o inquietud formulada	Respuesta por parte de Valor+ S.A.S.								
1	29/04/2026	En el punto (Se requiere que el proponente desarrolle y cumpla con lo siguiente:) se encuentra una tabla donde dice unidad de medida 8 meses. Se solicita amablemente a la entidad confirmar si lo esperado en este contrato es por los 8 meses en cada característica según la tabla.	De acuerdo con lo establecido en el documento "Condiciones de la Contratación Convocatoria Abreviada N° 012-2026", en el numeral "1.5. Alcance y/o Condiciones y/o Especificaciones Técnicas del Bien o Servicio a Contratar", se estipuló que el proponente debe desarrollar lo siguiente: 1.5. Alcance y/o Condiciones y/o Especificaciones Técnicas del Bien o Servicio a Contratar O objeto del presente documento constituye el desarrollo del servicio de Vigilancia Tecnológica en ciberseguridad, entendiendo a la vigilancia tecnológica como el proceso de identificación, análisis y monitoreo de tecnologías emergentes y tendencias tecnológicas que puedan representar una amenaza o oportunidad para la entidad contratante. El presente servicio comprenderá el desarrollo y ejecución del siguiente: <table><tr><th>Componente / Característica</th><th>Unidad de medida / Tiempo</th></tr><tr><td>Vigilancia y monitoreo</td><td>8 meses</td></tr><tr><td>Análisis de inteligencia</td><td>8 meses</td></tr><tr><td>Reportes de inteligencia</td><td>8 meses</td></tr></table> Adicional y según lo indicado en el numeral "1.6 Plazo de ejecución", se señaló que el plazo es: 1.6 Plazo de Ejecución Será desde la suscripción del acta (a la vez) hasta el 31 de diciembre del 2026.	Componente / Característica	Unidad de medida / Tiempo	Vigilancia y monitoreo	8 meses	Análisis de inteligencia	8 meses	Reportes de inteligencia	8 meses
Componente / Característica	Unidad de medida / Tiempo										
Vigilancia y monitoreo	8 meses										
Análisis de inteligencia	8 meses										
Reportes de inteligencia	8 meses										
2	29/04/2026	para el punto 1 VIGILANCIA TECNOLÓGICA, se solicita amablemente a la entidad compartir los dominios a monitorear y las marcas.	El alcance del servicio comprende los dominios, plataformas y ambientes tecnológicos asociados a Antioquia, Salud, Vehículos, Tasa de Seguridad, Educación, Hacienda, Seguridad Ciudadana, Catastro, Sede Electrónica, así como cualquier otro dominio, sistema o activo digital perteneciente o administrado por la Gobernación de Antioquia, de acuerdo con las necesidades y prioridades definidas por la entidad. En cumplimiento de los lineamientos de seguridad de la información, la Entidad se abstiene de divulgar marcas, fabricantes o versiones específicas de las tecnologías que conforman su infraestructura, dado que esta información es clasificada como sensible y su exposición podría incrementar la superficie de riesgo frente a amenazas cibernéticas externas. En consecuencia, el alcance del servicio de Vigilancia Tecnológica requerido por la Entidad comprende, de manera general, los siguientes componentes: -Infraestructura de red y mecanismos de seguridad perimetral (incluyendo firewalls de nueva generación). -Aplicaciones web y APIs. -Servicios en la nube y plataformas colaborativas. -Sistemas de información misionales y administrativos. -Gestión de identidades y accesos. -Estaciones de trabajo y servidores. -Activos expuestos en Internet, incluyendo aquellos presentes en espacios no indexados o de acceso restringido (Deep Web y Dark Web). El servicio de vigilancia tecnológica deberá cubrir tanto las tecnologías actualmente implementadas como aquellas que se incorporen durante la vigencia del contrato, garantizando un monitoreo continuo y actualizado frente a la evolución del entorno tecnológico y las amenazas emergentes. En caso de requerirse un mayor nivel de detalle técnico para asegurar la correcta prestación del servicio, la Entidad suministrará dicha información únicamente al proveedor adjudicatario, bajo la firma de acuerdos de confidencialidad y no divulgación de información y conforme a los procedimientos establecidos en su política de seguridad de la información.								
3	29/04/2026	Punto 2 GESTION DE VULNERABILIDADES: se aclara a la entidad que es necesario saber las cantidades y tipo de activos, por ejemplo cuantos activos de infraestructura son y cuantas paginas o sitios web, como tambien cuales son los servicios en nube, si es IaaS o se refiere a plataformas de proveedores publicos y si es infraestructura en nube cuantos activos son.	La Entidad cuenta con un entorno tecnológico híbrido que integra componentes on-premise y servicios en la nube. Se disponen ambientes web y sistemas de información desplegados tanto en infraestructura local (on-premise) como en múltiples proveedores de servicios en la nube, incluyendo Microsoft Azure, Google Cloud Platform y Oracle Cloud, entre otros. Se tiene una infraestructura tecnológica aproximada de 300 servidores, alrededor de 50 ambientes web y múltiples dispositivos de red, operando bajo un entorno híbrido que integra componentes locales y servicios en la nube, lo cual demanda una gestión integral, continua y especializada en materia de seguridad de la información y ciberseguridad.								
4	29/04/2026	Punto 2 GESTION DE VULNERABILIDADES: se solicita amablemente aclarar el alcance, debido a que en el 3er parrafo de este punto, se habla de Adversary Emulation, red teaming y threat Hunting, estos puntos son ejercicios totalmente diferentes a la gestion de vulnerabilidades, igualmente se requiere incluirlo?	En relación con el Punto 2 – Gestión de Vulnerabilidades, se aclara que el alcance del servicio sí incluye Adversary Emulation, Red Teaming y Threat Hunting, integrados de manera transversal al proceso de gestión de vulnerabilidades y no como ejercicios independientes. Estas capacidades se incorporan para contextualizar los hallazgos técnicos frente a escenarios reales de amenaza, correlando las vulnerabilidades identificadas con tácticas, técnicas y procedimientos utilizados por actores de amenaza, bajo la alineación conceptual del marco MITRE ATT&CK y la referencia metodológica del NIST SP 800-115, fortaleciendo la priorización del riesgo, la validación de la explotabilidad y la toma de decisiones de remediación, en complemento a los estándares CVSS y OWASP.								
5	29/04/2026	Punto 2 componente especializado. Se aclara a la entidad que podemos brindar acompañamiento en el ciclo de vida de las vulnerabilidades, sin embargo, la ejecución de la remediación es responsabilidad de Valor+.	La ejecución de las acciones de mitigación y remediación corresponde directamente a la entidad. Sin embargo, en múltiples ocasiones se requiere el acompañamiento de la empresa del Servicio de Vigilancia Tecnológica para brindar apoyo técnico especializado y estratégico a los responsables de la plataforma tecnológica, facilitando el proceso de mitigación de las brechas de seguridad informática derivadas de las vulnerabilidades identificadas. Este acompañamiento deberá incluir la realización de sesiones técnicas, orientados a explicar los vectores de explotación, recomendaciones para su adecuada mitigación y remediación. Contribuyendo de manera efectiva al proceso de gestión y cierre de vulnerabilidades.								

Fecha (DD/MM/AA)	Pregunta o inquietud formulada	Respuesta por parte de Valor+ S.A.S.
6 29/04/2026	se solicita a la entidad aclarar el alcance en la gestión de vulnerabilidades debido a que en el documento Pag 10, solicitan servicios de ethical hacking caja negra y/o gris, esto significa que también se debe aplicar ethical hacking a todos los activos de la entidad y de manera mensual? si es así, por favor indicar la cantidad y tipo de activos.	En el alcance del servicio se expresa lo siguiente: "Realización de pruebas de penetración mensuales (caja negra y/o caja gris) sobre la plataforma tecnológica de la entidad, priorizando los activos críticos y aquellos que la organización considere estratégicos, con el fin de identificar y mitigar oportunamente vulnerabilidades de seguridad informática". La entidad cuenta con una infraestructura tecnológica aproximada de 300 servidores, alrededor de 50 ambientes web y múltiples dispositivos de red, operando bajo un entorno híbrido que integra componentes locales y servicios en la nube. Lo anterior incluye tecnologías actuales y futuras que sean incorporadas durante la ejecución del contrato. El servicio se presta de manera continua bajo un enfoque de ciberseguridad preventiva y proactiva, orientado a la identificación temprana, gestión oportuna y mitigación efectiva de riesgos y vulnerabilidades, fortaleciendo de forma permanente la postura de seguridad de la entidad.
7 29/04/2026	Punto 3 La gestión de superficie de ataque, para este punto se solicita aclarar si lo requerido es una consultoría basada en la ISO/IEC 27001.	Se aclara que el servicio no corresponde a una consultoría específica para la Implementación o certificación de la Norma ISO/IEC 27001, sino que está orientado a la prestación de servicios especializados en seguridad de la Información y ciberseguridad, los cuales serán ejecutados conforme a las necesidades, requerimientos y prioridades definidas por la entidad durante la vigencia contractual. Es un servicio de Vigilancia Tecnológica (Deep Web y Dark Web). El servicio contempla la operación continua de un esquema de ciberseguridad preventiva y proactiva, estructurado en tres (3) ejes fundamentales: (1) Vigilancia Tecnológica, (2) Gestión de Vulnerabilidades y (3) Gestión de la Superficie de Ataque. Estos componentes permiten identificar, analizar y mitigar riesgos asociados a la exposición de activos digitales. Estos componentes permiten identificar, analizar y mitigar riesgos asociados a la exposición de activos digitales. Adicionalmente, incluye la realización de pruebas de penetración mensuales (caja negra y/o caja gris), así como la disponibilidad de una aplicación web para la visualización, seguimiento y control de las vulnerabilidades identificadas, tanto por el servicio de vigilancia como por otras herramientas de la entidad. Es de señalar, que en el documento "Condiciones de la contratación Convocatoria Abreviada N°012-2026", en el numeral "1.5. Alcance y/o Especificaciones Técnicas del Bien o Servicio a Contratar, en la Gestión tratamiento de vulnerabilidades" señala: <u>El proveedor deberá ejecutar las actividades descritas, garantizando el cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad (ISO 27001, NIST, MITRE ATTACK, OWASP, entre otros). Deberá presentar certificación manifiesto que garantiza lo anterior.</u>
8 29/04/2026	se solicita amablemente a la entidad ampliar el plazo de entrega, esto con el fin de validar de acuerdo a las respuestas a las observaciones las diferentes escenas del proyecto. Se sugiere el 12 de mayo del 2026	No se acepta la observación, considerando la alta criticidad, prioridad y urgencia que demanda la prestación del servicio, dado que su ejecución oportuna es fundamental para garantizar la continuidad, fortalecimiento y protección de la seguridad de la Información y la infraestructura tecnológica de la entidad. En el documento "Condiciones de la Contratación Convocatoria Abreviada N° 012-2026", en el numeral "1.2. Cronograma del Proceso" se tienen establecido los plazos para cada etapa. 1.2 Cronograma del Proceso
9 29/04/2026	Con relación a la convocatoria en asunto solicitamos aclaración sobre los activos que requieren gestión ya que en el punto N°2 hacen referencia a los activos internos. Vigilancia tecnológica ¿Cuántos dominios, marcas o activos digitales se deben monitorear? ¿El alcance incluye únicamente la entidad principal o también filiales? ¿Se requiere monitoreo en Deep y Dark Web con alertas en tiempo real? ¿Frecuencia esperada de reportes (semanal, mensual, ambos)? Se quiere cotizar takedowns, cuantos?	El alcance del servicio comprende los dominios, plataformas, sistemas y ambientes tecnológicos asociados a Antioquia, Salud, Vehículos, Tasa de Seguridad, Educación, Hacienda, Seguridad Ciudadana, Catastro, Sede Electrónica, así como cualquier otro dominio, activo digital o componente tecnológico perteneciente o administrado por la Gobernación de Antioquia, conforme a las necesidades, prioridades y criticidad definidas por la entidad. Adicionalmente, todo nuevo desarrollo, implementación tecnológica, aplicación, sistema o servicio digital que sea incorporado a la Infraestructura Institucional deberá ser objeto de un análisis de seguridad detallado, incluyendo evaluaciones técnicas especializadas, identificación de vulnerabilidades, validación de controles de seguridad y pruebas que permitan detectar riesgos potenciales antes de su salida a producción, garantizando así la protección integral de la plataforma tecnológica y el fortalecimiento continuo de la postura de ciberseguridad institucional. La Entidad cuenta con activos digitales expuestos a internet como portales web, aplicaciones, APIs y servicios en la nube. Se requiere que el servicio contemple capacidades de monitoreo en Deep Web y Dark Web, orientadas a la identificación de posibles filtraciones de información, credenciales comprometidas, suplantaciones de marca, dominios fraudulentos u otras amenazas asociadas a la Entidad. Se espera un esquema combinado de reportes que incluya: Reportes semanales y Mensuales con el consolidado de lo identificado. Adicionalmente, se deberán generar reportes extraordinarios en caso de hallazgos críticos o incidentes relevantes. El servicio de takedowns no se tiene incluido en el alcance del proyecto
10 29/04/2026	Gestión de vulnerabilidades ¿Cuántos activos se van a evaluar? () ¿Que tipo de activos son y cuantos por cada uno? (IPs, servidores, endpoints, aplicaciones web, servicios en la nube, etc) ¿Se requiere escaneo continuo o únicamente mensual? ¿Se espera incluir validación de remediación (retest)?	La entidad cuenta con una infraestructura tecnológica aproximada de 300 servidores, alrededor de 50 ambientes web y múltiples dispositivos de red, operando bajo un entorno híbrido que integra componentes locales y servicios en la nube, lo cual demanda una gestión integral, continua y especializada en materia de seguridad de la información y ciberseguridad. Se requiere escaneo continuo y un informe mensual En caso de requerirse la validación de remediación (retest), el proveedor deberá realizarlo.

Fecha (DD/MM/AA)	Pregunta o inquietud formulada	Respuesta por parte de Valor+ S.A.S.
11 29/04/2026	Pruebas de seguridad (Pentesting / Red Team) ¿Cuántos activos críticos desean evaluar? ¿Qué tipo de pruebas requieren (caja negra, gris, Red Team completo)? ¿Desean incluir ejercicios de Ingeniería social? ¿Tienen definida una duración estimada para estos ejercicios?	La entidad cuenta con una infraestructura tecnológica aproximada de 300 servidores, cerca de 50 ambientes web y múltiples dispositivos de red en un entorno híbrido. En este contexto, se prioriza la evaluación continua de los activos críticos y de aquellos componentes estratégicos que la entidad determine según su nivel de riesgo e impacto operativo. Respecto a los activos críticos; Dentro de la cantidad de ambientes se podría decir que la cantidad no es exacta ya que al tener alrededor de 50 y múltiples dispositivos estos serían los activos a tener en cuenta para ser evaluados en los momentos que se requieran. Se requiere la realización de pruebas de penetración mensuales bajo metodologías de caja negra y/o caja gris sobre la plataforma tecnológica institucional, enfocadas en identificar, evaluar y contribuir a la mitigación oportuna de vulnerabilidades de seguridad informática. No se contempla dentro del alcance la ejecución de ejercicios de Ingeniería social. La prestación del servicio se establece bajo un esquema continuo, con un enfoque preventivo, proactivo y de mejora permanente, orientado al fortalecimiento constante de la postura de ciberseguridad de la entidad. Es importante aclarar que el servicio de Vigilancia Tecnológica no se limita exclusivamente a los activos clasificados como críticos, sino que está orientado a la plataforma tecnológica de la Entidad.
12 29/04/2026	Gestión de superficie de ataque ¿Cuentan actualmente con un inventario de activos o debe construirse desde cero? ¿Cuántos dominios, subdominios e IPs públicas manejan? ¿Qué tan dinámico es su entorno (on-premise, nube, híbrido)?	La entidad cuenta con una infraestructura tecnológica aproximada de 300 servidores, alrededor de 50 ambientes web y múltiples dispositivos de red, operando bajo un entorno híbrido que integra componentes locales y servicios en la nube, lo cual demanda una gestión integral, continua y especializada en materia de seguridad de la Información y ciberseguridad. La Entidad dispone de un esquema de direccionamiento IP público con un bloque aproximado de 128 direcciones IP. No obstante, es importante precisar que la infraestructura tecnológica también incluye activos desplegados en servicios de hosting externo y entornos en la nube, particularmente en Microsoft Azure, así como otros proveedores, lo que puede incrementar la cantidad de direcciones IP públicas y recursos expuestos. El proveedor deberá contemplar mecanismos de descubrimiento y monitoreo continuo de la superficie de ataque externa, incluyendo dominios, subdominios e IPs públicas, tanto en infraestructura propia como en servicios de terceros, garantizando una cobertura integral y actualizada durante la ejecución del servicio. De acuerdo con lo señalado en el documento "Condiciones de la Contratación Convocatoria Abreviada N° 012-2026" en el numeral "1.5 Alcance y/o Condiciones y/o Especificaciones Técnicas del Bien o Servicio a Contratar", se establece que deberá entregar: ▪ Realizar el levantamiento, clasificación y documentación de los activos tecnológicos objeto del servicio.
13 29/04/2026	Evaluación de riesgo cibernético ¿Requieren una evaluación puntual o un seguimiento continuo? ¿Qué nivel de profundidad esperan (alto nivel o análisis cuantitativo detallado)?	La entidad requiere un servicio de evaluación y seguimiento continuo, ejecutado conforme a las necesidades institucionales, prioridades estratégicas y eventos de ciberseguridad que se presenten durante la vigencia contractual, garantizando una gestión permanente, preventiva y proactiva de la seguridad informática. Se espera un análisis cuantitativo detallado, orientado a identificar, validar y documentar técnicamente las vulnerabilidades detectadas, demostrando de manera clara su nivel de explotación, impacto potencial y criticidad sobre la infraestructura tecnológica. Cada hallazgo deberá estar debidamente soportado con evidencia técnica, análisis de riesgo y documentación precisa que facilite la toma de decisiones y la implementación efectiva de acciones de mitigación.
14 29/04/2026	Modelo de servicio y equipo ¿Se espera un servicio gestionado continuo o bajo demanda? ¿Horario requerido (8x5, 24x7)? ¿Nivel de especialización esperado del equipo?	La entidad requiere un servicio gestionado continuo, orientado a brindar apoyo permanente al área de ciberseguridad, bajo un enfoque preventivo, proactivo y estratégico que permita fortalecer de manera constante la postura de seguridad de la infraestructura tecnológica institucional. El servicio deberá prestarse bajo un esquema de disponibilidad 24/7, garantizando capacidad de atención, monitoreo, respuesta y acompañamiento oportuno ante vulnerabilidades, riesgos o eventos de ciberseguridad que puedan afectar la operación de la entidad. Se exige un alto nivel de especialización del equipo de trabajo, conformado por profesionales con perfil experto en ciberseguridad, experiencia comprobada y certificaciones especializadas en identificación, análisis, explotación ética y gestión de vulnerabilidades, asegurando así la calidad técnica, profundidad y efectividad de los servicios prestados. De acuerdo con lo señalado en el documento "Condiciones de la Contratación Convocatoria Abreviada N° 012-2026" en el numeral "1.5 Alcance y/o Condiciones y/o Especificaciones Técnicas del Bien o Servicio a Contratar", se establece: El Proveedor deberá disponer de un componente de personal especializado para la gestión de vulnerabilidades, el cual será responsable de la operación continua del servicio. Este equipo deberá garantizar la gestión integral del ciclo de vida de las vulnerabilidades, desde su identificación hasta su erradicación, incluyendo la validación de la explotación potencial. De igual forma, deberá garantizar que los datos obtenidos de la entidad se respalden en servidores seguros, respaldados y con políticas de retención y acceso de acuerdo a los requerimientos de la entidad.  Valor+ Sociedad por Acciones Simplificada Calle 100 No. 100-100, Bogotá, D.C. Teléfono: +57 (0)2 280 1000 Correo electrónico: contacto@valorplus.com.co Sitio web: www.valorplus.com.co El personal asignado deberá contar con formación profesional en áreas afines a tecnologías de la información y ciberseguridad, así como certificaciones vigentes de reconocidas empresas internacionales (como CISSP, OSCP, CISM, CREST o equivalentes). Adicionalmente, deberán acreditar experiencia comprobada en la ejecución de pruebas de penetración, análisis de vulnerabilidades y gestión de riesgos tecnológicos. Debe ser personal calificado, con experiencia y con acceso a la información de la entidad.

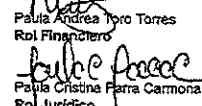
Equipo estructurador


Carlos Arturo Correa Parra
Revisor Técnico


Daniela María López Angulo
Rol Logístico


Verónica Restrepo Álvarez
Rol Financiero


Paula Andrea Toro Torres
Rol Financiero


Paula Cristina Parra Carmona
Rol Jurídico



RE: Respuesta a observaciones Convocatoria Abreviada N° 12-2026

Desde Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

Fecha Lun 04/05/2026 12:01

Para Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Sergio Andres Velez Upegui <coordinacion.mesa@valormas.gov.co>

CC Hector Dario Yepes Vega <dir.contratacion@valormas.gov.co>; Hernan Echavarria Duque <gerencia.tecnologia@valormas.gov.co>; Richard Rendon Hoyos <richard.rendon@valormas.gov.co>

Buen día Paula

Revisando el documento con las observaciones presentadas se aprueba con el fin de proceder con la publicación.

Atento a sus comentarios.

Gracias por su atención.



Carlos Arturo Correa Correa

Profesional Universitario

carlos.correa@valormas.gov.co

Calle 42 # 52-27, Edificio Edestel, Piso 3 Sector Alpujarra,
Medellín - Colombia

Este correo electrónico es confidencial y pertenece exclusivamente de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

De: Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

Enviado: lunes, 4 de mayo de 2026 11:36

Para: Sergio Andres Velez Upegui <coordinacion.mesa@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

Cc: Hector Dario Yepes Vega <dir.contratacion@valormas.gov.co>; Hernan Echavarria Duque <gerencia.tecnologia@valormas.gov.co>; Richard Rendon Hoyos <richard.rendon@valormas.gov.co>

Asunto: Respuesta a observaciones Convocatoria Abreviada N° 12-2026

Cordial saludo,

Se comparte documento en excel con respuesta a las observaciones presentadas. Se agradece validar y si es del caso y aprobar o realizar los comentarios respectivos a través de correo. Se agradece compartir antes de las 2:00 pm, con el fin de proceder a la publicación.

Cordialmente,



Paula Cristina Parra Carmona

Profesional Especializada Grado I

paula.parra@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alajuela
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) es dirigida.
Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución
o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos
cancelar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

**RE: Respuesta a observaciones Abreviada N° 012-2026**

Desde Victor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

Fecha Lun 04/05/2026 16:32

Para Compras Valor + 2 <compras2@valormas.gov.co>

CC Compras Valor + <compras@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

Buenas tardes.

Dando respuesta a lo solicitado se carga información al sitio web de la entidad.

Convocatoria Abreviada N°012-2026

Convocatoria Abreviada N°012-2026.

Objeto: "Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet"

1. Condiciones de la contratación
2. Cronograma Convocatoria Abreviada
3. CDP
4. Relación Experiencia Técnica
5. Formato Autorización de tratamiento de datos personales
6. Anexo Resolución de inquietudes
7. Formato Inhabildades e Incompatibilidades
8. Formato Certificación de lavado de activos y financiación del Terrorismo - SARLAFT.
9. Formato Propuesta Económica
10. Respuesta a Observaciones - Convocatoria Abreviada N°012-2026.pdf

Gracias por la atención prestada
Saludos



Victor Rodrigo Galvis Zuleta

Contratista
victor.galvis@valormas.gov.co
Carrera 53A #42-161 Torre B, Piso 6
Ed. Plaza de la Libertad
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige.
Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución
o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos
notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

De: Compras Valor + 2 <compras2@valormas.gov.co>

Enviado el: lunes, 4 de mayo de 2026 4:22 p. m.

Para: Victor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

CC: Compras Valor + <compras@valormas.gov.co>; Paula Andrea Toro Torres

<gerencia.financiera@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Carlos

Arturo Correa Correa <carlos.correa@valormas.gov.co>; Paula Cristina Parra Carmona

<paula.parra@valormas.gov.co>

Asunto: Respuesta a observaciones Abreviada N° 012-2026

Cordial saludo,

Amablemente solicito tu ayuda por favor, para publicar las respuestas a las observaciones en la página web de la entidad.

Convocatoria Abreviada N°012-2026.

Objeto: "Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet"

Quedo atenta,

Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.



Respuesta a observaciones Abreviada N° 012-2026

Desde Compras Valor + 2 <compras2@valormas.gov.co>

Fecha Lun 04/05/2026 16:22

Para Victor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

CC Compras Valor + <compras@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

 1 archivo adjunto (426 KB)

Respuesta a Observaciones - Convocatoria Abreviada N°012-2026.pdf;

Cordial saludo,

Amablemente solicito tu ayuda por favor, para publicar las respuestas a las observaciones en la página web de la entidad.

Convocatoria Abreviada N°012-2026.

Objeto: "Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet"

Quedo atenta,

Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,

Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

12/5/26, 11:15

Bandeja de entrada: Paula Cristina Parra Carmona - Outlook

ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."

Quedamos atentos a cualquier inquietud u observación.

Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,

Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

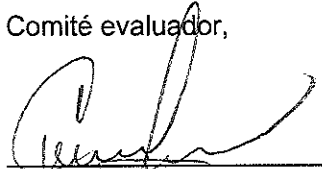
ACTA DE RECEPCIÓN DE PROPUESTAS
Convocatoria Abreviada N° 012 DE 2026

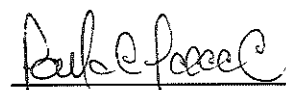
OBJETO: "Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."

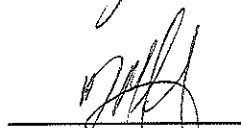
En cumplimiento del cronograma establecido dentro del proceso de la referencia, se deja constancia que siendo las **17:00 horas del día seis (06) de mayo de 2026**, fecha y hora límite para la recepción de propuestas, **se recibió la siguiente propuesta** por parte de posibles oferentes dentro del término señalado:

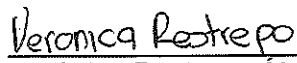
Proponente	Nit	Fecha y hora de Recepción	Valor Propuesta	Medio de recibo de la propuesta	# Folios
INTRUST SECURITY S.A.S	901.380.604-6	06/05/2026 16:12 horas	\$55.800.000	compras2@valormas.gov.co	Se recibe por medio digital

Comité evaluador,

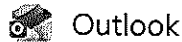

Carlos Arturo Correa Correa
Rol técnico


Paula Cristina Parra Carmona
Rol jurídico


Daniela Maria Lopez
Rol logístico


Verónica Restrepo Álvarez
Rol Financiero


Paula Andrea Toro Torres
Rol Financiero



RE: Acta presentacion de propuestas - Abreviada N° 012 -2026

Desde Victor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

Fecha Jue 07/05/2026 11:38

Para Compras Valor + 2 <compras2@valormas.gov.co>

CC Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

Buenos días

Dando respuesta a lo solicitado se carga documento al sitio web de la entidad.

Convocatoria Abreviada N°012-2026

Convocatoria Abreviada N°012-2026.

Objeto: "Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de Internet y Darknet"

1. Condiciones de la contratación
2. Cronograma Convocatoria Abreviada
3. COP
4. Relación Experiencia Técnica
5. Formulario Autorización de tratamiento de datos personales
6. Anexo Resolución de inquietudes
7. Formato Inhabilidades e incompatibilidades
8. Formato Certificación de lavado de activos y financiación del Terrorismo - SARLAFT.
9. Formato Propuesta Económica
10. Respuesta a Observaciones - Convocatoria Abreviada N°012-2026.pdf
11. ACTA RECEPCIÓN DE PROPUESTAS.pdf

Gracias por la atención prestada
Saludos



Victor Rodrigo Galvis Zuleta

Contratista

victor.galvis@valormas.gov.co

Carrera 53A #42-151, Torre B, Piso 6,

Ed. Plaza de la Libertad,

Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

De: Compras Valor + 2 <compras2@valormas.gov.co>

Enviado el: jueves, 7 de mayo de 2026 11:32 a. m.

Para: Victor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

CC: Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>;

Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>
Asunto: Acta presentacion de propuestas - Abreviada N° 012 -2026

Cordial saludo,

Amablemente solicito tu ayuda por favor, para publicar el Acta en la página web de la entidad.

Convocatoria Abreviada N°012-2026.

Objeto: ***"Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."***

Quedo atenta,
Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Aloujarra,
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige.
Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución
o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos
notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

PROPUESTA

Prestación de servicios de vigilancia tecnológica en ciberseguridad (monitorización Internet + Darknet)

PRESENTADA A:

VALOR + S.A.S.

Mayo, 2026

Contenido

Capítulo 1: Documentos legales	4
1.1 Presentación	4
1.2 Resumen.....	6
1.3 Referencias comerciales.	7
Capítulo 2: Propuesta técnica	10
2.1 Alcance	10
2.1.1 Vigilancia Tecnológica:	10
2.1.2 Gestión de Vulnerabilidades:	10
2.1.3 Gestión de Superficie de Ataque:	11
2.1.4 Levantamiento y análisis de la infraestructura tecnológica:	11
2.1.5 Evaluación del riesgo cibernético institucional:	11
2.1.6 Cumplimiento de estándares y buenas prácticas:	12
Capítulo 3: Entregables	12
Capítulo 4: Acuerdos de Nivel de Servicio	12
Capítulo 5: Metodología	13
5.1 Equipo técnico.	13
5.2 Experiencia demostrada:	13
5.3 Metodología de los servicios propuestos	14
5.3.1 Vigilancia Tecnológica	14
5.3.2 Gestión de Vulnerabilidades	14
5.3.3 Gestión de Superficie de Ataque	14
5.3.4 Levantamiento y Análisis de la Infraestructura Tecnológica	15
5.3.5 Evaluación del Riesgo Cibernético	15
5.4 Especificaciones de valores agregados propuestos en los servicios:	16
Capítulo 6: Propuesta económica	16
6.1 Precio por servicio por 8 meses:	16
6.2 Forma de pago.....	16
6.3 Condiciones comerciales.....	17

Contacto

Nombre	Dirección	Teléfono
Johanny Chacón Navas	Calle 72 sur # 33-59 Urb. Selvática	317 344 5232
Sergio Mauricio barón vera	Carrera 8 # 34 a 34 torre 3 apto 103, Ed. La Plazoleta	3012807037
Daniel Muñoz Giraldo	Carrera 63 B # 40 a Sur 75	300 213 7893
Sharon Quintero Navas	Calle 72 sur # 33-59 Urb. Selvática	320 570 9274

Capítulo 1: Documentos legales

1.1 Presentación

Señores

Valor + S.A.S

En Intrust Security S.A.S, entendemos que la ciberseguridad no es solo una necesidad operativa, sino una inversión estratégica para proteger la continuidad y reputación de su empresa. Con base en nuestra experiencia previa trabajando con ustedes, nos complace presentar nuestra propuesta mejorada, la cual integra servicios actuales y nuevas capacidades diseñadas para enfrentar un panorama de amenazas en constante evolución.

Nuestra filosofía va más allá de reaccionar a incidentes; anticipamos amenazas, protegemos proactivamente sus activos críticos y alineamos nuestras soluciones con sus objetivos de negocio. Nuestro enfoque considera no sólo los riesgos técnicos, sino también el impacto estratégico, asegurando que cada acción fortalezca el gobierno, riesgo y cumplimiento en su organización.

Nos enorgullece ser pioneros en el uso de herramientas avanzadas como sistemas de gestión de vulnerabilidades patentados, monitoreo continuo de la superficie de ataque y capacidades únicas de detección en Darknet. Estas tecnologías nos posicionan como líderes en soluciones integradas y nos diferencian de la competencia al ofrecer análisis más precisos y resultados medibles.

Con la inclusión de nuevos servicios como Red Team, gestión de vulnerabilidades, simulaciones de ataque basadas en MITRE ATT&CK y threat simulation utilizando plataformas como Vectr, fortalecemos la capacidad de detectar, mitigar y prevenir amenazas avanzadas. Estos servicios complementan nuestras soluciones previas de Ethical Hacking, ASM y Phishing Offensive Response, ofreciendo una cobertura integral que garantiza la resiliencia cibernética de su empresa.

Nuestra combinación de automatización e inteligencia artificial reduce costos operativos sin comprometer la calidad. Esto se traduce en un servicio altamente eficiente, permitiendo a su organización maximizar el retorno de inversión mientras garantiza un nivel óptimo de seguridad.

El liderazgo en Intrust Security no solo se limita al ámbito corporativo; nuestro CEO, COO y equipo participan activamente en la docencia y en conferencias globales como Defcon, Ekoparty y Bsides Las Vegas. Estas experiencias nos permiten mantenernos a la vanguardia de la industria y aplicar conocimientos de última generación en cada proyecto que emprendemos.

A diferencia de otros proveedores, nuestra combinación de tecnología exclusiva, experiencia global y enfoque en la personalización de soluciones nos permite adaptarnos rápida y específicamente a las necesidades de su organización. Entendemos las particularidades de su sector y nos comprometemos a ser más que un proveedor: un socio estratégico en ciberseguridad.

Estamos seguros de que esta propuesta representa una oportunidad para robustecer su estrategia de seguridad de forma efectiva y rentable. Quedamos atentos para programar una reunión y discutir cómo podemos empezar a trabajar juntos en la implementación de estas soluciones.

Agradecemos la confianza depositada en Intrust Security y reiteramos nuestro compromiso de continuar construyendo una relación sólida y beneficiosa para ambas partes.

Cordialmente,

Sergio Mauricio Barón Vera
Representante Legal
Intrust Security S.A.S
3012807037
sbaron@intrustsecurity.co

1.2 Resumen

Intrust Security S.A.S ha tenido una activa participación en las principales conferencias de ciberseguridad del mundo, como Defcon, Ekoparty y Bsides Las Vegas, que consolida nuestra posición como líderes en el sector. Este contacto directo con investigadores y expertos internacionales nos brinda un conocimiento de primera mano sobre los avances más recientes y las amenazas emergentes en el ámbito digital. Además, nuestro rol como voluntarios en estos eventos destaca nuestro compromiso genuino con la comunidad y nuestra constante búsqueda de mejora en la ciberseguridad.

En paralelo, nuestras colaboraciones con empresas como Importadoras Asociadas, la Universidad de Medellín y otras organizaciones, han demostrado nuestra capacidad para ofrecer servicios especializados con un enfoque integral. Por ejemplo:

Importadoras Asociadas: Llevamos a cabo una evaluación de seguridad externa que incluye 6 pruebas de penetración en modalidad caja gris, gestión continua de la superficie de ataque (ASM) y monitoreo continuo de marca, durante un período de 12 meses.

Universidad de Medellín: Implementamos un servicio basado en pruebas técnicas de ciberseguridad, incluyendo monitoreo, gestión de vulnerabilidades, catalogación de activos digitales, análisis de phishing y pruebas de penetración. Este proyecto abarcó un contrato desde noviembre de 2023 hasta noviembre de 2024, con entregas mensuales detalladas y el uso de metodologías avanzadas como Attack Surface Management y estrategias anti-phishing.

TCC S.A: La contratación de nuestros servicios abarcó el escaneo de vulnerabilidades, pruebas de seguridad en código y pruebas de intrusión, soporte durante incidentes de ciberseguridad, y la ejecución de campañas de ingeniería social. Este proyecto, con una duración inicial de 12 meses prorrogables automáticamente, también incluyó el alertamiento continuo de activos críticos mediante un SOC dedicado.

Aunque somos una empresa joven, nuestras experiencias abarcan desde la identificación de vectores de ataque novedosos hasta la implementación de soluciones modernas y efectivas, adaptadas a cada cliente. Este enfoque proactivo y actualizado nos permite mantenernos siempre un paso adelante frente a las amenazas, asegurando un valor agregado significativo para nuestros socios y la comunidad.

1.3 Referencias comerciales.

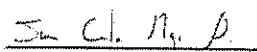


Medellín, 27 de noviembre de 2024

A quien corresponda;

Mediante esta carta, compartimos la referencia comercial de nuestro aliado **Intrust Security**, con el cual llevamos operando varios años iniciando en julio del 2022; el contrato actual inicio el 24 de julio del 2024 con una duración de 12 meses, donde se tienen los siguientes servicios de ciberseguridad: escaneo de vulnerabilidades, pruebas de seguridad (código e intrusión), campañas de ingeniería social, alertamiento de activos críticos y apoyo durante incidentes, para todas nuestras unidades de negocio (Agencia de Aduanas Mario Londoño S.A, Fracor S.A.S, Global Mensajería S.A.S y TCC S.A.S), por un valor de \$110.384.400 iva incluido.

Damos fe de todo esto en la ciudad de Medellín, a 27 de noviembre de 2024.



Juan Camilo Mejía Arango
Coordinador de Infraestructura y seguridad TI
Grupo Logístico TCC

GRUPO LOGÍSTICO TCC
TCC S.A.S.
Sede administrativa: Carrera 64 # 678 - 35 - Medellín, Colombia
Teléfono: (4) 444 48 88 / www.tcc.com.co



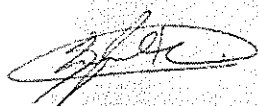
CERTIFICADO

A QUIEN PUEDA INTERESAR

Por medio de la presente hacemos constar que la empresa **INTRUST SECURITY S.A.S** con Nit.901.380.604-6 mantiene relaciones comerciales actualmente con **IMPORTADORA CELESTE** con Nit. 800004800 desde el primero de diciembre del 2023 con una duración de 12 meses, donde se tienen los siguientes servicios de ciberseguridad: escaneo de vulnerabilidades, pruebas de seguridad, campañas de ingeniería social y alertamiento de activos críticos.

Constancia que se emite a solicitud de la parte interesada en la ciudad de Medellín a los veintiséis (26) días del mes de noviembre del 2024.

Cordialmente,



DEBIER SNEYDER MARTINEZ
Jefe de Infraestructura TI

CLAS 8079
MAYEAD VENTAS
Certificación



AUTOPARTES ORIGINALES



ACDelco

MAZDA

MOTRIO

BOSCH

HYUNDAI

www.importadorasasociadas.com

Bogotá 27 noviembre de 2024

CERTIFICADO

A QUIEN PUEDA INTERESAR

Por medio de la presente certificamos que la empresa **INTRUST SECURITY S.A.S**, con Nit. 901.380.604-6, mantiene relaciones comerciales vigentes con **MODUSOFTWARE**, con Nit. 900229015 -1, desde el dieciséis (16) de enero de 2023, bajo un contrato con una duración de 12 meses. En el marco de esta relación comercial, se han desarrollado servicios especializados en ciberseguridad.

Constancia que se emite a solicitud de la parte interesada en la ciudad de Bogotá D.C a los veintisiete (27) días del mes de noviembre del 2024.

Cordialmente,



LUISA FERNANDA RÍOS ARANGO
GERENTE DE OPERACIONES
lfrios@modusoftware.com

Capítulo 2: Propuesta técnica

2.1 Alcance

La presente propuesta tiene como propósito fortalecer la postura de seguridad de Valor + S.A.S, mediante la implementación de servicios especializados de vigilancia tecnológica en ciberseguridad, orientados a proteger los diferentes proyectos de la entidad mediante monitorización continua de Internet y Darknet, detectar amenazas emergentes, gestionar vulnerabilidades, monitorear la superficie de ataque, evaluar el riesgo cibernético institucional y garantizar el cumplimiento de estándares internacionales.

Detalle de los servicios ofertados:

2.1.1 Vigilancia Tecnológica:

Se emplearán plataformas especializadas de inteligencia de amenazas (Threat Intelligence), cuya selección estará debidamente sustentada mediante criterios técnicos, funcionales y de cobertura. Esta actividad se complementará con la entrega periódica de informes ejecutivos y técnicos, los cuales contendrán como mínimo: los hallazgos identificados, su nivel de criticidad, análisis de riesgo, posibles impactos para la entidad y recomendaciones claras y accionables.

• **Entregables:**

- Informes semanales detallados con: hallazgos técnicos detectados, niveles de criticidad, riesgos asociados, tendencias o alertas relevantes, y recomendaciones inmediatas de contención o mitigación.
- Monitoreo constante del entorno digital, Internet y Darknet, para detectar amenazas emergentes, filtraciones de información, campañas de ataque, vulnerabilidades críticas y exposición de datos.

2.1.2 Gestión de Vulnerabilidades:

El servicio se ejecutará mediante escaneos de seguridad con periodicidad mínima mensual, así como análisis extraordinarios bajo demanda, en respuesta a incidentes de seguridad, cambios o solicitud expresa de la entidad. Se entregarán informes técnicos detallados y reportes ejecutivos con hallazgos, nivel de criticidad, evidencias, recomendaciones de mitigación y planes de remediación.

Para la clasificación y priorización de vulnerabilidades se aplicarán estándares internacionales como CVSS, buenas prácticas de OWASP para aplicaciones web,

y el marco metodológico NIST SP 800-115. Las actividades estarán articuladas con el marco MITRE ATT&CK, incorporando enfoques como Adversary Emulation, Red Teaming y Threat Hunting.

2.1.3 Gestión de Superficie de Ataque:

Se iniciará con el levantamiento, identificación, clasificación y análisis de la infraestructura tecnológica de la entidad. Se implementará un proceso de Gestión de Superficie de Ataque Cibernético orientado al descubrimiento, inventario, monitoreo y análisis continuo de todos los activos tecnológicos expuestos públicamente, incluyendo dominios y subdominios, direcciones IP públicas, servicios expuestos, certificados digitales y tecnologías web.

De manera complementaria, se realizará una evaluación integral del riesgo cibernético institucional, considerando el contexto actual de amenazas, la probabilidad de ocurrencia de incidentes y su impacto potencial a nivel operativo, técnico, legal y reputacional.

2.1.4 Levantamiento y análisis de la infraestructura tecnológica:

- Realizar el levantamiento, clasificación y documentación de los activos tecnológicos objeto del servicio.
- Identificar los componentes críticos, dependencias, puntos vulnerables y niveles de exposición a amenazas externas e internas.
- Priorizar los activos auditables para determinar el alcance y nivel de profundidad del análisis, con el fin de dimensionar el universo sujeto a vigilancia y gestión de vulnerabilidades.

2.1.5 Evaluación del riesgo cibernético institucional:

- Efectuar un análisis técnico y objetivo del nivel de riesgo al que se encuentra expuesta la entidad, considerando el entorno de amenazas actual, incidentes potenciales y el impacto operativo, reputacional, técnico y legal.
- Determinar la probabilidad de ocurrencia de un ciberataque y su severidad, con base en amenazas reales identificadas y verificables.
- Presentar una valoración cuantificable del riesgo cibernético, permitiendo la toma de decisiones informadas por parte de la entidad.

2.1.6 Cumplimiento de estándares y buenas prácticas:

Garantizar el cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad (ISO 27001, NIST, MITRE ATT&CK, OWASP, entre otros).

Capítulo 3: Entregables

Los documentos que se entregarán al cliente, de acuerdo a los servicios son los siguientes:

- Informe técnico detallado por cada ejercicio, que incluye:
 - Metodología implementada.
 - Hallazgos y vulnerabilidades identificadas, clasificadas por severidad.
 - Recomendaciones específicas para la mitigación de riesgos.
 - Planes de acción sugeridos.
- Informes ejecutivos y técnicos periódicos de Vigilancia Tecnológica con hallazgos, criticidad, análisis de riesgo, impactos y recomendaciones accionables.
- Informes semanales de monitoreo de Internet y Darknet.
- Informes mensuales de Gestión de Superficie de Ataque.
- Documento de levantamiento, clasificación y documentación de activos tecnológicos.
- Valoración cuantificable del riesgo cibernético institucional.
- Retest de vulnerabilidades, con su respectivo informe detallado.

Capítulo 4: Acuerdos de Nivel de Servicio

Los acuerdos de niveles de servicios van a estar definidos por las fases detalladas de alcance de la siguiente forma:

- Ejercicios de Red Team.
- Simulación de atacante interno.
- Pentesting a servicios en la Nube y onpremise.
- ASM.

- Gestión de vulnerabilidades.

Capítulo 5: Metodología

5.1 Equipo técnico.

Nuestro equipo técnico especializado cuenta con más de 5 años en el desarrollo de ejercicios en ciberseguridad para diferentes empresas del país y la región. El personal asignado contará con formación profesional en áreas afines a tecnologías de la información y ciberseguridad, así como certificaciones vigentes de reconocimiento internacional, tales como CEH, OSCP, CISA, CISSP, ISO 27001 Lead Implementer, ISO 27032 Lead Cybersecurity Manager y PMP, con experiencia comprobada en pruebas de seguridad, análisis de vulnerabilidades y gestión de riesgos tecnológicos.

Si lo requieren se presentarán los certificados con los que cuenta el equipo para garantizar la prestación del servicio y que cumple con las certificaciones y experiencia requerida.

5.2 Experiencia demostrada:

El equipo técnico de Intrust Security cuenta con más de 15 años de experiencia acumulada en ciberseguridad ofensiva, respuesta a incidentes, forense digital, seguridad en aplicaciones y gobierno de la seguridad de la información bajo marcos como ISO 27001, NIST CSF y CIS Controls. Hemos ejecutado compromisos reales en sectores financiero, logístico, educativo y de salud, incluyendo ejercicios de Red Team, análisis OSINT, pruebas de penetración sobre infraestructura crítica y gestión de incidentes activos.

Si lo requiere, podemos anexar referencias y casos de éxito de clientes anteriores bajo acuerdo de confidencialidad.

5.3 Metodología de los servicios propuestos

5.3.1 Vigilancia Tecnológica

Planeación:

- Selección y configuración de plataformas de Threat Intelligence sustentada con criterios técnicos, funcionales y de cobertura.
- Definición de indicadores de compromiso (IoC) y reglas de monitoreo específicas para la entidad.

Ejecución:

- Monitoreo continuo del entorno digital, Internet y Darknet.
- Generación de informes semanales con análisis de amenazas, tendencias y recomendaciones de contención.

5.3.2 Gestión de Vulnerabilidades

Identificación y rastreo:

- Ejecución de escaneos mensuales alineados con NIST SP 800-115 y OWASP.
- Clasificación de hallazgos mediante CVSS y articulación con MITRE ATT&CK.

Priorización y toma de decisiones:

- Clasificación de riesgos y propuestas de mitigación.
- Informes de estado con evolución de vulnerabilidades detectadas.

5.3.3 Gestión de Superficie de Ataque

Monitoreo continuo:

- Descubrimiento e inventario continuo de activos públicos: dominios, IPs, servicios, certificados.
- Generación de alertas tempranas para riesgos emergentes.

Priorización y análisis:

- Clasificación de vulnerabilidades y activos afectados según criticidad.
- Revisión mensual de hallazgos con propuestas de mitigación.

5.3.4 Levantamiento y Análisis de la Infraestructura Tecnológica

Como fase fundacional del servicio, Intrust Security ejecutará un proceso sistemático de identificación, clasificación y documentación exhaustiva de los activos tecnológicos objeto del contrato, en concordancia con los marcos de referencia ISO/IEC 27001:2022 e ISO/IEC 27005, así como las mejores prácticas del estándar NIST SP 800-171.

Este proceso comprende las siguientes actividades:

- **Inventario y clasificación de activos:** Se realizará el levantamiento integral de la infraestructura tecnológica del contratante, incluyendo activos de hardware, software, servicios en la nube, interfaces de red, sistemas de información y componentes de comunicaciones, con su correspondiente categorización por criticidad, propietario funcional y nivel de exposición.
- **Análisis de dependencias y superficie de ataque:** Se identificarán los componentes críticos del entorno tecnológico, sus interdependencias operativas, vectores de exposición ante amenazas de origen externo e interno, y las condiciones que puedan comprometer la disponibilidad, integridad o confidencialidad de la información.
- **Priorización y dimensionamiento del universo auditable:** Con base en los hallazgos del inventario y el análisis de riesgos asociado, se establecerá una matriz de priorización de activos auditables que permita definir con precisión el alcance, la profundidad analítica y la cobertura del servicio de vigilancia y gestión de vulnerabilidades, garantizando una asignación eficiente de los recursos técnicos disponibles.

Los resultados de esta fase se consolidarán en un informe técnico de línea base que servirá como referencia para la ejecución de las fases subsiguientes del contrato.

5.3.5 Evaluación del Riesgo Cibernético

- **Análisis técnico del nivel de riesgo considerando amenazas reales.**
- **Determinación de probabilidad de ocurrencia y severidad.**
- **Entrega de valoración cuantificable como insumo para decisiones estratégicas.**

5.4 Especificaciones de valores agregados propuestos en los servicios:

Los servicios propuestos tienen como objetivo fortalecer la infraestructura tecnológica de los clientes de Valor + S.A.S, manteniendo un continuo monitoreo de los activos. Se mantendrá una evaluación continua de los sistemas críticos, para garantizar la seguridad, disponibilidad y eficiencia operativa de los componentes que dependen de ellos.

Capítulo 6: Propuesta económica

6.1 Precio por servicio por 8 meses:

Items	Entregables	% sobre el total	Valor Unitario
Vigilancia Tecnológica	Informes semanales	25,00%	\$ 13.950.000
Gestión Vulnerabilidades	Informes mensuales	25,00%	\$ 13.950.000
Gestión de Superficie de Ataque	Monitoreo continuo	20,00%	\$ 11.160.000
Levantamiento y análisis de la infraestructura tecnológica	Documento inicial	12,00%	\$ 6.696.000
Evaluación del riesgo cibernético institucional	Valoración cuantificable	10,00%	\$ 5.580.000
Otros (Cumplimiento de estándares)	Certificados	8,00%	\$ 4.464.000
TOTAL		100,00%	\$ 55.800.000

6.2 Forma de pago

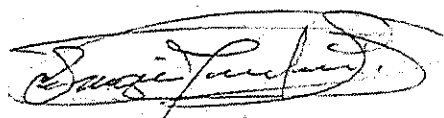
El valor total de esta propuesta es de Cincuenta y cinco millones ochocientos mil pesos (\$55.800.000) IVA incluido. La forma de pago será acordada con Valor + S.A.S según sus políticas internas de contratación.

6.3 Condiciones comerciales

Para la realización del presente contrato, se detallan las siguientes condiciones:

- Vigencia: La propuesta tiene una validez de 30 días calendario a partir de la fecha de emisión.
- Inicio: Los servicios iniciarán a la firma del contrato y acta de inicio.
- Confidencialidad: Ambas partes se comprometen a mantener la confidencialidad de toda la información compartida durante la ejecución del contrato y se firmara el NDA respectivo.

Firma del Representante Legal:



Sergio Mauricio Barón Vera

Representante Legal – Intrust Security S.A.S

NIT: 901380604-6

Objeto: Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet

Items	Entregables	% sobre el total	Valor Unitario
Vigilancia Tecnológica	El Proveedor deberá emplear plataformas especializadas de inteligencia de amenazas (Threat Intelligence), cuya selección deberá estar debidamente sustentada mediante criterios técnicos, funcionales y de cobertura. Esta actividad deberá complementarse con la entrega periódica de informes ejecutivos y técnicos, los cuales deberán contener como mínimo: los hallazgos identificados, su nivel de criticidad, análisis de riesgo, posibles impactos para la entidad y recomendaciones claras y accionables para la mitigación y gestión de las amenazas detectadas. -Realizar monitoreo constante del entorno digital, Internet y Darknet, con el propósito de detectar amenazas emergentes, filtraciones de información, campañas de ataque, vulnerabilidades críticas, exposición de datos, o actos que puedan comprometer los intereses de la entidad. -Emitir informes semanales detallados, que incluyan: - oHallazgos técnicos detectados. - oNiveles de criticidad. - oRiesgos asociados. - oTendencias o alertas relevantes. - oRecomendaciones inmediatas de contención o mitigación.	25,00%	\$ 13.950.000
Gestión Vulnerabilidades	El servicio deberá ejecutarse mediante la realización de escaneos de seguridad con una periodicidad mínima mensual, así como la ejecución de análisis extraordinarios bajo demanda, en respuesta a incidentes de seguridad, cambios o solicitud expresa de la entidad. Como resultado, el Proveedor deberá entregar informes técnicos detallados y reportes ejecutivos que incluyan hallazgos, nivel de criticidad, evidencias, recomendaciones de mitigación y planes de remediación. Para la clasificación y priorización de vulnerabilidades, el Proveedor deberá aplicar estándares internacionales, tales como el modelo CVSS (Common Vulnerability Scoring System). En el caso de aplicaciones web, deberá adoptar las buenas prácticas establecidas por OWASP (Open Web Application Security Project), y para la ejecución de pruebas técnicas, deberá alinearse con lo establecido en el marco metodológico NIST SP 800-115. Asimismo, las actividades deberán estar articuladas con el marco MITRE ATT&CK, incorporando enfoques como Adversary Emulation, Red Teaming y Threat Hunting, orientados a fortalecer la capacidad de detección y respuesta ante amenazas avanzadas. Deberá presentar certificado manifestando que aplica los estándares y buenas prácticas solicitadas en el párrafo anterior. El personal asignado deberá contar con formación profesional en áreas afines a tecnologías de la información y ciberseguridad, así como certificaciones vigentes de reconocimiento internacional, tales como CEH, OSCP, CISA, CISSP o equivalentes. Adicionalmente, deberán acreditar experiencia comprobada en la ejecución de pruebas de seguridad, análisis de vulnerabilidades y gestión de riesgos tecnológicos. Deberá presentar certificado manifestando que cuenta con el equipo para garantizar la prestación del servicio y que cumple con las certificaciones y experiencia requerida. El Proveedor será responsable de garantizar la confidencialidad, integridad y disponibilidad de la información a la que tenga acceso en el desarrollo del contrato, así como del cumplimiento de las políticas de seguridad de la entidad y la normativa vigente aplicable. Deberá presentar certificado manifestando que garantiza lo anterior. -Identificar, analizar y categorizar las vulnerabilidades presentes en los sistemas, plataformas y/o dispositivos objeto del servicio. -Emitir recomendaciones técnicas específicas, priorizadas según criticidad, para la corrección o mitigación de los riesgos identificados. -Entregar lineamientos para la mejora continua del ecosistema de ciberseguridad, fortaleciendo los controles existentes y promoviendo prácticas.	25,00%	\$ 13.950.000
Gestión de Superficie de Ataque	El Proveedor deberá iniciar con el levantamiento, identificación, clasificación y análisis de la Infraestructura tecnológica de la entidad, incluyendo los activos de información, plataformas, servicios, aplicaciones y demás componentes que conforman el ecosistema digital institucional. Este ejercicio deberá permitir la identificación de activos críticos, sus dependencias, niveles de exposición y posibles vectores de ataque, constituyéndose como base para la priorización de actividades de vigilancia, análisis y gestión de riesgos. Con fundamento en lo anterior, el Proveedor deberá implementar un proceso de Gestión de Superficie de Ataque Cibernético, orientado al descubrimiento, inventario, monitoreo y análisis continuo de todos los activos tecnológicos expuestos públicamente por la entidad. Esto incluye, entre otros, dominios y subdominios, direcciones IP públicas, servicios expuestos, certificados digitales y tecnologías web identificadas, con el propósito de minimizar la exposición no intencionada, fortalecer la postura de seguridad y anticipar posibles vectores de ataque mediante la identificación proactiva de riesgos y vulnerabilidades asociadas a dichos activos. De manera complementaria, el Proveedor deberá realizar una evaluación integral del riesgo cibernético institucional, considerando el contexto actual de amenazas, la probabilidad de ocurrencia de incidentes de seguridad y su impacto potencial a nivel operativo, técnico, legal y reputacional. Como resultado, se deberá entregar una valoración objetiva y cuantificable del riesgo, que sirva como insumo para la toma de decisiones estratégicas por parte de la entidad.	20,00%	\$ 11.160.000
Levantamiento y análisis de la Infraestructura tecnológica:	-Realizar el levantamiento, clasificación y documentación de los activos tecnológicos objeto del servicio. -Identificar los componentes críticos, dependencias, puntos vulnerables y niveles de exposición a amenazas externas e internas. -Priorizar los activos auditables para determinar el alcance y nivel de profundidad del análisis, con el fin de dimensionar el universo sujeto a vigilancia y gestión de vulnerabilidades	12,00%	\$ 6.696.000
Evaluación del riesgo cibernético institucional:	-Efectuar un análisis técnico y objetivo del nivel de riesgo al que se encuentra expuesta la entidad, considerando el entorno de amenazas actual, incidente potenciales y el impacto operativo, reputacional, técnico y legal que un ataque podría generar. -Determinar la probabilidad de ocurrencia de un ciberataque y su severidad, con base en amenazas reales identificadas y verificables. -Presentar una valoración cuantificable del riesgo cibernético, permitiendo la toma de decisiones informadas por parte de la entidad.	10,00%	\$ 5.580.000
Otros	Garantizar el cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad (ISO 27001, NIST, MITRE ATT&CK, OWASP, entre otros).	8,00%	\$ 4.464.000
TOTAL		100,00%	\$ 55.800.000

Valor Total (sin IVA): 45.198.000
IVA (si aplica): 10.602.000
Valor Total (con IVA): 55.800.000

Nombre de la empresa: Intrust Security S.A.S.

Firma del Representante Legal:

NIT: 901380504-6

Teléfono: 3012807037

Correo Principal: info@intrustsecurity.co

*Las propuestas presentadas deben ser económicas y técnicas respecto del desarrollo a ejecutar.

Medellín, 06 de mayo de 2026

Señores

VALOR+ S.A.S.

Área de Compras y Contratación

Carrera 42 # 52-28 Piso 3, Edificio Edatel

Medellín, Antioquia

compras2@valormas.gov.co

ASUNTO: Propuesta Económica y Técnica — Convocatoria Abreviada N° 012-2026, objeto: "Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor+ S.A.S. mediante monitorización continua de internet y Darknet"

Respetados señores:

En atención a la Convocatoria Abreviada N° 012-2026 publicada por VALOR+ S.A.S., INTRUST SECURITY SAS, sociedad comercial legalmente constituida bajo las leyes colombianas, identificada con NIT 901380604-6, representada por **Sergio Mauricio Barón Vera**, identificado con cédula de ciudadanía N° 91.286.268 expedida en Bucaramanga, en calidad de Representante Legal, presenta formalmente la propuesta para la prestación de los servicios de **vigilancia tecnológica en ciberseguridad, gestión de vulnerabilidades y gestión de superficie de ataque**, en cumplimiento de las especificaciones técnicas y condiciones establecidas en el citado proceso.

Intrust Security SAS es una empresa especializada en ciberseguridad con presencia en Colombia. Nuestro equipo está conformado por profesionales con certificaciones internacionales vigentes en las áreas de Ethical Hacking, Threat Intelligence, gestión de vulnerabilidades y análisis de superficie de ataque. A lo largo de nuestra trayectoria hemos prestado servicios de seguridad ofensiva y defensiva a organizaciones del sector financiero, de salud, logístico y gubernamental en la región, lo que nos permite comprender con precisión los riesgos a los que se expone la infraestructura tecnológica de entidades como la Gobernación de Antioquia.

Mediante la presentación de esta propuesta, declaramos bajo la gravedad de juramento:

- ✓ Conocemos, aceptamos y nos sometemos en su integridad a las condiciones establecidas en la Convocatoria Abreviada N° 012-2026 y sus respectivos anexos.
- ✓ No estamos incurso en ninguna causal de inhabilidad, incompatibilidad o prohibición para contratar con entidades del sector público colombiano.
- ✓ Nos encontramos a paz y salvo con el sistema de seguridad social integral, aportes parafiscales y obligaciones tributarias.
- ✓ Mantenemos la validez de la presente oferta por treinta (30) días calendario, contados desde la fecha límite de presentación.
- ✓ La información contenida en esta propuesta y en los documentos que la acompañan es veraz, verificable y de nuestra entera responsabilidad.

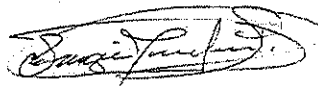
- ✓ En caso de ser favorecidos con la adjudicación, constituiremos las garantías requeridas dentro de los tres (3) días hábiles siguientes a la firma del contrato.
- ✓ Contamos con la capacidad técnica, operativa y de personal especializado para ejecutar los tres ejes del servicio: Vigilancia Tecnológica, Gestión de Vulnerabilidades y Gestión de Superficie de Ataque, aplicando los marcos de referencia exigidos: ISO 27001, NIST CSF, NIST SP 800-115, MITRE ATT&CK, OWASP y CVSS.

VALOR TOTAL DE LA PROPUESTA**\$55.800.000****CINCUENTA Y CINCO MILLONES OCHOCIENTOS MIL PESOS MONEDA LEGAL COLOMBIANA**Valor mensual: **\$6.975.000 COP** | Vigencia: **Hasta el 31 de diciembre de 2026**

Junto con la presente carta se adjunta la documentación que acredita nuestra capacidad jurídica, técnica, financiera y organizacional, conforme a lo solicitado: certificaciones de experiencia, formatos diligenciados y firmados, póliza de seriedad de la oferta con su comprobante de pago, y la propuesta económica en el formato definido por VALOR+ S.A.S.

Quedamos disponibles para atender cualquier requerimiento de aclaración o subsanación dentro del cronograma del proceso, y manifestamos nuestra disposición de asumir el contrato con el nivel de servicio, confidencialidad y rigurosidad técnica que la Gobernación de Antioquia requiere.

Cordialmente,

**Sergio Mauricio Barón Vera**

Representante Legal

INTRUST SECURITY SAS

NIT: 901380604-6

C.C. 91.286.268 — Bucaramanga

info@intrustsecurity.co

INFORMACIÓN DE CONTACTO**Razón social:** Intrust Security SAS **NIT:** 901380604-6 **Representante Legal:** Sergio Mauricio Barón Vera**Dirección:** CR 73 52 34 OF 3091, Medellín, Colombia **Correo:** info@intrustsecurity.co**Operaciones:** Colombia

131

Cámara de Comercio de Medellín para Antioquia
CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha de expedición: 06/05/2026 - 9:03:14 AM



Recibo No.: 0030217762

Valor: \$00

CÓDIGO DE VERIFICACIÓN: dRfoFCekokdbjBjb

Verifique el contenido y confiabilidad de este certificado, ingresando a www.certificadoscamara.com y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario, contados a partir de la fecha de su expedición.

CON FUNDAMENTO EN LA MATRÍCULA E INSCRIPCIONES EFECTUADAS EN EL REGISTRO MERCANTIL, LA CÁMARA DE COMERCIO CERTIFICA:

NOMBRE, IDENTIFICACIÓN Y DOMICILIO

Razón social: INTRUST SECURITY S.A.S. /
Sigla: No reportó
Nit: 901380604-6
Domicilio principal: MEDELLÍN, ANTIOQUIA, COLOMBIA

MATRÍCULA

Matrícula No.: 21-840363-12
Fecha de matrícula: 16 de Abril de 2020.
Último año renovado: 2026 /
Fecha de renovación: 04 de Febrero de 2026 /
Grupo NIIF: GRUPO III.

UBICACIÓN

Dirección del domicilio principal: Carrera 73 No. 52 34 OFICINA
3091-3092
Municipio: MEDELLÍN, ANTIOQUIA, COLOMBIA
Correo electrónico: info@intrustsecurity.co
Teléfono comercial 1: 3012807037
Teléfono comercial 2: 3234942349
Teléfono comercial 3: No reportó
Página web: No reportó

Dirección para notificación judicial: Calle 72 SUR No. 33 59 AP 1801
Municipio: SABANETA, ANTIOQUIA, COLOMBIA
Correo electrónico de notificación: info@intrustsecurity.co
Teléfono para notificación 1: No reportó
Teléfono para notificación 2: No reportó
Teléfono para notificación 3: No reportó

La persona jurídica INTRUST SECURITY S.A.S. SI autorizó para recibir notificaciones personales a través de correo electrónico, de conformidad con lo establecido en los artículos 291 del Código General del Proceso y

Cámara de Comercio de Medellín para Antioquia
CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha de expedición: 06/05/2026 - 9:03:14 AM



Recibo No.: 0030217762

Valor: \$00

CÓDIGO DE VERIFICACIÓN: dRfoFCekokdbjBjb

Verifique el contenido y confiabilidad de este certificado, ingresando a www.certificadoscamara.com y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario, contados a partir de la fecha de su expedición.

67 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo

CONSTITUCIÓN

Por Documento Privado del 13 de abril de 2020 del Accionista, inscrito(a) inicialmente en la Cámara de Comercio del Aburrá Sur el 16 de abril de 2020 y posteriormente, inscrito(a) en esta Cámara de Comercio el 03 de marzo de 2026, con el No. 7592 del Libro IX, se constituyó la Sociedad de naturaleza Comercial denominada INTRUST SECURITY S.A.S.

REFORMAS ESPECIALES

Por Acta No.14 del 20 de febrero de 2026 de la Asamblea de Accionistas, inscrito(a) inicialmente en la Cámara de Comercio del Aburrá Sur el 23 de febrero de 2026 y posteriormente inscrito(a) en esta Cámara de Comercio el 3 de marzo de 2026 con el No.7592 del libro IX, la sociedad cambia su domicilio de Sabaneta al municipio de Medellín.

OBJETO SOCIAL

La sociedad tendrá como objeto principal las siguientes actividades:

- Actividades de consultoría informática y actividades de administración de instalaciones informáticas.
- Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas)
- Otras actividades de tecnologías de información y actividades de servicios informáticos.

Es de anotar que no obstante esta relación, la sociedad podrá realizar cualquier actividad comercial o civil, lícita.

CAPITAL

		CAPITAL AUTORIZADO
Valor	:	\$1.000.000.000,00
No. de acciones	:	1.000.000,00
Valor Nominal	:	\$1.000,00

CAPITAL SUSCRITO

Cámara de Comercio de Medellín para Antioquia
CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha de expedición: 06/05/2026 - 9:03:14 AM



Recibo No.: 0030217762

Valor: \$00

CÓDIGO DE VERIFICACIÓN: drfoFCekokdbjBjb

 Verifique el contenido y confiabilidad de este certificado, ingresando a www.certificadoscamara.com y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario, contados a partir de la fecha de su expedición.

Valor	:	\$21.547.550,00
No. de acciones	:	21.547,55
Valor Nominal	:	\$1.000,00

CAPITAL PAGADO

Valor	:	\$21.547.550,00
No. de acciones	:	21.547,55
Valor Nominal	:	\$1.000,00

REPRESENTACIÓN LEGAL

La sociedad tendrá un Gerente General elegido por la Asamblea de Accionistas para períodos de dos (02) años, contado a partir de la inscripción en la Cámara de Comercio, quien podrá ser reelegido o removido en cualquier tiempo. El Gerente General será reemplazado en sus faltas absolutas, temporales o accidentales o en casos de incompatibilidad o inhabilidad, por un suplente, elegido también por la Asamblea de Accionistas.

REPRESENTACION LEGAL. El Gerente General será el Representante Legal de la sociedad y tendrá a su cargo la inmediata dirección y administración de los negocios sociales con sujeción a las disposiciones legales y estatutarias y a las decisiones de la asamblea general de accionistas. Todos los funcionarios y empleados de la sociedad, con excepción de los nombrados por la asamblea general, estarán subordinados a él y bajo su dirección e inspección inmediata.

FACULTADES Y LIMITACIONES DEL REPRESENTANTE LEGAL

Son funciones del Gerente General:

- 1.-Representar a la sociedad judicial y extrajudicialmente.
- 2.-Designar a los funcionarios o empleados de la compañía, cuyo nombramiento no corresponda a la asamblea de accionistas.
- 3.-Presentar anualmente a la Asamblea de Accionistas, los estados financieros de propósito general de fin de ejercicio que se vayan a someter a consideración de la asamblea, junto con sus notas, el informe de gestión y un proyecto de distribución de utilidades repartibles.
- 4.- Convocar a la asamblea general de accionistas a sesiones ordinarias,

Cámara de Comercio de Medellín para Antioquia
CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha de expedición: 06/05/2026 - 9:03:14 AM



Recibo No.: 0030217762

Valor: \$00

CÓDIGO DE VERIFICACIÓN: dRfoFCekokdbjBjb

Verifique el contenido y confiabilidad de este certificado, ingresando a www.certificadoscamara.com y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario, contados a partir de la fecha de su expedición.

en la oportunidad previsto en los estatutos y a sesiones extraordinarias cuando lo juzgue conveniente o cuando se lo solicite uno o más accionistas, en los términos de estos estatutos.

5.- Celebrar todo acto o contrato correspondiente al giro ordinario del negocio, y constituir prendas, hipotecas o cualquier otro gravamen que afecte los activos de la compañía, o celebrar actos o contratos de disposición de activos fijos o contraer obligaciones a cargo de la sociedad.

6.-Mantener a la Asamblea de Accionistas permanente y detalladamente enterada de la marcha de los negocios sociales y suministrar todos los datos e informes que le solicite.

7.-Otorgar los poderes necesarios para la inmediata defensa de los intereses de la sociedad, debiendo obtener autorización de la Asamblea de Accionistas cuando se trate de poderes generales.

8.-Apremiar a los empleados y funcionarios de la sociedad para que cumplan oportunamente con los deberes de sus cargos y vigilar continuamente la marcha de la empresa social.

9.-Cumplir y hacer cumplir las decisiones de la asamblea general de accionistas.

10.-Ejercer todas las funciones, facultades o atribuciones señaladas en la ley o los estatutos o las que le fije la Asamblea de Accionistas y las demás que le correspondan por la naturaleza de su cargo.

PARAGRAFO: El Gerente General podrá delegar en su suplente aquellas funciones que por ley o los estatutos no le corresponda ejercer de manera privativa. Así mismo, podrá reasumir en cualquier tiempo las funciones que hubiere delegado.

NOMBRAMIENTOS

REPRESENTANTES LEGALES

Por Acta No. 13 del 04 de febrero de 2026 de la Asamblea de Accionistas, inscrito(a) inicialmente en la Cámara de Comercio del Aburrá Sur el 09 de febrero de 2026 y posteriormente, inscrito(a) en esta Cámara de Comercio el 3 de marzo de 2026, con el No. 7592 del Libro IX, se

Cámara de Comercio de Medellín para Antioquia
CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha de expedición: 06/05/2026 - 9:03:14 AM



Recibo No.: 0030217762

Valor: \$00

CÓDIGO DE VERIFICACIÓN: dRfoFCekokdbjBjb

 Verifique el contenido y confiabilidad de este certificado, ingresando a www.certificadoscamara.com y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario, contados a partir de la fecha de su expedición.

designó a:

CARGO	NOMBRE	IDENTIFICACION
GERENTE GENERAL	✓ SERGIO MAURICIO BARON VERA	C.C 91.286.268
SUPLENTE DEL GERENTE GENERAL	SHARON ANDREA QUINTERO NAVAS	C.C 1.083.017.580

REFORMAS DE ESTATUTOS

Los estatutos de la Sociedad han sido reformados así:

DOCUMENTO	INSCRIPCION
Acta No.7 del 19/04/2023 de Asamblea	7592 del 03/03/2026 del L.IX
Acta No.14 del 20/02/2026 de Asamblea	7592 del 03/03/2026 del L.IX

RECURSOS CONTRA LOS ACTOS DE INSCRIPCIÓN

De conformidad con lo establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo y la Ley 962 de 2005, los actos administrativos de registro, quedan en firme dentro de los diez (10) días hábiles siguientes a la fecha de inscripción, siempre que no sean objeto de recursos. Para estos efectos, se informa que para la Cámara de Comercio de Medellín para Antioquia, los sábados NO son días hábiles.

Una vez interpuestos los recursos, los actos administrativos recurridos quedan en efecto suspensivo, hasta tanto los mismos sean resueltos, conforme lo prevé el artículo 79 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

A la fecha y hora de expedición de este certificado, NO se encuentra en curso ningún recurso.

CLASIFICACIÓN DE ACTIVIDADES ECONÓMICAS - CIIU

Actividad principal código CIIU: 6202
 Actividad secundaria código CIIU: 6201
 Otras actividades código CIIU: 6209

Cámara de Comercio de Medellín para Antioquia
CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Fecha de expedición: 06/05/2026 - 9:03:14 AM



Recibo No.: 0030217762

Valor: \$00

CÓDIGO DE VERIFICACIÓN: dRfoFCekokdbjBjb

Verifique el contenido y confiabilidad de este certificado, ingresando a www.certificadoscamara.com y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario, contados a partir de la fecha de su expedición.

TAMAÑO DE EMPRESA

De conformidad con lo previsto en el artículo 2.2.1.13.2.1 del decreto 1074 de 2015 y la Resolución 2225 de 2019 del DANE el tamaño de la empresa es micro.

Lo anterior de acuerdo a la información reportada por el matriculado o inscrito en el formulario RUES:

Ingresos por actividad ordinaria \$604.570.828,00

Actividad económica por la que percibió mayores ingresos en el período - CIIU: 6202

INFORMACIÓN COMPLEMENTARIA

Este certificado refleja la situación jurídica registral de la sociedad, a la fecha y hora de su expedición.

Este certificado cuenta con plena validez jurídica según lo dispuesto en la ley 527 de 1999. En él se incorporan tanto la firma mecánica que es una representación gráfica de la firma del Secretario de la Cámara de Comercio de Medellín para Antioquia, como la firma digital y la respectiva estampa cronológica, las cuales podrá verificar a través de su aplicativo visor de documentos PDF.

Si usted expidió el certificado a través de la plataforma virtual, puede imprimirlo con la certeza de que fue expedido por la Cámara de Comercio de Medellín para Antioquia. La persona o entidad a la que usted le va a entregar el certificado puede verificar su contenido de manera ilimitada, durante 60 días calendario contados a partir del momento de su expedición, ingresando a www.certificadoscamara.com y digitando el código de verificación que se encuentra en el encabezado del presente documento. El certificado a validar corresponde a la imagen y contenido del certificado creado en el momento en que se generó en las taquillas o a través de la plataforma virtual de la Cámara.

.....
.....

Cámara de Comercio de Medellín para Antioquia
CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL



Fecha de expedición: 06/05/2026 - 9:03:14 AM

CAMARA DE COMERCIO
DE MEDELLIN PARA ANTIOQUIA

Recibo No.: 0030217762

Valor: \$00

CÓDIGO DE VERIFICACIÓN: dRfoFCekokdbjBjb

Verifique el contenido y confiabilidad de este certificado, ingresando a www.certificadoscamara.com y digite el respectivo código, para que visualice la imagen generada al momento de su expedición. La verificación se puede realizar de manera ilimitada, durante 60 días calendario, contados a partir de la fecha de su expedición.

SANDRA MILENA MONTES PALACIO
Vicepresidente de Registros

DIAN		Formulario del Registro Único Tributario		001	
2. Concepto 02 Actualización		4. Número de formulario 141239116504			
		 (415)7707212489984(8020) 000014123911650 4			
5. Número de Identificación Tributaria (NIT) 9 0 1 3 8 0 6 0 4		6. DV 6	12. Dirección seccional Impuestos de Medellín		14. Buzón electrónico
IDENTIFICACIÓN					
24. Tipo de contribuyente Persona jurídica		25. Tipo de documento 1		26. Número de identificación	
Lugar de expedición		28. País		29. Departamento	
31. Primer apellido		32. Segundo apellido		33. Primer nombre	
35. Razón social INTRUST SECURITY S.A.S.		36. Nombre comercial		37. Sigla	
UBICACIÓN					
38. País COLOMBIA		39. Departamento Antioquia		40. Ciudad/Municipio Medellín	
41. Dirección principal CR 73 52 34 OF 3091					
42. Correo electrónico info@intrustsecurity.co					
43. Código postal		44. Teléfono 1		45. Teléfono 2	
CLASIFICACIÓN					
Actividad principal		Actividad económica		Ocupación	
46. Código	47. Fecha inicio actividad	48. Código	49. Fecha inicio actividad	50. Código	51. Código
6 2 0 2	2 0 2 0, 0 4, 0 6	6 2 0 1	2 0 2 0, 0 4, 0 6	6 2 0 9	
Responsabilidades, Calidades y Atributos					
53. Código 1 0 1 4 4 2 4 7 4 8 5 2 5 5					
10- Obligado aduanero					
14- Informante de exogena					
42- Obligado a llevar contabilidad					
47- Régimen Simple de Tributación - SIM					
48- Impuesto sobre las ventas - IVA					
52- Facturador electrónico					
55- Informante de Beneficiarios Finales					
Usuarios aduaneros			Exportadores		
54. Código 2 2			55. Forma 1		
			56. Tipo 2		
			Servicio 1		
			57. Modo 2		
			58. CPC 8 3		
IMPORTANTE: Sin perjuicio de las actualizaciones a que haya lugar, la inscripción en el Registro Único Tributario -RUT-, tendrá vigencia indefinida y en consecuencia no se exigirá su renovación.					
Para uso exclusivo de la DIAN					
59. Anexos ☐ SI ☒ NO		60. No. de Folios: 0		61. Fecha 2026-03-04 / 11:37:22AM	
La información suministrada a través del formulario oficial de inscripción, actualización, suspensión y cancelación del Registro Único Tributario (RUT), deberá ser exacta y veraz; en caso de constatar inexactitud en alguno de los datos suministrados se adelantarán los procedimientos administrativos sancionatorios o de suspensión, según el caso. Parágrafo del artículo 1.6.1.2.6 del Decreto 1625 del 2016. De igual manera al formalizar el trámite el usuario fue informado y acepta la política de tratamiento de datos ley 1581 de 2012. Firma del solicitante:			Sin perjuicio de las verificaciones que la DIAN realice. Firma autorizada: 984. Nombre QUINTERO NAVAS SHARON ANDREA 985. Cargo Representante Legal Suplente Certificado		

DIAN

Formulario del Registro Único Tributario

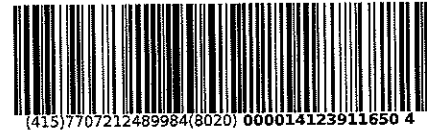
001

Página 2 de 4 Hoja 2

Espacio reservado para la DIAN

4. Número de formulario

141239116504



(415)7707212489984(8020) 000014123911650 4

5. Número de identificación Tributaria (NIT)

9 0 1 3 8 0 6 0 4

6. DV

6

12. Dirección seccional
Impuestos de Medellín

14. Buzón electrónico

Características y formas de las organizaciones

62. Naturaleza

2

63. Formas asociativas

1 2

65. Fondos

66. Cooperativas

68. Sin personería jurídica

69. Otras organizaciones no clasificadas

64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados
67. Sociedades y organismos extranjeros
70. Beneficio

1

Constitución, Registro y Última Reforma

Composición del Capital

Documento	1. Constitución	2. Reforma
71. Clase	0 4	
72. Número		
73. Fecha	2 0 2 0 0 4 1 3	
74. Número de notaría		
75. Entidad de registro	0 3	
76. Fecha de registro	2 0 2 0 0 4 1 6	
77. No. Matricula mercantil	2 2 9 2 4 0	
78. Departamento	0 5	
79. Ciudad/Municipio	0 5 5	
Vigencia		
80. Desde	2 0 2 0 0 4 1 3	
81. Hasta	2 0 9 9 1 2 3 1	

82. Nacional	1 0 0 %
83. Nacional público	0 . 0 %
84. Nacional privado	1 0 0 . 0 %
85. Extranjero	0 %
86. Extranjero público	0 . 0 %
87. Extranjero privado	0 . 0 %

Entidad de vigilancia y control

88. Entidad de vigilancia y control
Superintendencia de Sociedades

5

Estado y Beneficio

Item	89. Estado actual	90. Fecha cambio de estado	91. Número de identificación Tributaria (NIT)	92. DV
1	8 1	2 0 2 0 0 4 1 6		
2	1 2 5	2 0 2 0 0 4 1 6		
3				
4				
5				

Vinculación económica

93. Vinculación económica	94. Nombre del grupo económico y/o empresarial	95. Número de identificación Tributaria (NIT) de la Matriz o Controlante	96. DV.
97. Nombre o razón social de la matriz o controlante			
170. Número de identificación tributaria otorgado en el exterior	171. País	172. Número de identificación tributaria sociedad o natural del exterior con EP	
173. Nombre o razón social de la sociedad o natural del exterior con EP			

DIAN		Formulario del Registro Único Tributario Representación		001	
Espacio reservado para la DIAN			Página 3 de 4 Hoja 3		
			4. Número de formulario 141239116504		
			 (415)7707212489984(8020) 000014123911650 4		
5. Número de Identificación Tributaria (NIT) 9 0 1 3 8 0 6 0 4		6. DV 6	12. Dirección seccional Impuestos de Medellín		14. Buzón electrónico
Representación					
98. Representación REPRS LEGAL PRIN		18		99. Fecha inicio ejercicio representación 2 0 2 6 0 2 0 4	
100. Tipo de documento Cédula de Ciudadan 1 3		101. Número de identificación 9 1 2 8 6 2 6 8		102. DV 103. Número de tarjeta profesional	
104. Primer apellido BARON		105. Segundo apellido VERA		106. Primer nombre SERGIO	
107. Otros nombres MAURICIO		108. Número de Identificación Tributaria (NIT)		109. DV	
110. Razón social representante legal		111. Razón social representante legal		112. Razón social representante legal	
98. Representación REPRS LEGAL SUPL		19		99. Fecha inicio ejercicio representación 2 0 2 6 0 2 0 4	
100. Tipo de documento Cédula de Ciudadan 1 3		101. Número de identificación 1 0 8 3 0 1 7 5 8 0		102. DV 103. Número de tarjeta profesional	
104. Primer apellido QUINTERO		105. Segundo apellido NAVAS		106. Primer nombre SHARON	
107. Otros nombres ANDREA		108. Número de Identificación Tributaria (NIT)		109. DV	
110. Razón social representante legal		111. Razón social representante legal		112. Razón social representante legal	
98. Representación		99. Fecha inicio ejercicio representación		100. Tipo de documento	
101. Número de identificación		102. DV		103. Número de tarjeta profesional	
104. Primer apellido		105. Segundo apellido		106. Primer nombre	
107. Otros nombres		108. Número de Identificación Tributaria (NIT)		109. DV	
110. Razón social representante legal		111. Razón social representante legal		112. Razón social representante legal	
98. Representación		99. Fecha inicio ejercicio representación		100. Tipo de documento	
101. Número de identificación		102. DV		103. Número de tarjeta profesional	
104. Primer apellido		105. Segundo apellido		106. Primer nombre	
107. Otros nombres		108. Número de Identificación Tributaria (NIT)		109. DV	
110. Razón social representante legal		111. Razón social representante legal		112. Razón social representante legal	
98. Representación		99. Fecha inicio ejercicio representación		100. Tipo de documento	
101. Número de identificación		102. DV		103. Número de tarjeta profesional	
104. Primer apellido		105. Segundo apellido		106. Primer nombre	
107. Otros nombres		108. Número de Identificación Tributaria (NIT)		109. DV	
110. Razón social representante legal		111. Razón social representante legal		112. Razón social representante legal	

DIAN

Formulario del Registro Único Tributario
Revisor Fiscal y Contador

001

Página 4 de 4 Hoja 5

Espacio reservado para la DIAN

4. Número de formulario

141239116504



(415)7707212489984(8020) 000014123911650 4

5. Número de Identificación Tributaria (NIT)

6. DV

12. Dirección seccional
Impuestos de Medellín

14. Buzón electrónico

9 0 1 3 8 0 6 0 4 6

Revisor Fiscal y Contador

Revisor fiscal principal	124. Tipo de documento	125. Número de identificación	126. DV	127. Número de tarjeta profesional
	128. Primer apellido	129. Segundo apellido	130. Primer nombre	131. Otros nombres
	132. Número de Identificación Tributaria (NIT)	133. DV	134. Sociedad o firma designada	
	135. Fecha de nombramiento			
Revisor fiscal suplente	136. Tipo de documento	137. Número de identificación	138. DV	139. Número de tarjeta profesional
	140. Primer apellido	141. Segundo apellido	142. Primer nombre	143. Otros nombres
	144. Número de Identificación Tributaria (NIT)	145. DV	146. Sociedad o firma designada	
	147. Fecha de nombramiento			
Contador	148. Tipo de documento	149. Número de identificación	150. DV	151. Número de tarjeta profesional
	Cédula de Ciudadanía 1 3	1 0 3 7 6 3 9 0 6 1		2 6 1 4 1 5 T
	152. Primer apellido	153. Segundo apellido	154. Primer nombre	155. Otros nombres
	CARDONA	PUERTA	MATEO	
156. Número de Identificación Tributaria (NIT)		157. DV	158. Sociedad o firma designada	
159. Fecha de nombramiento				
2 0 2 3 0 2 1 8				

LA CONTRALORÍA DELEGADA PARA RESPONSABILIDAD FISCAL ,
INTERVENCIÓN JUDICIAL Y COBRO COACTIVO

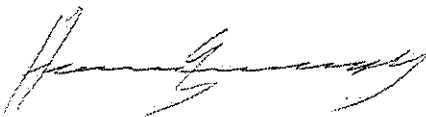
CERTIFICA:

Que una vez consultado el Sistema de Información del Boletín de Responsables Fiscales 'SIBOR', hoy martes 05 de mayo de 2026, a las 22:11:33, el número de identificación de la Persona Jurídica, relacionado a continuación, NO SE ENCUENTRA REPORTADO COMO RESPONSABLE FISCAL.

Tipo Documento	Número de identificación tributario
No. Identificación	9013806046
Código de Verificación	9013806046260505221133

Esta Certificación es válida en todo el Territorio Nacional, siempre y cuando el tipo y número consignados en el respectivo documento de identificación, coincidan con los aquí registrados.

De conformidad con el Decreto 2150 de 1995 y la Resolución 220 del 5 de octubre de 2004, la firma mecánica aquí plasmada tiene plena validez para todos los efectos legales.



HERNÁN GUILLERMO JOJOA SANTACRUZ
Contralor Delegado

LA CONTRALORÍA DELEGADA PARA RESPONSABILIDAD FISCAL ,
INTERVENCIÓN JUDICIAL Y COBRO COACTIVO

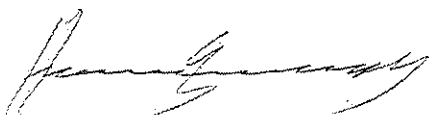
CERTIFICA:

Que una vez consultado el Sistema de Información del Boletín de Responsables Fiscales 'SIBOR', hoy martes 05 de mayo de 2026, a las 22:09:00, el número de identificación, relacionado a continuación, NO SE ENCUENTRA REPORTADO COMO RESPONSABLE FISCAL.

Tipo Documento	Cédula de Ciudadanía
No. Identificación	91286268
Código de Verificación	91286268260505220900

Esta Certificación es válida en todo el Territorio Nacional, siempre y cuando el tipo y número consignados en el respectivo documento de identificación, coincidan con los aquí registrados.

De conformidad con el Decreto 2150 de 1995 y la Resolución 220 del 5 de octubre de 2004, la firma mecánica aquí plasmada tiene plena validez para todos los efectos legales.



HERNÁN GUILLERMO JOJOA SANTACRUZ
Contralor Delegado

205



CERTIFICADO DE ANTECEDENTES

CERTIFICADO ORDINARIO
No. 295649672



LOB
07:28:41
Hoja 1 de 01

Bogotá DC, 11 de mayo del 2026

La PROCURADURIA GENERAL DE LA NACIÓN certifica que una vez consultado el Sistema de Información de Registro de Sanciones e Inhabilidades (SIRI), la persona INTRUST SECURITY S.A.S. identificado(a) con NIT número 9013806046:

NO REGISTRA SANCIONES NI INHABILIDADES VIGENTES

ADVERTENCIA: La certificación de antecedentes contiene las anotaciones de las sanciones o inhabilidades que se encuentren vigentes. Cuando se trate de nombramiento o posesión en cargos que exijan para su desempeño ausencia de antecedentes, se certificarán todas las anotaciones que figuren en el registro. Anterior, de acuerdo a los incisos 3o. y 4o. del artículo 238 Ley 1952 de 2019.

NOTA: El certificado de antecedentes disciplinarios es un documento que contiene las anotaciones e inhabilidades generadas por sanciones penales, disciplinarias, inhabilidades que se deriven de las relaciones contractuales con el estado, de los fallos con responsabilidad fiscal, de las decisiones de pérdida de investidura y de las condenas proferidas contra servidores, ex servidores públicos y particulares que desempeñen funciones públicas en ejercicio de la acción de repetición o llamamiento en garantía. **Este documento tiene efectos para acceder al sector público, en los términos que establezca la Constitución Política y la ley particular o demás disposiciones vigentes.** El Sistema SIRI reporta como antecedentes solamente las sanciones con debida ejecutoria recibidas de las autoridades nacionales colombianas. En caso de nombramiento o suscripción de contratos con el Estado, es responsabilidad de la Entidad, validar la información de antecedentes del aspirante en la página web: <https://www.procuraduria.gov.co/Pages/certificado-antecedentes.aspx>

Olga Lucía Tibocha Cortés
Jefe División de Relacionamento Con El Ciudadano

ATENCIÓN :
ESTE CERTIFICADO CONSTA DE 01 HOJA(S), SOLO ES VALIDO EN SU TOTALIDAD. VERIFIQUE QUE EL NUMERO DEL CERTIFICADO SEA EL MISMO EN TODAS LAS HOJAS.

División de Relacionamento con el Ciudadano.



www.procuraduria.gov.co



Carrera 5 No. 15 - 60 Piso 1; Pbx 5878750
ext. 13170; Bogotá D.C.



Línea gratuita 018000910315

Chrome

Archivo

Edición

Visualización

Historial

Favoritos

Perfiles

Pestañas

Ventana

Ayuda

GOV.CO

PROCURADURÍA GENERAL DE LA NACIÓN COLOMBIA

Inicio

Transparencia y acceso a la información pública

Atención y Servicios a la ciudadanía

Participa

Procuraduría

Sala de Prensa

De Interés

Paz Electoral

Informe de Gestión

Buscar

Editar widgets

Mayo

3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

procuraduria.gov.co/Pages/Generación-de-antecedentes.aspx

Generación de antecedentes

Permite consultar los antecedentes disciplinarios, penales, contractuales, fiscales y de pérdida de investidura con solo digitar el número de identificación de la persona natural o jurídica.

Tipo de identificación:

Nit

Número identificación:

901380604

Tipo de certificado:

☒ Ordinario

☐ Especial

¿Cuanto es 9 - 2 7

7

Generar

EL NÚMERO DE IDENTIFICACIÓN INGRESADO NO SE ENCUENTRA REGISTRADO EN EL SISTEMA.

Señor(a) ciudadano(a): la expedición del certificado de antecedentes disciplinarios de la Procuraduría General de la Nación es gratuita en todo el país.

El certificado de antecedentes ordinario, contiene las anotaciones de las sanciones o inhabilidades que se encuentren vigentes. (Inciso 3, artículo 238 de la ley 1952 de 2019, modificada por la Ley 2094 de 2021)

El certificado de antecedente especial, refleja todas las anotaciones que figuren en la base de datos, y se expide para acreditar requisitos de cuya elección, designación o nombramiento y posesión exige ausencia total o parcial antecedentes.



CERTIFICADO DE ANTECEDENTES
CERTIFICADO ORDINARIO
No. 295383337



PIB
22:15:59
Hoja 1 de 01

Bogotá DC, 05 de mayo del 2026

La PROCURADURIA GENERAL DE LA NACIÓN certifica que una vez consultado el Sistema de Información de Registro de Sanciones e Inhabilidades (SIRI), el(la) señor(a) SERGIO MAURICIO BARON VERA identificado(a) con Cédula de ciudadanía número 91286268:

NO REGISTRA SANCIONES NI INHABILIDADES VIGENTES

ADVERTENCIA: La certificación de antecedentes contiene las anotaciones de las sanciones o inhabilidades que se encuentren vigentes. Cuando se trate de nombramiento o posesión en cargos que exijan para su desempeño ausencia de antecedentes, se certificarán todas las anotaciones que figuren en el registro. Anterior, de acuerdo a los incisos 3o. y 4o. del artículo 238 Ley 1952 de 2019.

NOTA: El certificado de antecedentes disciplinarios es un documento que contiene las anotaciones e inhabilidades generadas por sanciones penales, disciplinarias, inhabilidades que se deriven de las relaciones contractuales con el estado, de los fallos con responsabilidad fiscal, de las decisiones de pérdida de investidura y de las condenas proferidas contra servidores, ex servidores públicos y particulares que desempeñen funciones públicas en ejercicio de la acción de repetición o llamamiento en garantía. **Este documento tiene efectos para acceder al sector público, en los términos que establezca la Constitución Política y la ley particular o demás disposiciones vigentes.** El Sistema SIRI reporta como antecedentes solamente las sanciones con debida ejecutoria recibidas de las autoridades nacionales colombianas. En caso de nombramiento o suscripción de contratos con el Estado, es responsabilidad de la Entidad, validar la información de antecedentes del aspirante en la página web: <https://www.procuraduria.gov.co/Pages/certificado-antecedentes.aspx>

Olga Lucía Tibocho Cortés
Jefe División de Relacionamento Con El Ciudadano

ATENCIÓN :
ESTE CERTIFICADO CONSTA DE 01 HOJA(S), SOLO ES VALIDO EN SU TOTALIDAD. VERIFIQUE QUE EL NUMERO DEL CERTIFICADO SEA EL MISMO EN TODAS LAS HOJAS.



www.procuraduria.gov.co



Carrera 5 No. 15 - 60 Piso 1; Pbx 5878750
ext. 13170; Bogotá D.C.



Línea gratuita 018000910315

Consulta en línea de Antecedentes Penales y Requerimientos Judiciales

La Policía Nacional de Colombia informa:

Que siendo las 08:19:37 AM horas del 06/05/2026, el ciudadano identificado con:

Cédula de Ciudadanía N° 91286268

Apellidos y Nombres: **BARON VERA SERGIO MAURICIO**

NO TIENE ASUNTOS PENDIENTES CON LAS AUTORIDADES JUDICIALES

de conformidad con lo establecido en el artículo 248 de la Constitución Política de Colombia.

En cumplimiento de la Sentencia SU-458 del 21 de junio de 2012, proferida por la Honorable Corte Constitucional, la leyenda "NO TIENE ASUNTOS PENDIENTES CON LAS AUTORIDADES JUDICIALES" aplica para todas aquellas personas que no registran antecedentes y para quienes la autoridad judicial competente haya decretado la extinción de la condena o la prescripción de la pena.

Esta consulta es válida siempre y cuando el número de identificación y nombres, correspondan con el documento de identidad registrado y solo aplica para el territorio colombiano de acuerdo a lo establecido en el ordenamiento constitucional.

Si tiene alguna duda con el resultado, consulte las preguntas frecuentes o acérquese a las instalaciones de la Policía Nacional más cercanas.



Policía Nacional de Colombia

[\(Default.aspx\)](#) 🔍

Portal de Servicios al Ciudadano PSC

Sistema Registro Nacional de Medidas Correctivas RNMC

Consulta Ciudadano

La Policía Nacional de Colombia informa:

Que a la fecha, 06/05/2026 09:04:32 a. m. el ciudadano con Cédula de Ciudadanía N°. **91286268** y Nombre: **SERGIO MAURICIO BARON VERA.**

NO TIENE MEDIDAS CORRECTIVAS PENDIENTES POR CUMPLIR.

De conformidad con la Ley 1801 de 2016 "Por la cual se expide el Código Nacional de Seguridad y Convivencia Ciudadana". Registro interno de validación No. **139609100** . La persona interesada podrá verificar la autenticidad del presente documento a través de la página web institucional digitando <https://www.policia.gov.co>, menú ciudadanos/ consulta medidas correctivas, con el documento de identidad y la fecha de expedición del mismo. Esta consulta es válida siempre y cuando el número de cédula corresponda con el documento de identidad suministrado.

Nueva Búsqueda

Imprimir



Policía Nacional de Colombia
Dirección General - Cra. 59 N° 26 - 21
Centro Administrativo Nacional CAN, Bogotá D.C.
Línea de atención: 018000-910112



CONSULTA EN LÍNEA DE INHABILIDADES DE QUIENES HAYAN SIDO CONDENADOS POR DELITOS SEXUALES COMETIDOS CONTRA MENORES DE 18 AÑOS

La Policía Nacional de Colombia informa:

Que siendo las 09:10:24 horas del 06/05/2026, el ciudadano identificado con cédula de ciudadanía No. 91286268, Apellidos y Nombres **BARON VERA SERGIO MAURICIO**

NO REGISTRA INHABILIDAD

La presente consulta se tendrá en consideración por la entidad o empresa **Valor + S.A.S.**, con NIT **900969726-2** y su utilización es exclusivamente dentro del proceso de selección al cargo, oficio o profesión, en cumplimiento de la Ley 1918 del 12/07/2018 *"por medio de la cual se establece el régimen de inhabilidades a quienes hayan sido condenados por delitos sexuales cometidos contra menores, se crea el registro de inhabilidades y se dictan otras disposiciones"* y su Decreto Reglamentario 753 del 30/04/2019 *"por medio del cual se reglamenta la Ley 1918 de 2018"*, con observancia de las Leyes 1581 del 17/10/2012, 1712 del 06/03/2014 y demás normatividad rectora frente al tratamiento de datos.

<https://inhabilidades.policia.gov.co:8080/consulta>



MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - MINTIC

CERTIFICA QUE

Una vez consultada la base de datos de deudores alimentarios morosos REDAM, el(la) ciudadano(a) con número de identificación CC 91286268 **NO SE ENCUENTRA INSCRITO EN EL REGISTRO DE DEUDORES ALIMENTARIOS MOROSOS**

Esta certificación es válida en todo el Territorio Nacional, siempre y cuando el tipo y número consignados en el respectivo documento de identificación, coincidan con los aquí registrados.

Se expide en Bogotá el 05/05/2026 10:01 PM



Código Verificación: RYWCN7L681

Válida hasta: 04/08/2026

Dirección de Gobierno Digital

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS
COMUNICACIONES - MINTIC



Versionamiento Formato
Código: FO13-DE-GDCO
Versión: 1.0
Fecha actualización: 24/01/2020

INHABILIDADES E INCOMPATIBILIDADES

El suscrito en su calidad de persona natural o jurídica, declara bajo la gravedad de juramento que:

Conozco las causales de inhabilidad e incompatibilidad para contratar con las Entidades Estatales de conformidad con las Leyes: 80 de 1993, 1150 de 2007, 1474 de 2011 y demás normas sobre la materia; así como las sanciones establecidas por transgresión a las mismas en los artículos 26 numeral 7o. y 52 y los efectos legales consagrados en el Art. 44 numeral. 1o. del Estatuto Contractual. **(sólo aplica en caso obrar como representante legal de una persona jurídica)** Como Representante Legal de la Sociedad, declaro bajo la gravedad del juramento que se entiende prestado con la firma del presente documento, que ni la Sociedad que Represento, ni los socios de ella, ni a nombre propio nos encontramos incurso en ninguna de ellas.

Sin perjuicio de lo anterior sírvase dar respuesta a las siguientes preguntas **(aplica para los representantes legales de una persona jurídica y para las personas naturales)**:

DECLARO BAJO MI RESPONSABILIDAD	SI	NO
¿Ha participado en licitaciones, concursos o ha celebrado contratos con el Estado estando incurso en alguna inhabilidad?		X
¿Ha sido sancionado con la declaratoria de caducidad?		X
¿Ha sido sancionado mediante sentencia judicial a la pena de interdicción de derechos y funciones públicas o ha sido sancionado con la destitución?		X
¿Ostenta la calidad de servidor público?		X
¿Su cónyuge o compañero permanente o cualquier otra persona que se encuentre dentro de su segundo grado de consanguinidad o afinidad, ha presentado propuesta para el presente proceso?		X
¿Usted o cualquiera de los socios de la sociedad a la cual representa, tienen una relación por parentesco en segundo grado de consanguinidad o segundo de afinidad con el representante legal o con cualquiera de los socios de una sociedad que formalmente haya presentado propuesta para el presente proceso? (Sólo aplica para los representantes legales de sociedad distintas a las anónimas abiertas)		X
¿Es socio de alguna sociedad de personas a la cual le hayan declarado la caducidad?		X
¿Ha sido declarado judicialmente responsable por la comisión de un delito, en contra de la Administración Pública o de cualquiera de los delitos y faltas que contempla la Ley 1474 de 2011, las demás normas que la modifican y reglamentan o de cualquiera de las conductas delictivas contempladas por las convenciones o tratados de lucha contra la corrupción ratificados por Colombia?		X
¿La sociedad a la cual representa ha sido declarada responsable administrativamente por la conducta de soborno transnacional?		X
¿Ha financiado campañas de candidatos del nivel departamental, efectivamente elegidos, por montos superiores al 2% de las sumas máximas a invertir?		X
¿Los socios sociedad a la cual representa, los miembros de junta directiva han financiado directamente o por interpuesta persona campañas de candidatos del nivel departamental, efectivamente elegidos, por montos superiores al 2% de las sumas máximas a invertir?		X
¿Tiene algún vínculo de parentesco, hasta del segundo grado de consanguinidad, segundo de afinidad o primero civil, con algún servidor público de Valor + S.A.S del nivel directivo, asesor, o con las personas que ejerzan el control interno o con algún miembro de su junta directiva?		X
¿Su cónyuge o compañero permanente es servidor público de Valor + S.A.S del nivel directivo, asesor, o ejerce el control interno, o es miembro de su junta directiva?		X

**Versionamiento Formato**

Código: FO13-DE-GDCO
Versión: 1.0
Fecha actualización: 24/01/2020

¿En los últimos dos años, ejerció cargos del nivel directivo en entidades del Estado o en sociedades en las cuales haya estado vinculado bajo cualquier título, que prestaran sus servicios en un sector relacionado con el objeto de la presente contratación?		X
¿Tiene algún vínculo de parentesco en el primer grado de consanguinidad, primero de afinidad, o primero civil, con alguna persona que, en los últimos dos años, ejerció cargos del nivel directivo en entidades del Estado o en sociedades en las cuales haya estado vinculado bajo cualquier título, que prestaran sus servicios en un sector relacionado con el objeto de la presente contratación?		X

De igual manera, autorizo expresamente a **VALOR + S.A.S.**, para que consulte los listados, sistemas de información y bases de datos a los que haya lugar y de encontrar algún reporte, autorizo a **VALOR + S.A.S.** para que proceda a adelantar las acciones contractuales y/o legales que correspondan.

Con la firma del presente documento, me obligo a realizar todas las actividades encaminadas a asegurar que todos los socios, administradores, clientes, proveedores, empleados, etc. y los recursos de éstos, no se encuentren relacionados o provengan, de actividades ilícitas (**sólo aplica en caso de obrar como representante legal de una persona jurídica**).

Adicionalmente manifiesto que ni la Sociedad, ni los socios, ni mi persona a la firma del presente documento hemos sido sancionados por cuestiones penales, fiscales y/o disciplinarias (**sólo aplica en caso de obrar como representante legal de una persona jurídica**).

Dado en el Municipio de Medellín, a los (06) seis días del mes de mayo de 2026

Nombre completo y firma
CC. 91286268 de Bucaramanga
Representante Legal
Empresa Intrust Security S.A.S.
NIT 901380604-6

AUTORIZACIÓN TRATAMIENTO DE DATOS PERSONALES

Con la firma de este documento manifiesto que he sido informado por **VALOR + S.A.S** de que:

1. **VALOR + S.A.S.** actuará en calidad de responsable del tratamiento de los datos personales de los cuales soy titular y que, podrá recolectar, usar y tratar mis datos personales conforme la Política de Tratamiento de Datos Personales de la empresa que se encuentra disponible en la página de la superintendencia de industria y comercio www.sic.gov.co y en la página www.valormas.gov.co.
2. Los datos personales que serán recolectados por **VALOR + S.A.S** son entre otros y sin limitarse a ellos (nombre, cedula, dirección de residencia, teléfono residencia, número de teléfono celular, huella digital, profesión, empresa donde labora, información financiera). El tratamiento de dichos datos personales obedecerá a las finalidades relacionadas al cumplimiento del objeto social de la empresa, entre ellas:
 - a. Facilitar la prestación, comercialización y consultoría de soluciones integrales para la administración y gestión de la información, recursos y comunicaciones.
 - b. Realizar encuestas relacionadas con los servicios o bienes.
 - c. Ofrecer y promocionar programas, actividades, noticias y servicios.
 - d. Desarrollo de programas de fidelización.
 - e. Conocer las necesidades y preferencias del cliente, para ofrecer mejores servicios.
 - f. Contactar a través del teléfono, correo electrónico y correo físico.
 - g. Lanzamiento de campañas publicitarias por correo electrónico, Marketing Digital, redes sociales, correo directo o telemarketing propias de la empresa.
 - h. Adelantar campañas de actualización de datos.
 - i. Envío de las modificaciones a la Política, así como la solicitud de nuevas autorizaciones para el Tratamiento de los datos.
 - j. Entre otras disposiciones contenidas en la Política de Tratamiento de Datos Personales.
 - k. Y en general todo lo que sea necesario para el desarrollo del objeto social de la empresa, respetando siempre los límites de la Constitución y la ley.
3. Los derechos como titular de datos personales son los previstos en la Constitución y la ley, entre ellos: el derecho a conocer, actualizar, rectificar y suprimir mi información personal, así como el derecho a revocar el consentimiento otorgado para el tratamiento de datos personales, en igual sentido se informa que es de carácter facultativo responder preguntas y otorgar información que versen sobre datos sensibles.
4. Los derechos pueden ser ejercidos a través de los canales de comunicación dispuestos por la empresa como: correo electrónico recepcion@valormas.gov.co o dirigiéndose personalmente a la dirección: Carrera 42 # 52-28 piso 3, Avenida Camellón de la Alpujarra – Edificio Edatel, Medellín.

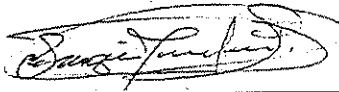
Antioquia y, observando la Política de Tratamiento de Datos Personales de la empresa, las cuales pueden ser revisadas en la página de la superintendencia de industria y comercio www.sic.gov.co y en la página www.valormas.gov.co.

5. Para cualquier inquietud o información adicional relacionada con el tratamiento de datos personales, puedo contactarme al correo electrónico antes mencionado.
6. La empresa garantiza la confidencialidad, libertad, seguridad, veracidad, transparencia, acceso y circulación restringida de mis datos y se reservan el derecho de modificar su Política de Tratamiento de Datos Personales en cualquier momento. Cualquier cambio me será informado previamente a la implementación de las nuevas políticas.

Teniendo en cuenta lo anterior, autorizo de manera voluntaria, previa, explícita, informada e inequívoca a **VALOR + S.A.S** para tratar mis datos personales de acuerdo con la Política de Tratamiento de Datos Personales de la empresa, conforme a los fines relacionados con su objeto social y para fines legales, contractuales, comerciales especificados en la Política de Tratamiento de Datos Personales. La información dada para el tratamiento de mis datos personales la he suministrado de forma voluntaria y es verídica.

Se firma en Medellín, a los (06) seis días del mes de mayo de 2026.

Firma: _____



Nombre: Sergio Mauricio Barón Vera

Nº de Identificación: 91286268 de Bucaramanga

CERTIFICACIÓN DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO

Este documento tiene como propósito certificar a **VALOR + S.A.S.**, que **XXXXXXX** y cada uno de sus integrantes (cuando se trate de Proponente Conjunto), cuenta con un SISTEMA DE PREVENCIÓN Y CONTROL DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO, el cual cumple a cabalidad con las normas colombianas que le son aplicables.

Así las cosas, Yo, Sergio Mauricio Barón Vera, en mi calidad de representante legal de Intrust Security S.A.S. CERTIFICO que:

1. **Intrust Security S.A.S.** da cumplimiento a las normas y regulaciones colombianas relacionadas con la prevención y control al lavado de activos y financiamiento del terrorismo que le son aplicables.

Si X No _____

2. **Intrust Security S.A.S.** cuenta con adecuadas políticas, manuales y procedimientos de prevención y control al lavado de activos y administración del terrorismo, que dan cabal cumplimiento a las regulaciones vigentes que le son aplicables.

Si X No _____

3. ¿Ha estado involucrado **Intrust Security S.A.S.** (y/o alguno de sus integrantes, accionistas, empleados y/o colaboradores) en investigaciones por violación a las leyes relacionadas con el Lavado de Activos y Financiación de Terrorismo?

Si _____ No X

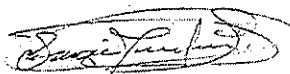
4. ¿Ha sido sancionado **Intrust Security S.A.S.** (y/o alguno de sus integrantes, accionistas, empleados y/o colaboradores) o alguno de sus empleados o directivos por violación de las leyes relacionadas con el Lavado de Activos y Financiación de Terrorismo?

Si _____ No X

Manifiesto que autorizo a VALOR+ SAS para que, directamente o por intermedio de las personas que designe, verifique y confirme la información acá suministrada, incluyendo la efectiva aplicación del SISTEMA DE PREVENCIÓN Y CONTROL DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO por parte nuestra.

Fecha: 06/05/2026

FIRMA



Nombre: Sergio Mauricio Barón Vera Teléfono: 3012807037

Dirección: Carrera 8 # 46 – 34 Apto 402

VALOR+ S.A.S – NIT. 900969726-2

Dirección: Carrera 42 # 52-28 piso 3 Avenida Camellón de la Alpujarra – Edificio Edatel

Teléfono: 444-37-47 Ext. 203

Email: recepcion@valormas.gov.co



SEGUROS
DEL
ESTADO S.A.
NIT. 850.009.575-6

PÓLIZA DE SEGURO DE CUMPLIMIENTO PARTICULAR
CUMPLIMIENTO ANTE ENTIDADES PÚBLICAS CON RÉGIMEN PRIVADO DE CONTRATACIÓN

CIUDAD DE EXPEDICIÓN: IBAGUE			SUCURSAL: IBAGUE			COD. SUCURSAL: 25			NO. PÓLIZA: 25-47-101009198			ANEXO: 0		
FECHA EXPEDICIÓN: DÍA: 06 MES: 05 AÑO: 2026			VIGENCIA DESDE: DÍA: 06 MES: 05 AÑO: 2026			A LAS: HORAS: 00:00			VIGENCIA HASTA: DÍA: 20 MES: 08 AÑO: 2026			A LAS: HORAS: 23:59		
TIPO MOVIMIENTO: EMISIÓN ORIGINAL														

DATOS DEL TOMADOR / GARANTIZADO					
NOMBRE O RAZÓN SOCIAL: INTRUST SECURITY S.A.S.					
DIRECCIÓN: CL 72 SUR NRO. 33 - 59					
CIUDAD: MEDELLIN - ANTIOQUIA					
IDENTIFICACIÓN: NIT. :901.380.604-6					
TELÉFONO: 3173445232					

DATOS DEL ASEGURADO / BENEFICIARIO					
ASEGURADO/ BENEFICIARIO: VALOR + S. A. S.					
DIRECCIÓN: CALLE 41 NO. 52-28 PISO 3 EDIF					
CIUDAD: MEDELLIN - ANTIOQUIA					
IDENTIFICACIÓN: NIT. :900.969.726-2					
TELÉFONO: 6044443747					
ADICIONAL:					

OBJETO DEL SEGURO					
CON SUJECCIÓN A LAS CONDICIONES GENERALES DE LA PÓLIZA QUE SE ANEXAN E-CU-028A, QUE FORMAN PARTE INTEGRANTE DE LA MISMA Y QUE EL ASEGURADO Y EL TOMADOR DECLARAN HABER RECIBIDO Y HASTA EL LÍMITE DE VALOR ASEGURADO SEÑALADO EN CADA AMPARO, SEGUROS DEL ESTADO S.A., GARANTIZA:					
GARANTIZAR LA SERIEDAD DE LA OFERTA PARA EL PROCESO DE SELECCION NO. CONVOCATORIA ABREVIADA N 012-2026 CUYO OBJETO ES: PRESTACIÓN DE SERVICIOS DE VIGILANCIA TECNOLÓGICA EN CIBERSEGURIDAD PARA PROTEGER A LOS DIFERENTES PROYECTOS DE VALOR + S.A.S MEDIANTE MONITORIZACIÓN CONTINUA DE INTERNET Y DARKNET.					

RIESGO: PRESTACION DE SERVICIOS			
AMPAROS:			
SERIEDAD DE LA OFERTA		VIGENCIA DESDE: 06/05/2026	VIGENCIA HASTA: 20/08/2026
		SUMA ASEG/ACTUAL: \$ 5,721,520.00	
ACLARACIONES:			
ACLARACIONES ASEGURADO VALOR+ y el Departamento de Antioquia - Secretaría de Infraestructura Física.			

VALOR PRIMA NETA:	GASTOS EXPEDICIÓN:	IVA:	TOTAL A PAGAR:	VALOR ASEGURADO TOTAL:	PLAN DE PAGO:
\$ 15,000.00	\$ 8,000.00	\$ 4,370.00	\$ 27,370.00	\$ 5,721,520.00	CONTADO

INTERMEDIARIO			DISTRIBUCIÓN COASEGURO		
NOMBRE:	CLAVE:	% DE PART	NOMBRE COMPAÑÍA:	% PART	VALOR ASEGURADO:
NIDIA CECILIA LAMPREA DE GIRALDO	71524	100,00			

QUEDA EXPRESAMENTE CONVENIDO QUE LAS OBLIGACIONES DE SEGUROS DEL ESTADO S.A. SE REFIERE ÚNICAMENTE AL OBJETO Y OBSERVACIONES DE LA(S) GARANTÍA(S) QUE SE ESPECIFICAN EN ESTE CUADRO

PARA EFECTO DE NOTIFICACIONES LA DIRECCIÓN DE SEGUROS DEL ESTADO S.A. ES CARRERA 4C NO. 33 - 08 - TELÉFONO: 2701040 - IBAGUE



25-47-101009198

FIRMA TOMADOR

FIRMA AUTORIZADA: Jose Luis Ojeda Acevedo - Vicepresidente de Fianzas

USTED PUEDE CONSULTAR ESTA PÓLIZA EN WWW.SEGUROSDELESTADO.COM

Oficina Principal: Autopista Norte # 103 - 60, Piso 5 Bogotá D.C. Teléfono: 601-2186977, 601-6019330

28780313

NO EFECTUAR RETENCIÓN EN LA FUENTE POR NINGUN CONCEPTO * RESPONSABLE IVA

SUPERINTENDENCIA FINANCIERA
DE COLOMBIA

VIGILADO

**CONDICIONES GENERALES DE LA PÓLIZA DE CUMPLIMIENTO ANTE ENTIDADES PÚBLICAS CON RÉGIMEN
PRIVADO DE CONTRATACIÓN NO.25-47-101009198**

SEGUROS DEL ESTADO S.A., EN ADELANTE DENOMINADA LA ASEGURADORA, EXPIDE EL PRESENTE CONTRATO DE SEGURO, SUJETO A ESTAS CONDICIONES GENERALES, LAS CUALES ESTÁN DEBIDAMENTE DEPOSITADAS EN LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA Y A LAS CONDICIONES PARTICULARES QUE SE DELIMITAN EN SU ALCANCE Y VIGENCIA SEGÚN LOS AMPAROS OTORGADOS EN FORMA EXPRESA EN LA CARÁTULA DEL SEGURO, CONFORME A LO NORMADO EN EL ARTÍCULO 1047 DEL CÓDIGO DE COMERCIO.

1. AMPAROS

1.1. SERIEDAD DE LOS OFRECIMIENTOS

LA ASEGURADORA CUBRE A LA ENTIDAD DE LAS SANCIONES IMPUTABLES AL PROponente DE LAS OBLIGACIONES ESTABLECIDAS EN EL PLIEGO DE CONDICIONES, LOS TÉRMINOS DE REFERENCIA, EL ESTUDIO PREVIO Y/ O LAS REGLAS DE PARTICIPACIÓN, EN LOS SIGUIENTES EVENTOS: (I) LA NO SUSCRIPCIÓN DEL CONTRATO SIN JUSTA CAUSA POR PARTE DEL PROponente SELECCIONADO. (II) LA NO AMPLIACIÓN DE LA VIGENCIA DE LA GARANTÍA DE SERIEDAD DE LA OFERTA CUANDO EL TÉRMINO PREVISTO EN EL PLIEGO DE CONDICIONES, LOS TÉRMINOS DE REFERENCIA, EL ESTUDIO PREVIO Y/ O LAS REGLAS DE PARTICIPACIÓN, SE PRORROGUE O CUANDO EL TÉRMINO PREVISTO PARA LA SUSCRIPCIÓN DEL CONTRATO SE PRORROGUE, SIEMPRE Y CUANDO ESAS PRÓRROGAS NO EXCEDAN UN TÉRMINO DE TRES (3) MESES. (III) EL RETIRO DE LA OFERTA DESPUÉS DE VENCIDO EL TÉRMINO FIJADO PARA LA PRESENTACIÓN DE LAS PROPUESTAS. IV) LA FALTA DE OTORGAMIENTO POR PARTE DEL PROponente SELECCIONADO DE LA GARANTÍA DE CUMPLIMIENTO EXIGIDA POR LA ENTIDAD PARA AMPARAR EL INCUMPLIMIENTO DE LAS OBLIGACIONES DEL CONTRATO.

1.2. ANTICIPOS

CUBRE CONTRA LOS PERJUICIOS IMPUTABLES AL CONTRATISTA DERIVADOS DE LA NO INVERSIÓN, USO INDEBIDO, APROPIACIÓN INDEBIDA DE LAS SUMAS EN DINERO O ESPECIE QUE SEAN ENTREGADAS EN CALIDAD DE ANTICIPO. SE ENTIENDE QUE ELLO HA OCURRIDO CUANDO LOS BIENES O DINERO NO SE HAN APLICADO O UTILIZADO EN EL DESARROLLO DEL CONTRATO O EN LAS OBLIGACIONES A CARGO DEL CONTRATISTA. CUANDO SE TRATE DE BIENES ENTREGADOS EN CALIDAD DE ANTICIPO, ÉSTOS DEBERÁN TASARSE EN DINERO PREVIAMENTE EN EL CONTRATO.

1.3. PAGO ANTICIPADO

CUBRE CONTRA LOS PERJUICIOS IMPUTABLES AL CONTRATISTA DERIVADOS DEL NO REINTEGRO DE LAS SUMAS EN DINERO O ESPECIE QUE SEAN ENTREGADAS EN CALIDAD DE PAGO ANTICIPADO Y QUE EL CONTRATISTA NO DEVUELVA A LA ENTIDAD.

EN CASO DE CUMPLIMIENTO PARCIAL DE LAS OBLIGACIONES, SE ESTIMARÁ LA PROPORCIÓN DE LA PARTE CUMPLIDA DEL CONTRATO, PARA DESCONTARLA DE LA INDEMNIZACIÓN.

1.4. CUMPLIMIENTO DE LAS OBLIGACIONES

CUBRE LOS PERJUICIOS DIRECTOS IMPUTABLES AL CONTRATISTA, DERIVADOS DEL INCUMPLIMIENTO DE LAS OBLIGACIONES ADQUIRIDAS POR EL CONTRATISTA CON LA SUSCRIPCIÓN DEL CONTRATO, Y CONTEMPLA TAMBIÉN EL CUMPLIMIENTO TARDÍO, DEFECTUOSO O IMPERFECTO DE LAS MISMAS, ASÍ COMO MULTAS Y CLAUSULA PENAL, SEGÚN SE PACTEN EN EL CONTRATO.

1.5. CALIDAD DE ELEMENTOS, BIENES Y EQUIPOS QUE ENTREGUE EL CONTRATISTA

CUBRE LOS PERJUICIOS IMPUTABLES AL CONTRATISTA CAUSADOS POR LA MALA CALIDAD, LA CALIDAD DEFICIENTE O DESEMPEÑO DEFECTUOSO DE LOS ELEMENTOS, BIENES Y EQUIPOS SUMINISTRADOS POR EL CONTRATISTA, FRENTE A LAS ESPECIFICACIONES CONTENIDAS EN LA LEY 1480 DE 2011 Y LAS NORMAS QUE LA MODIFIQUEN, Y AQUELLAS ADICIONALES PROPIAS DEL BIEN, EQUIPO Y ELEMENTO, ASÍ COMO AQUELLAS QUE SE PACTEN EN EL CONTRATO.

1.6. CALIDAD DE SERVICIOS

CUBRE LOS PERJUICIOS IMPUTABLES AL CONTRATISTA CAUSADOS POR LA MALA CALIDAD, LA CALIDAD DEFICIENTE O DESEMPEÑO DEFECTUOSO, FRENTE A LAS ESPECIFICACIONES QUE SE PACTEN EN EL CONTRATO, TODOS ELLOS SIEMPRE QUE SEAN EXIGIBLES EN LA ETAPA POST-CONTRACTUAL, UNA VEZ FINALICE EL PLAZO DE EJECUCIÓN.

1.7. PROVISIÓN DE REPUESTOS

CUBRE LOS PERJUICIOS IMPUTABLES AL CONTRATISTA CAUSADOS POR EL INCUMPLIMIENTO POR NO SUMINISTRAR LOS REPUESTOS, PARTES, MATERIALES E INSUMOS NECESARIOS PARA LA REPARACIÓN Y MANTENIMIENTO DE BIENES SUMINISTRADOS POR EL CONTRATISTA, FRENTE A LAS ESPECIFICACIONES QUE SE PACTEN EN EL CONTRATO O PREVISTAS EN LA LEY EN LA ETAPA POSTCONTRACTUAL.

1.8. PAGO DE SALARIOS Y PRESTACIONES SOCIALES

CUBRE A LA ENTIDAD EN SU CALIDAD DE CONTRATANTE, CONTRA LOS PERJUICIOS IMPUTABLES AL CONTRATISTA DERIVADOS DEL INCUMPLIMIENTO DE LAS OBLIGACIONES A CARGO DEL CONTRATISTA, DERIVADAS DE CONTRATOS LABORALES A QUE ESTÁ OBLIGADO, EN SU CALIDAD DE EMPLEADOR, INCLUIDAS LAS DE PAGO DE SALARIOS Y PRESTACIONES SOCIALES LEGALES, LIQUIDACIÓN DE CONTRATOS DE ACUERDO CON LAS OBLIGACIONES DE LEY ASUMIDAS POR EL EMPLEADOR Y QUE GUARDAN RELACIÓN DIRECTA CON EL PERSONAL UTILIZADO EN LA EJECUCIÓN DEL CONTRATO EN EL TERRITORIO NACIONAL.

1.9. ESTABILIDAD Y CALIDAD DE LA OBRA

EL AMPARO DE ESTABILIDAD Y CALIDAD DE LA OBRA, CUBRIRÁ A LA ENTIDAD EN CALIDAD DE CONTRATANTE, CON MOTIVO DE LOS PERJUICIOS QUE SE LE OCASIONEN COMO CONSECUENCIA DE CUALQUIER TIPO DE DAÑO O DETERIORO, INDEPENDIENTEMENTE DE SU CAUSA, SUFRIDOS POR LA OBRA ENTREGADA, IMPUTABLES AL CONTRATISTA GARANTIZADO.

1.10. OTROS AMPAROS

LA PRESENTE PÓLIZA TAMBIÉN CUBRE A LA ENTIDAD EN SU CALIDAD DE CONTRATANTE, POR LOS AMPAROS ADICIONALES QUE SE DETERMINEN Y DEFINAN ESPECÍFICAMENTE EN EL CONTRATO Y QUE SE ANOTAN EXPRESAMENTE EN LA CARÁTULA O EN ANEXOS QUE SE EXPIDAN EN AMPLIACIÓN A LA PRESENTE PÓLIZA.

2. EXCLUSIONES

2.1. CAUSA EXTRAÑA

CAUSA EXTRAÑA, ESTO ES LA FUERZA MAYOR O CASO FORTUITO, EL HECHO DE UN TERCERO O LA CULPA EXCLUSIVA DE LA VÍCTIMA.

2.2. MODIFICACIONES NO INFORMADAS

EN CASO DE PACTARSE O IMPONERSE CONDICIONES, CAMBIAR LOS TÉRMINOS DEL CONTRATO Y NO REPORTARLO DEBIDAMENTE AL ASEGURADOR, Y QUE NO SEAN ACEPTADAS EXPRESAMENTE POR ÉL, ÉSTE QUEDARÁ RELEVADO DEL PAGO DE LA PRESTACIÓN ASEGURADA, DERIVADA DE TALES CAMBIOS, PACTOS O MODIFICACIONES.

2.3. RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL

ESTE SEGURO NO CUBRE LOS PERJUICIOS DERIVADOS DE LOS RECLAMOS DE TERCEROS AJENOS AL CONTRATO, CON OCASIÓN DE EVENTUALES RESPONSABILIDADES DE CARÁCTER CIVIL EXTRA CONTRACTUAL. TAMPOCO SE CUBRE LA RESPONSABILIDAD CIVIL DE CARÁCTER PATRONAL, DERIVADA DE ACCIDENTE DE TRABAJO.

2.4. VICIOS POR TRANSCURSO DEL TIEMPO

LOS PERJUICIOS DERIVADOS DEL SIMPLE TRANSCURSO DEL TIEMPO SOBRE BIENES Y OBJETOS.

2.5. USO INDEBIDO

EL USO INDEBIDO O INADECUADO O LA FALTA DE MANTENIMIENTO PREVENTIVO A QUE ESTÉ OBLIGADA LA ENTIDAD CONTRATANTE.

3. TÉRMINO DEL AMPARO

LA VIGENCIA DE LOS AMPAROS SE REGISTRA EN LA CARÁTULA DE LA PÓLIZA. CUANDO EL CONTRATISTA O LA ENTIDAD REQUIERAN AL ASEGURADOR PARA AMPLIAR LA VIGENCIA DE LA GARANTÍA, EL ASEGURADOR PODRÁ HACERLO, MEDIANTE ANEXO A LA PÓLIZA, LAS VIGENCIAS PODRÁN SER MODIFICADAS DE COMÚN ACUERDO CON EL ASEGURADOR.


Versionamiento Formato

Código: FO11-DE-GCON
 Versión: 1.0
 Fecha actualización: 24/01/2020

APROBACIÓN DE GARANTÍAS

A los siete (07) días del mes de mayo del año dos mil veintiséis (2026), se procede a revisar y aprobar el anexo N° 0 de la Póliza N° 25-47-101009198, expedida por la compañía SEGUROS DEL ESTADO S.A., identificada con NIT.860.009.578-6, a favor de VALOR+ S.A.S., identificada con NIT.900.969.726-2, para garantizar LA SERIEDAD DE LA PROPUESTA DE LA INVITACIÓN N° 012-2026, cuyo objeto es: *"Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."*, cuyo tomador es la empresa INTRUST SECURITY S.A.S. identificada con NIT.901.380.604.

PÓLIZA / AMPAROS	VALOR ASEGURADO	VIGENCIA					
		DESDE			HASTA		
		DÍA	MES	AÑO	DÍA	MES	AÑO
SERIEDAD DE LA OFERTA	\$5.721.520	06	05	2026	20	08	2026

PAULA CRISTINA PARRA CARMONA
 Profesional Especializado

Sucursal Virtual Negocios

Pago PSE

6 May 2026 15:01

NIT 901380604

Usuario: ELVY JOHANNY CHACON NAVAS



Pago exitoso

CUS 286834782

Comercio
SEGUROS DEL ESTADO S.A.

Referencia 1
1743227230

Fecha
6 May 2026 15:01

Referencia 2
NIT

Número de factura
1743227230

Referencia 3
8600095786

Descripción del pago
Internet

Valor del Pago
\$27.370

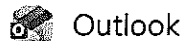
Número de comprobante
TR260506150118En1n4p

Costo de la transacción
\$ 0

Producto origen
Producto
****** 0701**

7/5/26, 14:24

Bandeja de entrada: Paula Cristina Parra Carmona - Outlook



Outlook

Evaluación de propuestas - Convocatoria Abreviada N°012

Desde Compras Valor + 2 <compras2@valormas.gov.co>

Fecha Jue 07/05/2026 14:16

Para Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

 1 archivo adjunto (63 KB)

FO25-DE-GCYN_Evaluación de propuestas (Abreviada_Pública)_v1.0.xlsx;

Cordial saludo,

Adjunto el documento de evaluación de propuestas correspondiente a la Convocatoria Abreviada N.º 012, con el fin de que puedan diligenciarlo y posteriormente se pueda consolidar la información.

Gracias.

Cordialmente;



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alajuela,

Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

INFORME DE RESPUESTA TÉCNICA A DOCUMENTACIÓN
PRESENTADA POR EL PROPONENTE
INTRUST SECURITY S.A.S.

En atención a la revisión de los documentos allegados por el **INTRUST SECURITY S.A.S.**, y en el marco del proceso contractual correspondiente a la Convocatoria Abreviada N° 012-2026, se procede a emitir las siguientes consideraciones técnicas.

1. Sobre la aclaración técnica del desarrollo

Tras la evaluación de la aclaración presentada por el proponente, se determina que la propuesta **CUMPLE parcialmente** con los requerimientos técnicos del desarrollo establecidos en la convocatoria.

A continuación, se describen los puntos en los cuales el proponente aporta la información necesaria:

- Aporta el certificado de idoneidad del personal, capacidad operativa y compromiso de confidencialidad.
- Enumera cinco (5) experiencias de relación certificaciones de las cuales tres (3) de ellas tienen certificación (**Modussoftware y TCC**) quedando por certificar dos (2), **Distribuciones AXA y Valor+**.
- Se evidencia en la propuesta técnica la importancia de proteger los activos de información, la infraestructura tecnológica y los servicios; así mismo, este servicio contempla la monitorización permanente de Internet, Deep Web y Darknet, con el fin de identificar a tiempo filtraciones de información, exposición de credenciales, fuga de datos, venta o intercambio de información institucional, como cualquier actividad maliciosa o amenaza que pueda comprometer los sistemas de la Gobernación de Antioquia. Describe los tres (3) pilares que fundamentan la necesidad del servicio de Vigilancia Tecnológica, Gestión de Vulnerabilidades y Superficie de Ataque,
- Cumplimiento de los tres (3) ejes fundamentales:
 1. **Vigilancia Tecnológica:** El proveedor cumple cada una de las actividades que se requieren para el desarrollo de este ítem, donde empleará plataformas especializadas de inteligencias con informes periódicos con su respectivo nivel de criticidad.
 2. **Gestión de Vulnerabilidades:** El servicio se ejecuta bajo la realización de escaneos de seguridad de manera mensual, como también se ejecutará análisis extraordinarios bajo demanda, en respuesta a incidentes de seguridad. Se aplicarán estándares internacionales como CVSS, buenas prácticas de OWASP para aplicaciones web, y el marco metodológico NIST SP 800-115 con el personal

especializado responsable de la operación continua del servicio. Las actividades estarán articuladas con el marco MITRE ATT&CK, incorporando enfoques como Adversary Emulation, Red Teaming y Threat Hunting.

3. **Gestión de Superficie de Ataque:** El proveedor iniciará con un levantamiento, inventario y análisis de la infraestructura tecnológica de la entidad. A lo mencionado anteriormente se realizará unas evaluaciones integrales de riesgos cibernéticos institucionales.

Conclusión: Cumple parcialmente (requiere subsanación documental).

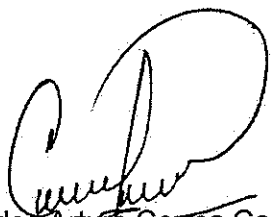
2. Conclusión General

Tras la revisión integral de la propuesta y sus documentos aclaratorios, se concluye que el proveedor:

- Presenta una propuesta técnicamente sólida en materia de seguridad.
- Sin embargo, no cumple parcialmente con los documentos que validan la experiencia requerida.

En consecuencia, el proponente deberá **subsanar las observaciones señaladas** para dar cumplimiento integral a las condiciones del proceso.

Cordialmente,



Carlos Arturo Correa Correa
Profesional Universitario
Valor+ S.A.S



RE: Informe preliminar convocatoria N°12-2026

Desde Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

Fecha Vie 08/05/2026 14:12

Para Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>

CC Sergio Andres Velez Upegui <coordinacion.mesa@valormas.gov.co>; Hector Dario Yepes Vega <dir.contratacion@valormas.gov.co>; Daniela Maria Lopez Angulo <daniela.lopez@valormas.gov.co>

Buena tarde, Paula

Se realiza revisión del informe preliminar convocatoria N°12-2026 el cual se aprueba.

Gracias por su atención y gestión.



Carlos Arturo Correa Correa

Profesional Universitario

carlos.correa@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el receptor de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

De: Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

Enviado: viernes, 8 de mayo de 2026 11:43

Para: Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>

Cc: Sergio Andres Velez Upegui <coordinacion.mesa@valormas.gov.co>; Hector Dario Yepes Vega <dir.contratacion@valormas.gov.co>; Daniela Maria Lopez Angulo <daniela.lopez@valormas.gov.co>

Asunto: Informe preliminar convocatoria N°12-2026

Cordial saludo,

Se comparte la proyección del informe preliminar de la convocatoria del asunto, con el fin de que sea validada y si es del caso aprobada o comentada por ustedes a través de correo. Se construyó con el insumo aportado con cada una de las áreas que intervienen en el proceso.

Agradezco sus comentarios o validaciones antes de las 2:00 pm del día de hoy, con el fin de revisar con el Director Jurídico y poder hacer los ajustes del caso y publicar antes de las 3:00 p.m.

Cordialmente,



Paula Cristina Parra Carmona

Profesional Especializada Grado I

paula.parra@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alajuela
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige.
Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución
o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos
notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.



RV: Evaluacion de propuestas - Convocatoria Abreviada N°012

Desde Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>

Fecha Vie 08/05/2026 13:26

Para Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

3 archivos adjuntos (2 MB)

FO25-DE-GCYN_Evaluación de propuestas (Abreviada_Pública)_v1.0.xlsx; Capacidad_Financiera_INTRUST SECURITY S.A.S.xlsx; EEFF Intrust finales 2025.pdf;

Buen día,

Se adjunta información financiera evaluada de indicadores financieros según información reportada en el RUP del proponente.

El presupuesto o demás información financiera será evaluada por el rol técnico del proceso.

Cordialmente,



Paula Andrea Toro Torres

Gerente Financiera

gerencia.financiera@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

De: Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>

Enviado: Jueves, 07 de Mayo de 2026 15:35

Para: Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>

Asunto: RV: Evaluacion de propuestas - Convocatoria Abreviada N°012

Buen día,

Adjunto la evaluación de la capacidad financiera del proponente de la Convocatoria Abreviada N°012-2026.

Desde el rol financiero solo se revisa y se evalúa los indicadores financieros de los proponentes en el RUP, el presupuesto y demás valores deben ser evaluados desde el rol técnico.

Atentamente,



Veronica Restrepo Alvarez

Profesional Especializado Grado I

veronica.restrepo@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

De: Compras Valor + 2 <compras2@valormas.gov.co>

Enviado el: jueves, 7 de mayo de 2026 2:16 p. m.

Para: Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

Asunto: Evaluacion de propuestas - Convocatoria Abreviada N°012

Cordial saludo,

Adjunto el documento de evaluación de propuestas correspondiente a la Convocatoria Abreviada N.º 012, con el fin de que puedan diligenciarlo y posteriormente se pueda consolidar la información.

Gracias.

Cordialmente;

11/5/26, 7:19

Correo: Paula Cristina Parra Carmona - Outlook

**Daniela María López Angulo**

Profesional Universitaria

compras2@valormas.gov.coCalle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alquíbarra,
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

ANÁLISIS CAPACIDAD FINANCIERA																		
FECHA:	jueves, 7 de mayo de 2026																	
OBJETO:	<i>"Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."</i>																	
PRESUPUESTO:	57.215.200																	
INFORMACIÓN SUMINISTRADA:	SMMLV 1.750.905																	
FUENTE:	PROPONENTE 1 INTRUST SECURITY S.A.S NIT:901.380.604 Estados Financieros 2025, emitido 24-02-2026 CORTE 31/12/2025 Página 4 de 7 <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;">VIGENCIA ESTADOS FINANCIEROS</td> <td style="width: 40%; text-align: right;">2.025</td> </tr> <tr><td>399.412.782</td><td></td></tr> <tr><td>470.059.215</td><td></td></tr> <tr><td>183.418.821</td><td></td></tr> <tr><td>183.418.821</td><td></td></tr> <tr><td>286.640.395</td><td></td></tr> <tr><td>38.586.805</td><td></td></tr> <tr><td>2.471.976</td><td></td></tr> </table>		VIGENCIA ESTADOS FINANCIEROS	2.025	399.412.782		470.059.215		183.418.821		183.418.821		286.640.395		38.586.805		2.471.976	
VIGENCIA ESTADOS FINANCIEROS	2.025																	
399.412.782																		
470.059.215																		
183.418.821																		
183.418.821																		
286.640.395																		
38.586.805																		
2.471.976																		
ACTIVO CORRIENTE ACTIVO TOTAL PASIVO CORRIENTE PASIVO TOTAL PATRIMONIO UTILIDAD / PERDIDA OPERACIONAL GASTO DE INTERESES																		
ANÁLISIS REALIZADO	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #cccccc;"> <th style="width: 40%; text-align: center;">REQ. FINANCIEROS ESTABLECIDOS</th> <th style="width: 60%;"></th> </tr> </thead> <tbody> <tr> <td>INDICE DE LIQUIDEZ</td> <td>Mayor o igual a 1.3</td> </tr> <tr> <td>INDICE DE ENDEUDAMIENTO</td> <td>Menor o igual al 60%</td> </tr> <tr> <td>RAZÓN DE COBERTURA DE INTERESES</td> <td>Mayor o igual a 2.0</td> </tr> <tr> <td>RENTABILIDAD DEL PATRIMONIO</td> <td>Mayor o igual a 0.05</td> </tr> <tr> <td>RENTABILIDAD DEL ACTIVO</td> <td>Mayor o igual a 0.02</td> </tr> </tbody> </table>		REQ. FINANCIEROS ESTABLECIDOS		INDICE DE LIQUIDEZ	Mayor o igual a 1.3	INDICE DE ENDEUDAMIENTO	Menor o igual al 60%	RAZÓN DE COBERTURA DE INTERESES	Mayor o igual a 2.0	RENTABILIDAD DEL PATRIMONIO	Mayor o igual a 0.05	RENTABILIDAD DEL ACTIVO	Mayor o igual a 0.02				
REQ. FINANCIEROS ESTABLECIDOS																		
INDICE DE LIQUIDEZ	Mayor o igual a 1.3																	
INDICE DE ENDEUDAMIENTO	Menor o igual al 60%																	
RAZÓN DE COBERTURA DE INTERESES	Mayor o igual a 2.0																	
RENTABILIDAD DEL PATRIMONIO	Mayor o igual a 0.05																	
RENTABILIDAD DEL ACTIVO	Mayor o igual a 0.02																	
CONCLUSIÓN	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;"></td> <td style="width: 40%; text-align: center;"> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 60%; text-align: center;">2,18</td><td style="width: 40%; text-align: center;">CUMPLE</td></tr> <tr><td style="text-align: center;">39%</td><td style="text-align: center;">CUMPLE</td></tr> <tr><td style="text-align: center;">16</td><td style="text-align: center;">CUMPLE</td></tr> <tr><td style="text-align: center;">0,1346</td><td style="text-align: center;">CUMPLE</td></tr> <tr><td style="text-align: center;">0,08</td><td style="text-align: center;">CUMPLE</td></tr> </table> </td> </tr> <tr> <td colspan="2" style="padding: 5px;">Cumple los ítem requeridos de capacidad financiera.</td> </tr> <tr> <td colspan="2" style="padding: 5px;">Ver otras anotaciones.</td> </tr> </table>			<table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 60%; text-align: center;">2,18</td><td style="width: 40%; text-align: center;">CUMPLE</td></tr> <tr><td style="text-align: center;">39%</td><td style="text-align: center;">CUMPLE</td></tr> <tr><td style="text-align: center;">16</td><td style="text-align: center;">CUMPLE</td></tr> <tr><td style="text-align: center;">0,1346</td><td style="text-align: center;">CUMPLE</td></tr> <tr><td style="text-align: center;">0,08</td><td style="text-align: center;">CUMPLE</td></tr> </table>	2,18	CUMPLE	39%	CUMPLE	16	CUMPLE	0,1346	CUMPLE	0,08	CUMPLE	Cumple los ítem requeridos de capacidad financiera.		Ver otras anotaciones.	
	<table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 60%; text-align: center;">2,18</td><td style="width: 40%; text-align: center;">CUMPLE</td></tr> <tr><td style="text-align: center;">39%</td><td style="text-align: center;">CUMPLE</td></tr> <tr><td style="text-align: center;">16</td><td style="text-align: center;">CUMPLE</td></tr> <tr><td style="text-align: center;">0,1346</td><td style="text-align: center;">CUMPLE</td></tr> <tr><td style="text-align: center;">0,08</td><td style="text-align: center;">CUMPLE</td></tr> </table>	2,18	CUMPLE	39%	CUMPLE	16	CUMPLE	0,1346	CUMPLE	0,08	CUMPLE							
2,18	CUMPLE																	
39%	CUMPLE																	
16	CUMPLE																	
0,1346	CUMPLE																	
0,08	CUMPLE																	
Cumple los ítem requeridos de capacidad financiera.																		
Ver otras anotaciones.																		
OTRAS ANOTACIONES:																		



Factor de evaluación	Formula	Criterio	INTRUST SECURITY S.A.S						
			Cumple / No cumple	Cumple / No cumple	Cumple / No cumple	Cumple / No cumple	Cumple / No cumple	Cumple / No cumple	
			CAPACIDAD FINANCIERA (indicadores de						
INDICE DE LIQUIDEZ	Activo corriente / Pasivo corriente	Mayor o igual a 1.3	Cumple						
INDICE DE ENDEUDAMIENTO	Pasivo total / Activo total	Menor o igual al 60%	Cumple						
RAZÓN DE COBERTURA DE INTERESES	Utilidad operativa Gastos por intereses	Mayor o igual a 2.0	Cumple						
CAPACIDAD ORGANIZACIONAL (indicadores de Rentabilidad)									
RENTABILIDAD DEL PATRIMONIO	Utilidad /patrimonio	Mayor o igual a 0.05	Cumple						
RENTABILIDAD DEL ACTIVO	Utilidad / activos	Mayor o igual a 0.02	Cumple						



Versionamiento Formato

Código: FO16-DE-GCYN
Versión: 1.0
Fecha actualización: 8/11/2023

Medellín, 08 de mayo de 2026

Convocatoria Abreviada N° 012 - 2026

Objeto: “Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet”

Valor+ S.A.S.

INFORME DE EVALUACIÓN PRELIMINAR

De conformidad con el cronograma de la “Convocatoria Abreviada N° 012-2026”, el día 28 de abril de 2026, se envió el documento Condiciones de la Contratación con todos sus anexos a cinco (05) personas jurídicas y se publicó en plataforma Web (Página Web de la empresa), en el cual se informaron todos los requisitos y exigencias para participar en el proceso.

#	Proponente	Nit	Medio de Comunicación
1	3 POINTECH S.A.S.	900.131.823	gerencia@3pointech.net , compras@3pointech.net
2	INTRUST SECURITY S.A.S.	901.380.604-6	sbaron@intrustsecurity.co
3	CCD COMPAÑIA DE CIBERSEGURIDAD Y DEFENSA S.A.S.	900.096.184	procesoscomerciales@ccd.com.co
4	GAMMA INGENIEROS S.A.S.	891.501.783	natalia.molina@gammaingenieros.com
5	HEIMCORE S.A.S.	900.425.697	yvasquez@heimcore.com.co , larodriguez@heimcore.com.co

Hasta las 18:00 horas del día 29 de abril de 2026, se estableció el plazo para la presentación de observaciones y/o solicitud de aclaraciones a las condiciones de la contratación.

Se presentaron observaciones y/o solicitud de aclaraciones a las condiciones de la contratación por parte de las siguientes empresas: (Ver Adjunto Observaciones)

#	Proponente	Fecha y Hora	Medio de Comunicación
1	INCOREDITO	29/04/2026 a las 16:51 horas	chenao@incocredito.com.co
2	GAMMA INGENIEROS S.A.S.	29/04/2026 a las 15:02 horas	natalia.molina@gammaingenieros.com

Posterior a esto, se generó de acuerdo con lo establecido en el cronograma, la respuesta a las observaciones presentadas, lo cual tenía plazo hasta el 04 de mayo de 2026 a las 17:00 horas. (Ver adjunto Respuesta Observaciones)

La empresa 3 POINTECH S.A.S., el día 28 de abril de 2026 estando dentro del plazo establecido, manifestó lo siguiente: “(...)encontramos que no se encuentra dentro de nuestro portafolio esa **solución**”. También la empresa GAMMA INGENIEROS S.A.S. el día 06 de mayo de 2026 indicó a través de correo electrónico lo siguiente: “(...)en este caso NO es posible participar, el motivo es NO poder llegar al presupuesto asignado,(...)”

El plazo establecido para la presentación de las propuestas fue hasta el día 06 de mayo de 2026, hasta las 17:00 horas y se presentó el siguiente proponente, tal y como consta en el acta de recepción:

Proponente	Nit	Fecha y hora de Recepción	Valor Propuesta	Medio de recibo de la propuesta	# Folios
INTRUST SECURITY S.A.S	901.380.604-6	06/05/2026 16:12 horas	\$55.800.000	compras2@valormas.gov.co	Se recibe por medio digital



Versionamiento Formato
 Código: FO16-DE-GCYN
 Versión: 1.0
 Fecha actualización: 8/11/2023

De acuerdo con lo anterior y continuando con el cronograma establecido, se realiza la revisión de la oferta económica del proponente, con el fin de validar su participación en el proceso de contratación y continuar con los requisitos de admisibilidad o habilitantes.

N°	PROPONENTES	VALOR PROPUESTA	CUMPLE / NO CUMPLE
1	INTRUST SECURITY S.A.S.	\$55.800.000	Cumple

El proponente **INTRUST SECURITY S.A.S. CUMPLE** con el factor económico, el valor de la propuesta esta ajustado al presupuesto oficial establecido por la entidad.

En consecuencia, de lo anterior se evaluarán los aspectos jurídicos, técnicos, financieros, organizacionales, equipo de trabajo y certificaciones solicitadas al proveedor.

1. VERIFICACIÓN REQUISITOS HABILITANTES:

De acuerdo con los requisitos habilitantes establecidos en el documento Condiciones de la Contratación y los documentos aportados con la oferta, se procede con la validación del proponente **INTRUST SECURITY S.A.S.:**

1.1. Capacidad Jurídica:

N°	DOCUMENTO	INTRUST SECURITY S.A.S. CUMPLE / NO CUMPLE	OBSERVACIÓN
1	Carta de presentación de la propuesta debidamente diligenciada.	Cumple	Aporta carta de presentación de la propuesta debidamente diligenciada y suscrita por el Representante Legal, fechada a 06 de mayo de 2026.
2	Certificado de existencia y representación legal del proponente, con fecha de expedición no mayor a treinta (30) días anteriores a la fecha de presentación de la oferta.	Cumple	Presentado con fecha del 06/05/2026.
3	Acta de la Junta o Asamblea que autoriza al representante legal del Proponente a presentar la oferta, cuando se trate de persona jurídica (Si aplica).	N/A	De conformidad con el certificado de existencia y representación legal, el proponente no tiene restricciones de contratación por razón de la naturaleza ni de la cuantía de los actos que celebre. Adicional, el Certificado señala: "REPRESENTACION LEGAL. El Gerente General será el Representante Legal de la sociedad y tendrá a su cargo la inmediata dirección y administración de los negocios sociales con sujeción a las disposiciones legales y estatutarias y a las decisiones de la asamblea general de

			accionistas. Todos los funcionarios y empleados de la sociedad, con excepción de los nombrados por la asamblea general, estarán subordinados a él y bajo su dirección e inspección inmediata."
4	Certificado de estar a paz y salvo con el sistema de seguridad social integral (salud, pensión, riesgos profesionales y ARL) y aportes parafiscales (ICBF, Sena y Cajas de Compensación Familiar), expedido por el representante legal y/o contador o revisor fiscal (adjuntando copia de la cédula, copia de la tarjeta profesional y certificado de antecedentes disciplinarios expedido por la junta central de contadores del contador) o Planilla integrada de autoliquidación de aportes a la seguridad social integral y aportes parafiscales.	Cumple	Aporta certificado con fecha del 06 de mayo de 2026, suscrito por el Representante Legal y el Contador. También aporta: -Copia de la cédula del contador. -Copia de la tarjeta profesional del contador. -Certificado de antecedentes disciplinarios expedido por la junta central de contadores del 24 de abril de 2026 con vigencia de tres (3) meses contados a partir de la fecha de su expedición.
5	Copia del documento de identidad del representante legal o apoderado.	Cumple	Aporta cédula de ciudadanía
6	Copia del Registro Único Tributario (RUT)	Cumple	Aporta el documento actualizado con fecha de generación del 06/05/2026.
7	Certificado Registro de Deudores Alimentarios Morosos – REDAM	Cumple	Aporta certificado del 05/05/2026 del representante legal, sin reporte de antecedentes y valido hasta el 04/08/2026.
8	Certificado de la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST, emitido por la ARL o el Ministerio del Trabajo, con vigencia no mayor a noventa (90) días antes de la presentación de la oferta.	Cumple	Aporta certificado emitido por Sura con fecha del 19 de marzo de 2026.
9	Certificado Antecedentes fiscales (Representante legal y persona jurídica).	Cumple	Aporta certificados del Representante Legal y de la Persona Jurídica del 05/05/2026 sin reporte de antecedentes.
10	Certificado Antecedentes Disciplinarios (Representante legal y persona jurídica).	No Cumple	Aporta certificado del 05/05/2026 del Representante Legal sin reportes de antecedentes. No aporta certificado de la persona jurídica.
11	Certificado Antecedentes judiciales del Representante legal.	Cumple	Aporta certificado del 06/05/2026 del representante legal, sin reporte de antecedentes.
12	Certificado Antecedentes Medidas correctivas del Representante legal.	Cumple	Aporta certificado del 06/05/2026 del representante legal, sin reporte de antecedentes.
13	Certificado Antecedentes de delitos sexuales cometidos contra menores de 18 años del Representante legal.	Cumple	Aporta certificado del 06/05/2026 del representante legal, sin reporte de antecedentes.
14	Certificación Bancaria.	No Cumple	Aporta certificado del 04/03/2026 expedida por Bancolombia.



Versionamiento Formato

Código: FO16-DE-GCYN
 Versión: 1.0
 Fecha actualización: 8/11/2023

			La expedición de los certificados no podrá tener una anterioridad superior a treinta (30) días calendario, contado a partir de la fecha de cierre del proceso.
15	Formato Inhabilidades e Incompatibilidades Persona Jurídica diligenciado.	Cumple	Debidamente diligenciado y suscrito por el representante legal con fecha del 06/05/2026.
16	Formato Autorización tratamiento de datos diligenciado.	Cumple	Debidamente diligenciado y suscrito por el representante legal con fecha del 06/05/2026.
17	Formato Certificación de lavado de activos y financiación del terrorismo diligenciado.	No Cumple	El formato esta suscrito por el Representante Legal y fechado al 06/05/2026, pero no se encuentra debidamente diligenciado.
18	Garantía de seriedad de la oferta.	Cumple	Póliza emitida por Seguros del Estado S.A. Vigencia desde el 06/05/2026 hasta el 20/08/2026. Valor Asegurado de \$5.721.520 (10% del valor del presupuesto oficial). Aporta comprobante de pago de la prima.
19	Registro Único de Proponentes – RUP renovado y en firme. Los proponentes deberán estar inscritos y clasificados en el Registro Único de Proponentes de la Cámara de Comercio de su jurisdicción, de acuerdo con las condiciones establecidas en el Título VI Registro Único de Proponentes –RUP del Decreto 1082 de 2015. La expedición de dicho certificado no podrá tener una anterioridad superior a treinta (30) días calendario, contado a partir de la fecha de cierre del proceso. En caso de no contar con el RUP renovado en firme, se deberán aportar Balances o Estados Financieros aprobados del año inmediatamente anterior.	Cumple	Aporta Estados Financieros 2025, elaborados el 24 de febrero de 2026, aprobados por el Representante Legal y Contador de la empresa.
20	Manifestación Juramentada de Ausencia de Multas y/o Sanciones: El proponente deberá hacer manifestación juramentada de ausencia o presencia de multas y/o sanciones impuestas por entidades públicas en los cinco (5) últimos años anteriores al cierre de esta convocatoria.	Cumple	Aporta Manifestación Juramentada de Ausencia de Multas y/o Sanciones con fecha del 06/05/2026 suscrita por el representante legal.

CONCLUSIÓN: De acuerdo con lo anterior, el proponente **INTRUST SECURITY S.A.S. CUMPLE DE MANERA PARCIAL** con los requisitos jurídicos habilitantes, por lo tanto, **DEBE SUBSANAR** lo siguiente:

- “10. Certificado Antecedentes Disciplinarios (Representante legal y persona jurídica)”. **Debe aportar certificado de la persona jurídica.**
- “14. Certificación Bancaria. **Debe aportar certificado vigente,** ya que como se determinó en las condiciones de la contratación: “La expedición de los certificados no podrá tener una

anterioridad superior a treinta (30) días calendario, contado a partir de la fecha de cierre del proceso.”

- **“17. Formato Certificación de lavado de activos y financiación del terrorismo diligenciado.” Debe aportar certificado debidamente diligenciado.**

1.2. Capacidad Técnica:

1.2.1. PROPUESTA (Alcance):

Atendiendo a las “Condiciones de la Contratación Convocatoria Abreviada N° 012-2026”, específicamente para el numeral “**Alcance y/o Condiciones y/o Especificaciones Técnicas del Bien o Servicio a Contratar**”, en el “**Servicio de Vigilancia Tecnológica, Gestión de Vulnerabilidades y Superficie de Ataque**”, **en los ejes fundamentales**, se tiene para **los ejes** lo siguiente:

1. ***“Vigilancia Tecnológica: (...) Para el cumplimiento de esta obligación, el Proveedor deberá emplear plataformas especializadas de inteligencia de amenazas (Threat Intelligence), cuya selección deberá estar debidamente sustentada mediante criterios técnicos, funcionales y de cobertura.”***; si bien, en el documento “Propuesta” se menciona lo anterior, no se indica cual es la plataforma o plataformas para utilizar por el proveedor y la sustentación desde lo técnico, lo funcional y la cobertura.

CONCLUSIÓN: De acuerdo con lo anterior, el proponente **CUMPLE DE MANERA PARCIAL** con este ítem, ya que, no indicó cual es la plataforma o plataformas que utilizará y la sustentación de esto. **Para poder evaluarlo correctamente, se requiere que el proponente realice las precisiones respecto a la plataforma o plataformas a emplear y su descripción y alcance,** con el fin de asegurar que la oferta cumple con todas las especificaciones técnicas y se eviten riesgos en la ejecución.

2. ***“Gestión de Vulnerabilidades, (...) Para la clasificación y priorización de vulnerabilidades, el Proveedor deberá aplicar estándares internacionales, tales como el modelo CVSS (Common Vulnerability Scoring System). En el caso de aplicaciones web, deberá adoptar las buenas prácticas establecidas por OWASP (Open Web Application Security Project), y para la ejecución de pruebas técnicas, deberá alinearse con lo establecido en el marco metodológico NIST SP 800-115. Asimismo, las actividades deberán estar articuladas con el marco MITRE ATT&CK, incorporando enfoques como Adversary Emulation, Red Teaming y Threat Hunting, orientados a fortalecer la capacidad de detección y respuesta ante amenazas avanzadas. Deberá presentar certificado manifestando que aplica los estándares y buenas prácticas solicitadas en el párrafo anterior.”***

CONCLUSIÓN: De acuerdo con lo anterior, el proponente **CUMPLE DE MANERA PARCIAL** con este ítem, ya que, no presentó **certificado manifestando que aplica los estándares y buenas prácticas solicitadas en el párrafo anterior.** **Se solicita aportar este certificado,** todo esto, con el fin de asegurar que la oferta cumple con todas las especificaciones técnicas y se eviten riesgos en la ejecución.

Adicional a lo anterior, en el alcance se estableció lo siguiente: ***“Gestión y tratamiento de vulnerabilidades (...) El proveedor deberá ejecutar las actividades descritas, garantizando el cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad (ISO 27001, NIST, MITRE ATT&CK, OWASP, entre otros). Deberá presentar certificado manifestando que garantiza lo anterior.”***



Versionamiento Formato

Código: FO16-DE-GCYN
 Versión: 1.0
 Fecha actualización: 8/11/2023

CONCLUSIÓN: De acuerdo con lo anterior, el proponente **CUMPLE DE MANERA PARCIAL** con este ítem, ya que, no presentó **certificado manifestando que garantiza lo anterior. Se solicita aportar este certificado**, todo esto, con el fin de asegurar que la oferta cumple con todas las especificaciones técnicas y se eviten riesgos en la ejecución.

También, **se debe indicar** como se estableció en el alcance, si en el desarrollo del objeto contractual y en cumplimiento de esta gestión, desarrollará "(...) *ejercicios especializados tales como pruebas de penetración (caja negra y/o caja gris) sobre los activos críticos definidos por la entidad, así como actividades de Threat Hunting, Adversary Emulation y Red Teaming, orientadas a fortalecer la capacidad de detección y respuesta frente a amenazas avanzadas.*"

CONCLUSIÓN: De acuerdo con lo anterior, el proponente **CUMPLE DE MANERA PARCIAL** con este ítem, ya que, no realizó precisiones al respecto en la propuesta y documentos aportados. **Se solicita realizar las claridades respectivas en la propuesta o en documento adjunto suscrito por el Representante Legal**, todo esto, con el fin de asegurar que la oferta cumple con todas las especificaciones técnicas y se eviten riesgos en la ejecución.

1.2.2. Adicionalmente y de acuerdo con los requisitos de capacidad técnica establecidos en el documento condiciones de la contratación "(...) **el proponente deberá acreditar la cuantía en máximo dos (2) contratos relacionados con el objeto del presente proceso, en ejecución, ejecutados o terminados a la fecha de cierre de la convocatoria y cuya sumatoria sea igual o superior al presupuesto oficial establecido para esta contratación.**"

Las certificaciones deberán contener por lo menos la siguiente información:

- Contratante.
- Contratista.
- Objeto.
- Valor.
- Plazo.
- Estado: (en ejecución, ejecutado o terminado)

Los certificados de experiencia deben ser en idioma español.

Para los contratos en ejecución, adicionalmente se deberá certificar cual es el valor ejecutado a la fecha."

Nº	CONTRATANTE	OBJETO DEL CONTRATO	VALOR EN SMMLV/PESOS	CUMPLE/ NO CUMPLE	OBSERVACIONES
1	MODUSOFTWARE	Evaluar y fortalecer la postura de seguridad de los activos tecnológicos de ALDEAMO mediante ejercicios avanzados de Red Team y Ethical Hacking, con el fin de identificar vulnerabilidades	\$65.000.000	Cumple	Plazo: Desde el 01/09/2025 hasta el 05/10/2025 45,66 SMMLV.

		críticas, validar controles existentes y proponer medidas de mitigación alineadas a estándares internacionales y necesidades estratégicas de la organización			
2	MODUSOFTWARE	Prestar el servicio profesional de auditoría para evaluar el cumplimiento frente a las buenas prácticas: ISO 27032 (Cybersecurity Framework) y Cybersecurity Framework NIST (National Institute of Estandar and Technology) y realizar una verificación de los controles establecidos por el cliente de MODUSOFTWARE en ese caso la CCB, para mitigar los riesgos de ciberseguridad, a través de la emisión de recomendaciones que permitan tomar acciones para mejorar el programa de gobierno de la ciberseguridad y de los controles implementados.	\$139.200.000	Cumple	Plazo: Desde el 29/07/2024 hasta el 27/10/2024 107, 07 SMMLV

Nota: La sumatoria de los contratos que se acreditan como experiencia habilitante, cumple con lo solicitado en este criterio.

CONCLUSIÓN: De acuerdo con lo anterior, el proponente **CUMPLE DE MANERA PARCIAL** con los requisitos habilitantes de carácter técnico, lo anterior, **ya que debe realizar claridades respecto de los ejes 1 y 2, el alcance y aportar las certificaciones y documentos ya señalados.**

1.3. Capacidad Financiera:

“Los requisitos financieros para participar en el presente proceso serán verificados a partir de la información que deberán aportar el o los proponentes en el correspondiente Registro Único de

Proponentes – RUP debidamente actualizado y renovado y/o Balances o Estados Financieros aprobados del año inmediatamente anterior.”

Para validar la capacidad financiera, el oferente deberá aportar los siguientes indicadores:

INDICADOR	FÓRMULA	INDICADOR	INDICADOR PROPONENTE	CUMPLE/NO CUMPLE
Índice de Liquidez	$\frac{\text{Activo corriente}}{\text{Pasivo Corriente}}$	Mayor o igual a 1.3	2.18	Cumple
Índice de endeudamiento	$\frac{\text{Activo Total}}{\text{Pasivo Total}}$	Menor o igual al 60%	39%	Cumple
Razón de Cobertura de Intereses	$\frac{\text{Utilidad operacional}}{\text{Gasto de Intereses}}$	Mayor o igual a 2.0	16	Cumple

1.4. Capacidad organizacional:

“Para validar la capacidad organizacional se tomará la información que aparezca en el Registro Único de Proponentes (RUP) y/o Balances o Estados Financieros aprobados del año inmediatamente anterior.”

Para validar la capacidad organizacional, el oferente deberá aportar los siguientes indicadores:

FACTOR EVALUACIÓN	FORMULA	CRITERIO	INDICADOR PROPONENTE	CUMPLE/NO CUMPLE
Indicadores de Rentabilidad				
ROE	$\frac{\text{Utilidad Operacional}}{\text{Patrimonio}}$	Mayor o igual al 5%	13.46%	Cumple
ROA	$\frac{\text{Utilidad Operacional}}{\text{Activo Total}}$	Mayor o igual al 2%	8%	Cumple

De acuerdo con la revisión de los indicadores financieros exigidos en la convocatoria abreviada, se evidencia que el proponente **cumple** con los requisitos establecidos.

En relación con el índice de liquidez, la entidad registra un valor de 2.18, superior al mínimo requerido de 1.3, lo que evidencia una sólida capacidad para atender sus obligaciones de corto plazo, así como un adecuado respaldo de sus pasivos corrientes. Además, el índice de endeudamiento se sitúa en 39%, por debajo del límite máximo establecido de 60%; este resultado refleja una menor dependencia de recursos de terceros en la financiación de los activos, lo que reduce la exposición al riesgo financiero sin afectar la percepción de solvencia de la entidad.

En cuanto a la razón de cobertura de intereses, la entidad alcanza un valor de 16, superior al mínimo exigido de 2, lo que demuestra una capacidad holgada para cubrir los gastos financieros derivados de sus obligaciones, evidenciando estabilidad operativa.

Adicionalmente, la rentabilidad del patrimonio (ROE) se ubica en 13.46% superior al mínimo exigido de 5%, lo que refleja una alta eficiencia en la generación de utilidades a partir de los recursos propios. De manera complementaria, la rentabilidad del activo (ROA) alcanza un valor de 8% superior al mínimo exigido del 2%, evidenciando una gestión eficiente de los activos y una sólida capacidad de generación de beneficios.

Los indicadores analizados evidencian que la entidad presenta fortalezas significativas en liquidez, rentabilidad y capacidad de cobertura financiera, respaldando una posición financiera sólida y estable.

CONCLUSIÓN: De acuerdo con lo anterior, el proponente **CUMPLE** con los requisitos habilitantes de carácter financieros.

1.5. Personal Especializado:

*De acuerdo con lo establecido en el documento "Condiciones de la Contratación Convocatoria Abreviada N°012-2026", respecto del personal, "(...) El Proveedor deberá disponer de un **componente de personal especializado** para la gestión de vulnerabilidades, el cual será responsable de la operación continua del servicio. Este equipo deberá garantizar la gestión integral del ciclo de vida de las vulnerabilidades, desde su identificación hasta su cierre, incluyendo la validación de la remediación aplicada. De igual forma, deberá coordinar con las áreas técnicas de la entidad la implementación de controles correctivos, realizar seguimiento a los planes de acción y asegurar la trazabilidad de cada hallazgo.*

El personal asignado deberá contar con formación profesional en áreas afines a tecnologías de la información y ciberseguridad, así como certificaciones vigentes de reconocimiento internacional, tales como CEH, OSCP, CISA, CISSP o equivalentes. Adicionalmente, deberán acreditar experiencia comprobada en la ejecución de pruebas de seguridad, análisis de vulnerabilidades y gestión de riesgos tecnológicos. Deberá presentar certificado manifestando que cuenta con el equipo para garantizar la prestación del servicio y que cumple con las certificaciones y experiencia requerida

Documento aportado: ***"Certificación de idoneidad del personal, capacidad operativa y compromiso de confidencialidad."***: Aporta certificación suscrita por el Representante Legal de la empresa, donde indican que cuentan con *"el personal profesional asignado para la ejecución del contrato, que estos cuentan con formación académica en áreas afines a las tecnologías de la información y la ciberseguridad, así como con certificaciones vigentes de reconocimiento internacional, entre las que se incluyen CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), CISA, CISSP y/o sus equivalentes, según el perfil de cada profesional asignado."*, lo anterior, con la finalidad de garantizar la adecuada prestación del servicio objeto del presente proceso de selección.

CONCLUSIÓN: De acuerdo con lo anterior, el personal requerido **CUMPLE** con los requisitos habilitantes de carácter técnico, toda vez que, se aportó por parte del proponente, certificado suscrito por el Representante Legal, donde **manifiesta que cuenta con el equipo para garantizar la prestación del servicio.**

1.6. Certificaciones solicitadas al proveedor:

Frente a lo requerido para garantizar la confidencialidad, integridad y disponibilidad de la información a la que tenga acceso en el desarrollo del contrato, así como del cumplimiento de las políticas de seguridad de la entidad y la normativa vigente aplicable, el proveedor presenta documento ***“Certificación de idoneidad del personal, capacidad operativa y compromiso de confidencialidad.”***, a través del cual manifiesta: ***“TERCERO – CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD Intrust Security S.A.S. se compromete a garantizar la confidencialidad, integridad y disponibilidad de toda la información a la que tenga acceso en desarrollo del contrato. En consecuencia: • Toda la información obtenida será tratada como estrictamente confidencial y no será divulgada, cedida ni utilizada para fines distintos a los establecidos contractualmente. • El personal asignado suscribirá acuerdos individuales de confidencialidad antes del inicio de las actividades. • Se cumplirán en su totalidad las políticas de seguridad de la información de la entidad contratante, así como la normativa vigente aplicable, incluyendo la Ley 1581 de 2012 y demás disposiciones en materia de protección de datos personales y seguridad de la información.”***

CONCLUSIÓN: De acuerdo con lo anterior, **CUMPLE** con los requisitos habilitantes de carácter técnico, toda vez que, se aportó por parte del proponente, certificado suscrito por el Representante Legal, donde manifiesta su compromiso de confidencialidad.

2. RESUMEN DE LA VERIFICACIÓN DE LOS REQUISITOS HABILITANTES

Los requisitos habilitantes son objeto de verificación, por lo tanto, únicamente se considera habilitado aquel oferente que cumpla con todos los requisitos solicitados. Se evaluarán como “Cumple”. En caso contrario, se evaluarán como “No Cumple” y, por tanto, no será objeto de evaluación en los requisitos de calificación, sin perjuicio de la subsanación que los oferentes puedan realizar en el término que otorgue Valor+ S.A.S.

N	Proponente	Verificación Jurídica	Verificación Técnica	Verificación Financiera	Verificación Organizacional	Verificación Equipo de Trabajo	Certificaciones solicitadas al proveedor
1	INTRUST SECURITY S.A.S.	CUMPLE DE MANERA PARCIAL	CUMPLE DE MANERA PARCIAL	CUMPLE	CUMPLE	CUMPLE	CUMPLE

3. CRITERIOS DE EVALUACIÓN:

Según lo establecido en el documento “Condiciones de la Contratación Convocatoria Abreviada N°012-2026 para el numeral 4. EVALUACIÓN DE PROPUESTAS”: (...) El criterio de selección que permita identificar la oferta más favorable para Valor+ S.A.S., será la ponderación de los siguientes criterios, siempre que haya cumplido con las especificaciones técnicas y requisitos habilitantes del proceso.

Lo anterior, de acuerdo con lo siguiente:

ÍTEM DE EVALUACIÓN	PUNTOS
PRECIO: Oferta de menor valor	85
APOYO A LA INDUSTRIA NACIONAL	10
EMPRENDIMIENTO Y EMPRESAS DE MUJERES	5
TOTAL	100

(...)”, se encuentra lo siguiente:

N°	Proponente	Criterio 1. Precio	Criterio 2. Apoyo a la industria Nacional	Criterio 3. Emprendimiento y empresas de mujeres	Puntaje	Observaciones
1	INTRUST SECURITY S.A.S.	0	0	0	0	N/A

4. SOLICITUD DE SUBSANACIÓN:

Valor+ se permite solicitar la subsanación de los siguientes requisitos y/o documentos:

N°	Proponente	Verificación Jurídica	Verificación Técnica	Verificación Financiera	Verificación Organizacional	Verificación Equipo de Trabajo	Certificaciones solicitadas al proveedor:
1	INTRUST SECURITY S.A.S.	CUMPLE DE MANERA PARCIAL. Debe aportar y/o aclarar y/o diligenciar: -Certificado Antecedentes Disciplinarios (persona jurídica) -Certificación Bancaria vigente. -Diligenciar de manera correcta el Formato Certificación de lavado de activos y financiación del terrorismo diligenciado.	CUMPLE DE MANERA PARCIAL. Debe aportar y/o precisar: -Realizar las precisiones respecto a la plataforma o plataformas a emplear y su descripción y alcance. -Aportar certificado manifestando que aplica los estándares y buenas prácticas solicitadas para Gestión de Vulnerabilidades. -Aportar certificado donde señale que ejecutará las actividades descritas en el alcance, garantizando el cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad (ISO 27001, NIST, MITRE ATT&CK, OWASP, entre otros). -Indicar a través de documento suscrito por el Representante Legal si en el desarrollo del objeto contractual y en cumplimiento de esta gestión, desarrollará "(...) ejercicios especializados tales como pruebas de penetración (caja negra y/o caja gris) sobre los activos	CUMPLE	CUMPLE	CUMPLE	CUMPLE



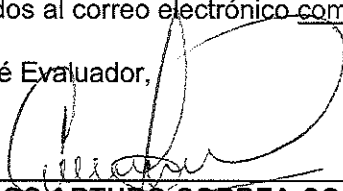
Versionamiento Formato

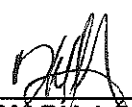
Código: F016-DE-GCYN
 Versión: 1.0
 Fecha actualización: 8/11/2023

			críticos definidos por la entidad, así como actividades de Threat Hunting, Adversary Emulation y Red Teaming, orientadas a fortalecer la capacidad de detección y respuesta frente a amenazas avanzadas."				
--	--	--	---	--	--	--	--

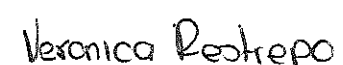
El presente informe es puesto a consideración del proponente, con el fin de que subsane y/o presente observaciones conforme con lo indicado, para lo cual se le otorga un plazo máximo hasta el día 11 de mayo de 2026 hasta las 18:00 horas. Los documentos de subsanación y/o observaciones, deberán ser enviados al correo electrónico compras2@valormas.gov.co

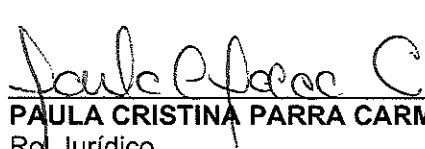
Comité Evaluador,


CARLOS ARTURO CORREA CORREA
 Rol técnico


DANIELA MARÍA LOPEZ ANGULO
 Rol logístico


PAULA ANDREA TORO TORRES
 Rol Financiero


VERÓNICA RESTREPO ÁLVAREZ
 Rol Financiero


PAULA CRISTINA PARRA CARMONA
 Rol Jurídico

Informe de Evaluación Preliminar- Convocatoria Abreviada N°012-2026 - INTRUST SECURITY S.A.S.

Desde Compras Valor + 2 <compras2@valormas.gov.co>

Fecha Vie 08/05/2026 15:30

Para Sergio Mauricio Baron Vera <sbaron@intrustsecurity.co>

CC Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

 1 archivo adjunto (2 MB)

Informe Preliminar Convocatoria N°12-2026.pdf;

Cordial saludo,

Adjunto se envía informe de evaluación preliminar, para la Convocatoria Abreviada N°012-2026, cuyo objeto es: ***“Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet.”***

Quedamos atentos a cualquier inquietud u observación.

Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distracción o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

Informe preliminar- Abreviada N° 012 -2026

Desde Compras Valor + 2 <compras2@valormas.gov.co>

Fecha Vie 08/05/2026 15:21

Para Victor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

CC Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

 1 archivo adjunto (2 MB)

Informe Preliminar Convocatoria N°12-2026.pdf;

Cordial saludo,

Amablemente solicito tu ayuda por favor, para publicar el informe preliminar en la página web de la entidad.

Convocatoria Abreviada N°012-2026.

Objeto: “Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet.”

Quedo atenta,

Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,

Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

RE: Informe preliminar- Abreviada N° 012 -2026

Desde Víctor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

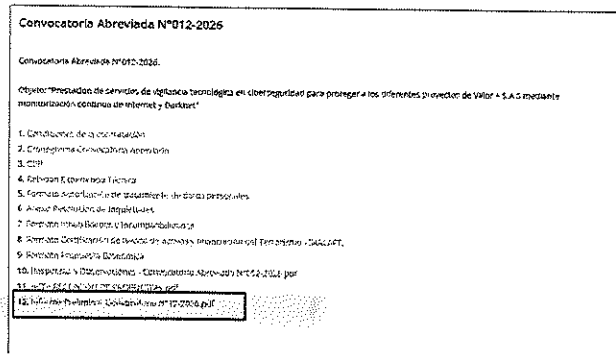
Fecha Vie 08/05/2026 15:26

Para Compras Valor + 2 <compras2@valormas.gov.co>

CC Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

Buenas tardes.

Dando respuesta a lo solicitado se carga documento al sitio web de la entidad.



Gracias por la atención prestada.
Saludos



Víctor Rodrigo Galvis Zuleta
Contratista
victor.galvis@valormas.gov.co
Carrera 53A #42-161, Torre B, Piso 6
Ed. Plaza de la Libertad
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si al lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error, le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

De: Compras Valor + 2 <compras2@valormas.gov.co>

Enviado el: viernes, 8 de mayo de 2026 3:21 p. m.

Para: Víctor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

CC: Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

Asunto: Informe preliminar- Abreviada N° 012 -2026

Cordial saludo,

Amablemente solicito la ayuda por favor, para publicar el informe preliminar en la página web de la entidad.

Convocatoria Abreviada N°012-2026.

Objeto: "Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."

Quedo atenta,

Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatei, Piso 3 Sector Alajuela,

Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.



RV: Informe de Evaluación Preliminar- Convocatoria Abreviada N°012-2026 - INTRUST SECURITY S.A.S.

Desde Compras Valor + 2 <compras2@valormas.gov.co>

Fecha Mar 12/05/2026 10:02

Para Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

CC Compras Valor + <compras@valormas.gov.co>

📎 2 archivos adjuntos (234 KB)

Certificado bancario - mayo 2026.pdf, INTRUST SECURITY SAS.pdf;

Cordial saludo,

De conformidad con el cronograma de la presente Convocatoria Abreviada N°012, remito correo por parte del proveedor con las aclaraciones y/o subsanaciones.

Cordialmente;



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 43 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

De: Sergio Mauricio Baron Vera <sbaron@intrustsecurity.co>

Enviado: lunes, 11 de mayo de 2026 15:48

Para: Compras Valor + 2 <compras2@valormas.gov.co>

Cc: Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Sergio Andres Velez Upegui <coordinacion.mesa@valormas.gov.co>

Asunto: Re: Informe de Evaluación Preliminar- Convocatoria Abreviada N°012-2026 - INTRUST SECURITY S.A.S.

Buenas tardes

Amablemente anexamos el certificado bancario.

Cordialmente,

El 11/05/2026, a la(s) 10:08 a.m., Sergio Mauricio Baron Vera <sbaron@intrustsecurity.co> escribió:

Buenos días

Espero que se encuentren muy bien.

Amablemente envió el certificado de antecedentes de persona jurídica ya que desde la personería contestaron el PQR.

Cordialmente,



El dom, 10 may 2026 a la(s) 11:00 a.m., Sergio Mauricio Baron Vera (sbaron@intrustsecurity.co) escribió:

Buenos días

Espero que tengan un excelente día.

Amablemente comparto los documentos para la subsanación de los documentos de la propuesta, solo queda pendiente la certificación bancaria actualizada debido a que por un inconveniente en la app no se pudo generar.

Quedo atento a lo que requieran.

Cordialmente,

12/5/26, 11:17

Correo: Paula Cristina Parra Carmona - Outlook



Sergio M. Barón V.
CEO



+57 3012807037
sbaron@intrustsecurity.co

www.intrustsecurity.co

Medellín, Colombia

Intrust-security

El vie, 8 may 2026 a la(s) 5:30 p.m., Compras Valor + 2 (compras2@valormas.gov.co) escribió:

Cordial saludo,

Adjunto se envía informe de evaluación preliminar, para la Convocatoria Abreviada N°012-2026, cuyo objeto es: ***"Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."***

Quedamos atentos a cualquier inquietud u observación.

Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

[Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,](#)

[Medellín - Colombia](#)

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.



Informe de Documentos para Subsanaciones

Desde Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

Fecha Mar 12/05/2026 16:38

Para Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

CC Sergio Andres Velez Upegui <coordinacion.mesa@valormas.gov.co>

📎 1 archivo adjunto (52 KB)

INFORME DE RESPUESTA TÉCNICA A DOC PRESENTADA POR PROPONENTE VULNERABILIDADES.docx;

Buena tarde, envié documento de validación aprobando las subsanaciones enviadas de los documentos requeridos.

Gracias por su atención.



Carlos Arturo Correa Correa

Profesional Universitario

carlos.correa@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige.
Si el titular de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución
o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos
notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

12/5/26, 11:17

Correo: Paula Cristina Parra Carmona - Outlook



RV: Informe de Evaluación Preliminar- Convocatoria Abreviada N°012-2026 - INTRUST SECURITY S.A.S.

Desde Compras Valor + 2 <compras2@valormas.gov.co>**Fecha** Mar 12/05/2026 10:02**Para** Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>**CC** Compras Valor + <compras@valormas.gov.co>

2 archivos adjuntos (234 KB)

Certificado bancario - mayo 2026.pdf; INTRUST SECURITY SAS.pdf;

Cordial saludo,

De conformidad con el cronograma de la presente Convocatoria Abreviada N°012, remito correo por parte del proveedor con las aclaraciones y/o subsanaciones.

Cordialmente;

**Daniela María López Angulo**

Profesional Universitaria

compras2@valormas.gov.co[Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,](#)[Medellín - Colombia](#)

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

De: Sergio Mauricio Baron Vera <sbaron@intrustsecurity.co>**Enviado:** lunes, 11 de mayo de 2026 15:48**Para:** Compras Valor + 2 <compras2@valormas.gov.co>**Cc:** Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>;

Sergio Andres Velez Upegui <coordinacion.mesa@valormas.gov.co>

Asunto: Re: Informe de Evaluación Preliminar- Convocatoria Abreviada N°012-2026 - INTRUST SECURITY S.A.S.

Buenas tardes

Amablemente anexamos el certificado bancario.

Cordialmente,

El 11/05/2026, a la(s) 10:08 a.m., Sergio Mauricio Baron Vera <sbaron@intrustsecurity.co> escribió:

Buenos días

Espero que se encuentren muy bien.

Amablemente envió el certificado de antecedentes de persona jurídica ya que desde la personería contestaron el PQR.

Cordialmente,



El dom, 10 may 2026 a la(s) 11:00 a.m., Sergio Mauricio Baron Vera (sbaron@intrustsecurity.co) escribió:

Buenos días

Espero que tengan un excelente día.

Amablemente comparto los documentos para la subsanación de los documentos de la propuesta, solo queda pendiente la certificación bancaria actualizada debido a que por un inconveniente en la app no se puedo generar.

Quedo atento a lo que requieran.

Cordialmente,

12/5/26, 11:17

Correo: Paula Cristina Parra Carmona - Outlook



Sergio M. Barón V.
CEO



+57 3012807037
sbaron@intrustsecurity.co
www.intrustsecurity.co
Medellín, Colombia
Intrust-security

El vie, 8 may 2026 a la(s) 5:30 p.m., Compras Valor + 2 (compras2@valormas.gov.co)
escribió:

Cordial saludo,

Adjunto se envía informe de evaluación preliminar, para la Convocatoria Abreviada N°012-2026, cuyo objeto es: ***“Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet.”***

Quedamos atentos a cualquier inquietud u observación.

Gracias.



Daniela María López Angulo

Profesional Universitaria
compras2@valormas.gov.co
[Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Atquejarra,](#)
[Medellín - Colombia](#)

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.



Re: Informe de Evaluación Preliminar- Convocatoria Abreviada N°012-2026 - INTRUST SECURITY S.A.S.

Desde Sergio Mauricio Baron Vera <sbaron@intrustsecurity.co>

Fecha Lun 11/05/2026 8:09

Para Compras Valor + 2 <compras2@valormas.gov.co>

CC Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Sergio Andres Velez Upegui <coordinacion.mesa@valormas.gov.co>

📎 1 archivo adjunto (86 KB)

INTRUST SECURITY SAS.pdf

Buenos días

Espero que se encuentren muy bien.

Amablemente envió el certificado de antecedentes de persona jurídica ya que desde la personería contestaron el PQR.

Cordialmente,



Sergio M. Barón V.
CEO

+57 3012807037
sbaron@intrustsecurity.co

www.intrustsecurity.co

Medellín, Colombia

Intrust-security

El dom, 10 may 2026 a la(s) 11:00 a.m., Sergio Mauricio Baron Vera (sbaron@intrustsecurity.co) escribió:

Buenos días

Espero que tengan un excelente día.

Amablemente comparto los documentos para la subsanación de los documentos de la propuesta, solo queda pendiente la certificación bancaria actualizada debido a que por un inconveniente en la app no se puedo generar.

Quedo atento a lo que requieran.

Cordialmente,



Sergio M. Barón V.
CEO

+57 3012807037
sbaron@intrustsecurity.co

www.intrustsecurity.co

Medellín, Colombia

Intrust-security

El vie, 8 may 2026 a la(s) 5:30 p.m., Compras Valor + 2 (compras2@valormas.gov.co) escribió:
Cordial saludo,

Adjunto se envía informe de evaluación preliminar, para la Convocatoria Abreviada N°012-2026, cuyo objeto es: ***"Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."***

Quedamos atentos a cualquier inquietud u observación.

Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,

Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.



Re: Informe de Evaluación Preliminar- Convocatoria Abreviada N°012-2026 - INTRUST SECURITY S.A.S.

Desde Sergio Mauricio Baron Vera <sbaron@intrustsecurity.co>

Fecha Dom 10/05/2026 9:02

Para Compras Valor + 2 <compras2@valormas.gov.co>

CC Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Sergio Andres Velez Upegui <coordinacion.mesa@valormas.gov.co>

📎 6 archivos adjuntos (2 MB)

CERT-ALTAIR-2026-001_Gestion_Vulnerabilidades.pdf; CERT-GTV-2026-001_Gestion_Tratamiento_Vulnerabilidades.pdf; CERT-VKC-2026-001_VektCore.pdf; 8.Certificacion lavado de activos y financiación del terrorismo_v2.0 (1).pdf; CERT-RT-2026-001_RedTeam_Pentesting.pdf; Certificado_Antecedentes_Persona_Juridica.pdf;

Buenos días

Espero que tengan un excelente día.

Amablemente comparto los documentos para la subsanación de los documentos de la propuesta, solo queda pendiente la certificación bancaria actualizada debido a que por un inconveniente en la app no se puedo generar.

Quedo atento a lo que requieran.

Cordialmente,



Sergio M. Barón V.
CEO

+57 3012807037
sbaron@intrustsecurity.co

www.intrustsecurity.co

Medellín, Colombia

Intrust-security

El vie, 8 may 2026 a la(s) 5:30 p.m., Compras Valor + 2 (compras2@valormas.gov.co) escribió:
Cordial saludo,

Adjunto se envía informe de evaluación preliminar, para la Convocatoria Abreviada N°012-2026, cuyo objeto es: **“Prestación de servicios de vigilancia tecnológica en**

ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."

Quedamos atentos a cualquier inquietud u observación.

Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Aranjuez.

Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

Medellín, 9 de mayo de 2026

A QUIEN PUEDA INTERESAR

Certificación y sustentación técnica de plataforma de Vigilancia Tecnológica (Threat Intelligence)

Yo, **Sergio Mauricio Barón Vera**, identificado con cédula de ciudadanía N.º **91'286.268 de Bucaramanga**, actuando en calidad de Representante Legal de **INTRUST SECURITY S.A.S.**, sociedad identificada con NIT **901380604-6**, registrada en la Cámara de Comercio de Medellín, mediante la presente me permito **CERTIFICAR Y SUSTENTAR** técnicamente lo siguiente:

PRIMERO – IDENTIFICACIÓN DE LA PLATAFORMA

Intrust Security S.A.S. certifica que para la prestación de servicios de Vigilancia Tecnológica (Threat Intelligence) utiliza la plataforma propietaria denominada VektCore, desarrollada internamente por el equipo de ingeniería de la empresa con capacidades nativas de Inteligencia Artificial.

Atributo	Descripción
Nombre comercial	VektCore
Sitio web	https://vektcore.com
Desarrollador / Titular	KorvLabs LLC – Florida, Estados Unidos
Operador comercial LATAM	Intrust Security S.A.S. – Medellín, Colombia
Modelo de servicio	ASM-as-a-Service (SaaS) / Plataforma On-Demand
Tipo de desarrollo	100% propietario – desarrollo interno con Inteligencia Artificial
Motor de IA	Machine Learning para correlación de hallazgos, priorización inteligente de vulnerabilidades, detección de patrones anómalos y generación de recomendaciones automatizadas
Cobertura geográfica	Global, con especialización en LATAM (Colombia, Chile, Ecuador, Perú, Argentina, México)
Sectores objetivo	Financiero, Salud, Energía, Gobierno, Retail, Logística, Educación
Frecuencia de operación	Continuo (24/7) con alertas en tiempo real, o por engagement bajo demanda

SEGUNDO – PROTOCOLO V.E.K.T. (MARCO METODOLÓGICO)

VektCore opera bajo el Protocolo V.E.K.T., marco metodológico propietario que gobierna la ejecución de cada servicio de Attack Surface Management. Las cuatro fases del protocolo son:

V – VISIBILITY (Descubrimiento de superficie)

Descubrimiento automatizado de todos los activos digitales expuestos de la organización. Esta fase construye el inventario completo de la superficie de ataque externa.

- Enumeración de subdominios mediante múltiples motores (subfinder, amass, crt.sh, ChaosDB, SecurityTrails).
- Descubrimiento de direcciones IP, rangos CIDR y registros ASN asociados.
- Identificación de puertos abiertos y servicios expuestos.
- Mapeo de certificados SSL/TLS, fechas de expiración y cadenas de confianza.
- Descubrimiento de activos cloud mal configurados (buckets S3, Azure Blobs, GCP Storage).
- Detección de Shadow IT: activos no inventariados vinculados al dominio raíz.

E – EXPOSURE (Análisis de exposición)

Fingerprinting y análisis de tecnologías, configuraciones y metadatos expuestos para determinar el nivel de exposición real.

- Fingerprinting de tecnologías web: CMS, frameworks, servidores (Apache, Nginx, IIS).
- Identificación de versiones de software y correlación con CVE/NVD.
- Análisis de encabezados de seguridad HTTP (HSTS, CSP, X-Frame-Options).
- Detección de paneles de administración, APIs expuestas y endpoints no documentados.
- Identificación de configuraciones por defecto y archivos sensibles accesibles.
- Evaluación de políticas DNS: SPF, DKIM, DMARC.

K – KNOWLEDGE (Evaluación de vulnerabilidades)

Evaluación activa de vulnerabilidades utilizando motores de escaneo automatizados y bases de datos de amenazas actualizadas.

- Evaluación mediante plantillas Nuclei: CVEs conocidos, misconfigs, credenciales por defecto, exposiciones sensibles.
- Correlación automática con CVE/NVD, Exploit-DB y advisories de fabricantes.
- Detección de credenciales filtradas en Dark Web, foros clandestinos, Telegram y repositorios públicos.
- Análisis de vulnerabilidades web según OWASP Top 10.
- Identificación de exposición de ejecutivos y personal clave mediante OSINT.
- Monitoreo de menciones de la organización en Dark Web y mercados clandestinos.

T – TRIAGE (Priorización inteligente con IA)

Análisis asistido por Inteligencia Artificial para priorización, contextualización de riesgos y generación de recomendaciones accionables.

- Priorización basada en scoring contextual: severidad CVSS + explotabilidad activa + impacto de negocio.
- Correlación de hallazgos múltiples para identificar cadenas de ataque (attack chains).
- Generación automatizada de reportes ejecutivos y técnicos.
- Mapeo contra MITRE ATT&CK, OWASP y NIST CSF.
- Recomendaciones de remediación contextualizadas por sector y región.
- Dashboard interactivo con KRIs y tendencias de superficie de ataque.
- Alertas proactivas en tiempo real ante nuevas exposiciones críticas.

TERCERO – MÓDULOS FUNCIONALES (V-SUITE)

Complementando el Protocolo V.E.K.T., VektCore dispone de una suite de módulos funcionales especializados que amplían las capacidades hacia dominios específicos de la ciberseguridad corporativa:

Módulo	Descripción y alcance	Framework
V-THREAT	Detección y correlación de amenazas en tiempo real (SIEM-lite). Análisis de logs, eventos y alertas priorizadas por severidad e impacto. Monitoreo de IOCs y patrones de ataque activos.	MITRE ATT&CK
V-RISK	Gestión continua de riesgos. Inventario automatizado de activos, valoración cuantitativa y cualitativa de riesgos, planes de tratamiento con seguimiento.	ISO 27005 / NIST RMF
V-COMPLY	Panel de cumplimiento normativo. Evaluación automatizada de brechas contra estándares internacionales y regulaciones locales. Generación de evidencia para auditorías.	ISO 27001 / NIST CSF / Ley 1581
V-PHISH	Simulación de phishing y formación de usuarios. Campañas automatizadas con plantillas personalizables, métricas de concienciación y seguimiento por área.	NIST SP 800-50
V-SCAN	Escaneo automatizado de vulnerabilidades de infraestructura y aplicaciones web. Integración con CVE/NVD para clasificación por criticidad.	OWASP / CVE / CVSS
V-REPORT	Generación automatizada de informes ejecutivos y técnicos para juntas directivas, comités de riesgo, auditorías y reguladores.	ISO 27001 Annex

CUARTO – FUENTES DE INTELIGENCIA Y COBERTURA

VektCore integra las siguientes categorías de fuentes para garantizar cobertura integral de inteligencia de amenazas:

Categoría	Detalle de cobertura
OSINT	Registros DNS, WHOIS, certificados SSL, repositorios públicos, redes sociales, Google Dorks
Dark Web / Deep Web	Foros clandestinos, mercados Tor/I2P, canales Telegram, paste sites (Pastebin, GitHub Gists)
Feeds de amenazas	Integración con feeds STIX/TAXII para correlación automatizada de IOCs
Bases de vulnerabilidades	CVE/NVD (NIST), Exploit-DB, advisories de fabricantes, Nuclei Templates Community
HUMINT digital	Exposición de ejecutivos y personal clave, perfilado de actores de amenaza regionales
Entregables	Dashboard interactivo, reportes PDF/DOCX, alertas por correo, integración API REST

QUINTO – ALINEACIÓN CON MARCOS DE REFERENCIA

La plataforma VektCore está alineada con los siguientes marcos de referencia internacionales:

Marco / Normativa	Aplicación en VektCore
ISO/IEC 27001:2022	Control A.5.7 – Threat Intelligence: vigilancia y gestión de inteligencia de amenazas
ISO/IEC 27032:2023	Directrices de seguridad en el ciberespacio y protección de activos digitales
ISO/IEC 23894:2023	Gestión de riesgos de Inteligencia Artificial aplicada a los motores de IA de VektCore
NIST CSF 2.0	Funciones Identify (ID.AM, ID.RA), Protect (PR.DS), Detect (DE.CM, DE.AE)
MITRE ATT&CK	Taxonomía de TTPs para clasificación de hallazgos y actores de amenaza
OWASP Top 10	Clasificación de vulnerabilidades web en superficie de ataque
ISO 31000:2018	Marco de gestión de riesgos aplicado a la priorización de hallazgos

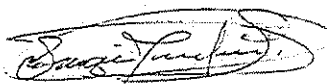
SEXTO – JUSTIFICACIÓN DEL DESARROLLO PROPIO

La decisión de desarrollar VektCore como plataforma propietaria con Inteligencia Artificial nativa responde a los siguientes criterios:

- Independencia tecnológica: eliminación de dependencia de proveedores internacionales de ASM, reduciendo costos de licenciamiento, restricciones funcionales y riesgos de disponibilidad.
- Contextualización regional: VektCore incorpora conocimiento del panorama de amenazas en América Latina, incluyendo actores de amenaza locales, regulaciones de protección de datos regionales (Ley 1581/2012, LGPD Brasil) y vectores de ataque prevalentes en sectores críticos de la región.
- Inteligencia Artificial nativa: los motores de ML/NLP fueron concebidos desde la arquitectura fundacional de la plataforma, no como características agregadas, permitiendo correlación, priorización y generación de inteligencia con velocidad y precisión superiores al procesamiento manual.
- Evolución continua: al ser propietaria, VektCore evoluciona al ritmo de las necesidades de los clientes y del panorama de amenazas, sin depender de roadmaps ni ciclos de release de fabricantes externos.
- Propiedad intelectual: todo el código fuente, modelos de IA y datos generados son propiedad exclusiva de KorvLabs LLC / Intrust Security S.A.S., garantizando control total sobre la tecnología.

La presente certificación y sustentación técnica se expide en cumplimiento de los requisitos establecidos en el proceso de evaluación, y la información contenida en este documento es veraz y verificable mediante demostración técnica de la plataforma y acceso al sitio web <https://vektcore.com>.

Se expide a los nueve (9) días del mes de mayo de 2026, en la ciudad de Medellín, Colombia.



Sergio Mauricio Barón Vera

Representante Legal

Intrust Security S.A.S.

NIT: 901380604-6

CC: 91'286.268 de Bucaramanga

Medellín, 9 de mayo de 2026

A QUIEN PUEDA INTERESAR

Certificación de aplicación de estándares y buenas prácticas en Gestión de Vulnerabilidades

(CVSS, OWASP, NIST SP 800-115, MITRE ATT&CK)

Yo, **Sergio Mauricio Barón Vera**, identificado con cédula de ciudadanía N.º **91'286.268 de Bucaramanga**, actuando en calidad de Representante Legal de **INTRUST SECURITY S.A.S.**, sociedad identificada con NIT **901380604-6**, registrada en la Cámara de Comercio de Medellín, mediante la presente me permito **CERTIFICAR** lo siguiente:

PRIMERO – APLICACIÓN DE ESTÁNDARES EN GESTIÓN DE VULNERABILIDADES

Intrust Security S.A.S., en el ejercicio de sus servicios profesionales de ciberseguridad, aplica de manera sistemática los siguientes estándares y marcos de referencia internacionales en todos sus procesos de identificación, evaluación, priorización, remediación y seguimiento de vulnerabilidades:

Estándar / Marco	Descripción	Aplicación en Intrust Security
CVSS (Common Vulnerability Scoring System)	Sistema estándar de la industria para evaluar la severidad de las vulnerabilidades de seguridad informática mediante una puntuación numérica de 0.0 a 10.0, mantenido por el FIRST (Forum of Incident Response and Security Teams).	Todas las vulnerabilidades identificadas son clasificadas utilizando CVSS v3.1 como sistema de scoring primario. La priorización de remediación se establece según los rangos.
OWASP (Open Worldwide Application Security Project)	Proyecto de código abierto dedicado a mejorar la seguridad del software. Su marco de referencia OWASP Top 10 establece las categorías de vulnerabilidades más críticas en aplicaciones web.	Las evaluaciones de seguridad de aplicaciones web siguen la metodología OWASP Testing Guide (OTG) v4.2 y clasifican hallazgos conforme al OWASP Top 10 (versión 2021).
NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment)	Guía técnica del Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos que establece las directrices para la planificación, ejecución y reporte de evaluaciones de seguridad de la información.	Las evaluaciones técnicas de seguridad (pentesting, análisis de vulnerabilidades, auditorías) se ejecutan conforme a las fases definidas por NIST.
MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)	Base de conocimiento mantenida por MITRE Corporation que documenta las tácticas, técnicas y procedimientos (TTPs) utilizados por actores de amenaza reales, organizada en matrices por plataforma.	Los hallazgos de seguridad se mapean contra la matriz MITRE ATT&CK para Enterprise, identificando las técnicas específicas (T-ID) explotadas o explotables, lo que permite contextualizar el riesgo frente a amenazas reales y documentadas.

SEGUNDO – PLATAFORMA ALTAIR PARA GESTIÓN Y SEGUIMIENTO DE VULNERABILIDADES

Para garantizar la trazabilidad, seguimiento y cierre efectivo de las vulnerabilidades identificadas, Intrust Security S.A.S. ha desarrollado internamente la plataforma propietaria denominada ALTAIR, la cual constituye el eje central del ciclo de vida de gestión de vulnerabilidades de todos nuestros servicios.

Atributo	Descripción
Nombre comercial	ALTAIR
Desarrollador	Intrust Security S.A.S. – Medellín, Colombia
Tipo de desarrollo	100% propietario – desarrollo interno con Inteligencia Artificial
Propósito	Gestión integral del ciclo de vida de vulnerabilidades: registro, evidencia, seguimiento, remediación, retest y cierre
Usuarios	Equipo técnico de Intrust Security (carga de hallazgos) y clientes (gestión de remediación y evidencia de cierre)
Modelo de acceso	Plataforma web con acceso controlado por cliente mediante credenciales individuales

TERCERO – CICLO DE VIDA DE GESTIÓN DE VULNERABILIDADES EN ALTAIR

ALTAIR implementa un ciclo de vida completo y automatizado de gestión de vulnerabilidades que integra los estándares CVSS, OWASP, NIST SP 800-115 y MITRE ATT&CK en cada una de sus fases:

CUARTO – INTEGRACIÓN DE ESTÁNDARES EN ALTAIR

La plataforma ALTAIR integra de manera nativa los cuatro estándares y marcos de referencia requeridos en el proceso de evaluación, conforme al siguiente detalle:

Estándar	Integración en ALTAIR
CVSS v3.1	Cada hallazgo registrado incluye obligatoriamente su vector CVSS y puntuación numérica. ALTAIR utiliza el score CVSS como criterio primario de priorización, estableciendo plazos máximos de remediación diferenciados por severidad: Crítico (72 horas), Alto (7 días), Medio (30 días), Bajo (90 días).
OWASP	Los hallazgos de aplicaciones web son categorizados conforme al OWASP Top 10 (2021). ALTAIR presenta la categoría OWASP asociada a cada hallazgo, facilitando al cliente la comprensión del tipo de vulnerabilidad y su contexto dentro de los riesgos más prevalentes en aplicaciones web.
NIST SP 800-115	El flujo operativo de ALTAIR está alineado con las fases de NIST SP 800-115: Planificación (definición de alcance), Descubrimiento (reconocimiento y enumeración), Ataque (explotación controlada) y Reporte (documentación de hallazgos). Cada hallazgo referencia la fase en la que fue identificado.
MITRE ATT&CK	ALTAIR mapea cada hallazgo contra la matriz MITRE ATT&CK para Enterprise, asociando la(s) técnica(s) específica(s) (identificador T-ID), la táctica correspondiente y, cuando es posible, el grupo de amenaza (G-ID) que utiliza dicha técnica. Esto contextualiza el hallazgo frente a amenazas reales documentadas.

QUINTO – BENEFICIOS DE ALTAIR PARA EL CLIENTE

La utilización de ALTAIR como plataforma de gestión de vulnerabilidades proporciona al cliente los siguientes beneficios:

- Trazabilidad completa del ciclo de vida de cada vulnerabilidad, desde su identificación hasta su cierre verificado.
- Evidencia documentada de las acciones de remediación para fines de auditoría, cumplimiento normativo y gobierno corporativo.
- Automatización de alertas de retest, eliminando el riesgo de que vulnerabilidades remediadas queden sin verificación.
- Priorización objetiva basada en CVSS, asegurando que los recursos se concentren en las vulnerabilidades de mayor impacto.
- Contextualización de riesgos mediante MITRE ATT&CK, permitiendo entender cómo cada vulnerabilidad podría ser explotada por actores de amenaza reales.
- Métricas de gestión: tiempo medio de remediación (MTTR), porcentaje de cierre, tendencias de vulnerabilidades por categoría y severidad.
- Cumplimiento demostrable de estándares internacionales.

SEXTO – ALINEACIÓN CON MARCOS DE REFERENCIA COMPLEMENTARIOS

Además de los cuatro estándares principales objeto de esta certificación, la metodología de gestión de vulnerabilidades de Intrust Security y la plataforma ALTAIR se alinean con los siguientes marcos complementarios:

Marco	Aplicación
ISO/IEC 27001:2022	Controles A.8.8 (Gestión de vulnerabilidades técnicas) y A.5.7 (Threat Intelligence)
ISO/IEC 27002:2022	Control 8.8 – Directrices para la identificación, evaluación y tratamiento de vulnerabilidades técnicas
NIST CSF 2.0	Funciones Identify (ID.RA – Risk Assessment) y Detect (DE.CM – Continuous Monitoring)
PTES (Penetration Testing Execution Standard)	Estándar de ejecución de pruebas de penetración, aplicado en la fase de evaluación previa al registro en ALTAIR
OSSTMM	Metodología de pruebas de seguridad de código abierto, utilizada como referencia complementaria en evaluaciones de infraestructura

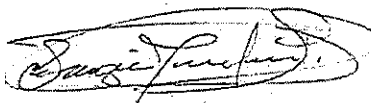
SÉPTIMO – DECLARACIÓN

En virtud de lo expuesto, certifico que Intrust Security S.A.S.:

- Aplica de manera sistemática y documentada los estándares CVSS v3.1, OWASP Top 10, NIST SP 800-115 y MITRE ATT&CK en todos sus servicios de evaluación de seguridad y gestión de vulnerabilidades.
- Dispone de la plataforma propietaria ALTAIR como herramienta tecnológica para la gestión, seguimiento, remediación y cierre verificado de vulnerabilidades, integrando nativamente los cuatro estándares mencionados.
- Garantiza la trazabilidad completa del ciclo de vida de cada vulnerabilidad, incluyendo evidencias técnicas, acciones de remediación, verificación de cierre y métricas de gestión.
- La información contenida en esta certificación es veraz y verificable mediante demostración técnica de la plataforma ALTAIR.

La presente certificación se expide en cumplimiento de los requisitos establecidos en el proceso de evaluación y a solicitud de la entidad interesada.

Se expide a los nueve (9) días del mes de mayo de 2026, en la ciudad de Medellín, Colombia.



Sergio Mauricio Barón Vera

Representante Legal

Intrust Security S.A.S.

NIT: 901380604-6

CC: 91'286.268 de Bucaramanga

Medellín, 9 de mayo de 2026

A QUIEN PUEDA INTERESAR

Certificación de cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad en Gestión y Tratamiento de Vulnerabilidades

Yo, **Sergio Mauricio Barón Vera**, identificado con cédula de ciudadanía N.º **91'286.268 de Bucaramanga**, actuando en calidad de Representante Legal de **INTRUST SECURITY S.A.S.**, sociedad identificada con NIT **901380604-6**, registrada en la Cámara de Comercio de Medellín, mediante la presente me permito **CERTIFICAR** que Intrust Security S.A.S. cumple a cabalidad con los estándares técnicos, normativos y buenas prácticas de ciberseguridad que se detallan a continuación, aplicados de manera integral en todos sus servicios de gestión y tratamiento de vulnerabilidades:

PRIMERO – ISO/IEC 27001:2022 (Sistema de Gestión de Seguridad de la Información)

Intrust Security S.A.S. ejecuta sus servicios de gestión y tratamiento de vulnerabilidades alineados con los requisitos y controles del estándar internacional ISO/IEC 27001:2022. El CEO y Co-Fundador de la empresa cuenta con la certificación ISO 27001 Lead Implementer, lo que garantiza el conocimiento profundo y la aplicación rigurosa de este marco normativo.

Control	Denominación	Aplicación en los servicios de Intrust Security
A.5.7	Threat Intelligence	Recolección, análisis y uso de inteligencia de amenazas para identificar vulnerabilidades en contexto de amenazas reales. Utilización de la plataforma propietaria VektCore para vigilancia tecnológica continua.
A.8.8	Gestión de vulnerabilidades técnicas	Identificación, evaluación, priorización y tratamiento sistemático de vulnerabilidades. Registro, seguimiento y cierre verificado a través de la plataforma propietaria ALTAIR.
A.8.9	Gestión de configuración	Evaluación de configuraciones de seguridad en infraestructura, servidores, aplicaciones y dispositivos de red como parte integral del análisis de vulnerabilidades.
A.8.25	Ciclo de vida de desarrollo seguro	Evaluación de seguridad en aplicaciones siguiendo prácticas de desarrollo seguro, incluyendo revisión de código y pruebas de seguridad en aplicaciones web y móviles.
A.8.28	Codificación segura	Verificación de prácticas de codificación segura durante las evaluaciones de seguridad de aplicaciones, identificando vulnerabilidades derivadas de deficiencias en el código.
A.5.23	Seguridad de la información para uso de servicios en la nube	Evaluación de configuraciones de seguridad en entornos cloud (AWS, Azure, GCP) como parte del análisis de superficie de ataque y vulnerabilidades.



Adicionalmente, Intrust Security opera bajo los principios de confidencialidad, integridad y disponibilidad que rigen el estándar ISO 27001, suscribiendo acuerdos de confidencialidad con todo el personal asignado y cumpliendo las políticas de seguridad de la información de cada cliente.

SEGUNDO – NIST (National Institute of Standards and Technology)

Intrust Security S.A.S. aplica los siguientes marcos y publicaciones del NIST en sus procesos de gestión y tratamiento de vulnerabilidades:

Publicación NIST	Aplicación en los servicios de Intrust Security
NIST SP 800-115 (Technical Guide to Information Security Testing)	Guía que estructura la ejecución de las evaluaciones técnicas de seguridad en cuatro fases: Planificación, Descubrimiento y Reporte.
NIST SP 800-30 Rev. 1 (Guide for Conducting Risk Assessments)	Marco de evaluación de riesgos que se aplica para contextualizar las vulnerabilidades identificadas dentro del perfil de riesgo de la organización, considerando la probabilidad de explotación, el impacto potencial y los controles existentes.
NIST SP 800-53 Rev. 5 (Security and Privacy Controls)	Catálogo de controles de seguridad y privacidad utilizado como referencia para las recomendaciones de remediación. Los hallazgos se asocian a los controles NIST correspondientes, facilitando la alineación del cliente con este marco regulatorio.
NIST CSF 2.0 (Cybersecurity Framework)	Marco de ciberseguridad cuyas funciones Govern, Identify, Protect, Detect, Respond y Recover orientan la estructura de los servicios. La gestión de vulnerabilidades se enmarca en las funciones Identify (ID.RA – Risk Assessment, ID.AM – Asset Management) y Detect (DE.CM – Continuous Monitoring).
NIST SP 800-40 Rev. 4 (Guide to Enterprise Patch Management)	Guía de gestión de parches que orienta las recomendaciones de remediación entregadas al cliente, priorizando la aplicación de parches críticos según ventanas de exposición y criticidad del activo afectado.

TERCERO – MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

Intrust Security S.A.S. integra el framework MITRE ATT&CK como pieza fundamental en la contextualización y comunicación de los hallazgos de seguridad. La aplicación de este marco se materializa en los siguientes aspectos:

- Mapeo de hallazgos contra la matriz MITRE ATT&CK para Enterprise (Windows, Linux, macOS, Cloud, Network, Containers), identificando la(s) técnica(s) específica(s) asociadas a cada vulnerabilidad mediante su identificador oficial (T-ID).
- Identificación de la táctica correspondiente dentro de la cadena de ataque (Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact).
- Asociación con grupos de amenaza documentados (G-ID) cuando la técnica identificada es utilizada por actores de amenaza conocidos con actividad relevante para el sector o la región del cliente.
- Contextualización del riesgo: al mapear vulnerabilidades contra técnicas reales de adversarios, el cliente comprende no solo la debilidad técnica, sino cómo podría ser explotada en un ataque real y por qué actores.
- Priorización basada en amenazas: las vulnerabilidades asociadas a técnicas activamente explotadas por grupos de amenaza con interés en el sector del cliente reciben mayor prioridad de remediación.
- Reportes técnicos que incluyen la referencia MITRE ATT&CK para cada hallazgo, permitiendo al equipo de seguridad del cliente correlacionar con sus propias capacidades de detección y respuesta.

CUARTO – OWASP (Open Worldwide Application Security Project)

Intrust Security S.A.S. aplica los siguientes recursos y metodologías del proyecto OWASP en la evaluación de seguridad de aplicaciones web, móviles y APIs:

Recurso OWASP	Aplicación
OWASP Top 10 (2021)	Clasificación de todas las vulnerabilidades web identificadas conforme a las diez categorías de riesgo más críticas: A01-Broken Access Control, A02-Cryptographic Failures, A03-Injection, A04-Insecure Design, A05-Security Misconfiguration, A06-Vulnerable and Outdated Components, A07-Identification and Authentication Failures, A08-Software and Data Integrity Failures, A09-Security Logging and Monitoring Failures, A10-Server-Side Request Forgery.
OWASP Testing Guide (OTG) v4.2	Metodología de ejecución de pruebas de seguridad en aplicaciones web que estructura las evaluaciones en categorías de prueba: gestión de identidades, autenticación, autorización, gestión de sesiones, validación de entrada, manejo de errores, criptografía y lógica de negocio.
OWASP ASVS (Application Security Verification Standard)	Estándar de verificación de seguridad de aplicaciones utilizado como lista de controles para evaluaciones profundas de seguridad en aplicaciones críticas, cubriendo los tres niveles de verificación según la criticidad de la aplicación.
OWASP Mobile Top 10	Clasificación de riesgos para aplicaciones móviles, aplicada cuando el alcance del servicio incluye la evaluación de aplicaciones en plataformas Android e iOS.
OWASP API Security Top 10	Marco de referencia para la evaluación de seguridad de APIs REST y GraphQL, identificando vulnerabilidades específicas de interfaces de programación de aplicaciones.

QUINTO – METODOLOGÍA INTEGRAL DE GESTIÓN Y TRATAMIENTO DE VULNERABILIDADES

Intrust Security S.A.S. integra los cuatro estándares y marcos anteriores en una metodología unificada de gestión y tratamiento de vulnerabilidades, cuyo ciclo de vida se ejecuta en las siguientes fases:

Fase 1 – Planificación y alcance

Definición del alcance, reglas de engagement, activos objetivo y autorizaciones, conforme a NIST SP 800-115. Identificación de los marcos normativos aplicables al cliente (ISO 27001, regulaciones sectoriales) para contextualizar las recomendaciones.

Fase 2 – Descubrimiento y evaluación

Ejecución de reconocimiento, enumeración y evaluación de vulnerabilidades siguiendo NIST SP 800-115, con clasificación OWASP para aplicaciones web y pruebas estructuradas conforme al OWASP Testing Guide. Utilización de VektCore para el descubrimiento de superficie de ataque.

Fase 3 – Explotación controlada

Cuando el alcance contractual lo autoriza, se ejecutan pruebas de explotación controlada para validar la criticidad real de las vulnerabilidades y documentar cadenas de ataque, mapeando cada técnica utilizada contra la matriz MITRE ATT&CK.

Fase 4 – Clasificación y priorización

Cada hallazgo se clasifica utilizando CVSS v3.1 como métrica de severidad, se categoriza según OWASP Top 10 (cuando aplica), se mapea contra MITRE ATT&CK y se contextualiza dentro del perfil de riesgo del cliente conforme a NIST SP 800-30.

Fase 5 – Registro en ALTAIR y remediación

Todos los hallazgos se registran en la plataforma propietaria ALTAIR con su documentación completa (evidencias, clasificación, mapeo de frameworks, recomendaciones). El cliente gestiona la remediación desde ALTAIR, registrando evidencia de las correcciones implementadas. Las recomendaciones de remediación referencian controles ISO 27001 y NIST SP 800-53.

Fase 6 – Verificación (retest) y cierre

ALTAIR genera alertas automáticas de retest cuando el cliente marca hallazgos como remediados. El equipo de Intrust Security ejecuta la verificación técnica y documenta el cierre o la persistencia de cada vulnerabilidad, garantizando trazabilidad completa del ciclo de vida.

SEXTO – HERRAMIENTAS TECNOLÓGICAS PROPIETARIAS

Para soportar tecnológicamente la aplicación de los estándares certificados, Intrust Security S.A.S. ha desarrollado internamente las siguientes plataformas con capacidades de Inteligencia Artificial:

Plataforma	Función principal	Estándares integrados
VektCore ASM	Vigilancia Tecnológica y Attack Surface Management. Descubrimiento continuo de activos expuestos, evaluación de vulnerabilidades y Threat Intelligence operacional.	MITRE ATT&CK, OWASP, NIST CSF, ISO 27001 (A.5.7)
ALTAIR	Gestión del ciclo de vida de vulnerabilidades. Registro, seguimiento, remediación, retest automatizado y cierre verificado con trazabilidad completa.	CVSS v3.1, OWASP Top 10, NIST SP 800-115, MITRE ATT&CK, ISO 27001 (A.8.8)

SÉPTIMO – CERTIFICACIONES PROFESIONALES DEL EQUIPO

El equipo directivo y técnico de Intrust Security S.A.S. cuenta con certificaciones profesionales que respaldan la competencia en la aplicación de los estándares mencionados:

- ISO 27001 Lead Implementer: certificación que acredita la competencia para implementar, mantener y auditar Sistemas de Gestión de Seguridad de la Información conforme a ISO/IEC 27001.
- ISO 27032 Lead Cybersecurity Manager: certificación que acredita la competencia en la gestión de programas de ciberseguridad conforme al estándar ISO/IEC 27032.
- PMP (Project Management Professional): certificación del PMI que garantiza la gestión profesional de los proyectos de ciberseguridad conforme a estándares internacionales de dirección de proyectos.
- El personal técnico asignado a los servicios cuenta con formación y certificaciones en seguridad ofensiva y defensiva (CEH, OSCP, CISA, CISSP y/o equivalentes), según el perfil de cada profesional.

OCTAVO – DECLARACIÓN

En virtud de lo expuesto, certifico que Intrust Security S.A.S.:

- Cumple a cabalidad con los estándares técnicos, normativos y buenas prácticas de ciberseguridad ISO/IEC 27001, NIST (SP 800-115, SP 800-30, SP 800-53, CSF 2.0), MITRE ATT&CK y OWASP (Top 10, Testing Guide, ASVS) en todos sus servicios de gestión y tratamiento de vulnerabilidades.
- Dispone de las plataformas propietarias VektCore y ALTAIR como herramientas tecnológicas que integran nativamente dichos estándares en la ejecución operativa de los servicios.



- Cuenta con equipo profesional certificado en los marcos de referencia aplicables.
- Garantiza la trazabilidad completa del ciclo de vida de cada vulnerabilidad, desde su identificación hasta su cierre verificado, con evidencias documentadas para fines de auditoría y cumplimiento.

La presente certificación se expide en cumplimiento de los requisitos establecidos en el proceso de evaluación y a solicitud de la entidad interesada. La información aquí contenida es veraz y verificable mediante demostración técnica de las plataformas y presentación de las certificaciones profesionales referenciadas.

Se expide a los nueve (9) días del mes de mayo de 2026, en la ciudad de Medellín, Colombia.

A handwritten signature in black ink, appearing to read "Sergio Mauricio Barón Vera", enclosed within an oval-shaped stamp.

Sergio Mauricio Barón Vera

Representante Legal

Intrust Security S.A.S.

NIT: 901380604-6

CC: 91'286.268 de Bucaramanga

Medellín, 9 de mayo de 2026

A QUIEN PUEDA INTERESAR

Certificación de alcance de actividades de Red Team, Pruebas de Penetración, Threat Hunting y Adversary Emulation

Yo, **Sergio Mauricio Barón Vera**, identificado con cédula de ciudadanía N.º **91'286.268** de **Bucaramanga**, actuando en calidad de Representante Legal de **INTRUST SECURITY S.A.S.**, sociedad identificada con NIT **901380604-6**, registrada en la Cámara de Comercio de Medellín, mediante la presente me permito **CERTIFICAR Y PRECISAR** el alcance de las actividades de seguridad ofensiva que Intrust Security ejecuta en el desarrollo de sus servicios de ciberseguridad, conforme a lo siguiente:

PRIMERO – CONFIRMACIÓN DE ACTIVIDADES

Intrust Security S.A.S. confirma que en el desarrollo del objeto contractual ejecuta la totalidad de las siguientes actividades de seguridad ofensiva:

Actividad	Se ejecuta	Descripción del alcance
Pruebas de Penetración (Caja Negra)	Sí	Evaluación de seguridad sin información previa del entorno objetivo. Se ejecuta como primera fase de toda evaluación, simulando un atacante externo sin conocimiento interno de la organización.
Pruebas de Penetración (Caja Gris)	Sí	Evaluación con credenciales y contextualización proporcionada por el cliente. Se ejecuta como segunda fase, posterior a la caja negra, permitiendo profundizar en vectores de ataque internos y validar controles de acceso.
Threat Hunting	Sí	Búsqueda proactiva de amenazas activas o latentes dentro de la infraestructura del cliente, utilizando hipótesis basadas en inteligencia de amenazas y análisis de comportamiento anómalo.
Adversary Emulation	Sí	Simulación de las tácticas, técnicas y procedimientos (TTPs) de actores de amenaza reales y documentados, utilizando la matriz MITRE ATT&CK como referencia para replicar escenarios de ataque específicos del sector del cliente.
Red Teaming	Sí	Ejercicio integral de seguridad ofensiva que combina pruebas de penetración, ingeniería social, acceso físico (cuando aplica) y explotación de vulnerabilidades técnicas para evaluar la capacidad real de detección y respuesta de la organización frente a un adversario sofisticado.

SEGUNDO – MODELO SECUENCIAL DE EJECUCIÓN: CAJA NEGRA + CAJA GRIS

Intrust Security S.A.S. aplica un modelo de ejecución secuencial en dos fases para todas las pruebas de penetración, el cual maximiza la cobertura de la evaluación y permite identificar vulnerabilidades tanto desde la perspectiva de un atacante externo como desde la de un usuario con acceso autorizado:

Fase 1 – Prueba de penetración en Caja Negra (Black Box)

Se ejecuta en primer lugar, sin ningún tipo de información previa proporcionada por el cliente. El equipo de Intrust Security actúa como un atacante externo que desconoce por completo la infraestructura, aplicaciones y configuraciones del objetivo. Esta fase permite:

- Evaluar la superficie de ataque real tal como la percibiría un adversario externo.
- Identificar vulnerabilidades explotables sin conocimiento previo del entorno.
- Validar la efectividad de los controles perimetrales, WAFs, firewalls y mecanismos de detección.
- Descubrir activos expuestos, servicios no documentados y configuraciones erróneas visibles desde internet.
- Documentar las rutas de ataque viables desde la perspectiva de un adversario no autenticado.

Fase 2 – Prueba de penetración en Caja Gris (Gray Box)

Una vez completada la fase de caja negra, el cliente proporciona credenciales de acceso y contextualización técnica (diagramas de red, inventario de activos, roles de usuario) para la ejecución de la segunda fase. Esta modalidad permite:

- Profundizar en vectores de ataque que requieren autenticación para su explotación.
- Evaluar controles de autorización, segregación de funciones y escalamiento de privilegios.
- Validar la seguridad de funcionalidades internas, paneles de administración y APIs protegidas.
- Identificar vulnerabilidades de lógica de negocio que solo son detectables con acceso autenticado.
- Evaluar la seguridad de la comunicación entre componentes internos y la protección de datos en tránsito y en reposo.
- Comparar los hallazgos de ambas fases para construir un mapa completo de riesgos.

Este modelo secuencial de dos fases se aplica de manera estándar a todos los clientes de Intrust Security, garantizando una evaluación integral que cubre tanto la perspectiva externa (caja negra) como la interna con contexto (caja gris).

TERCERO – THREAT HUNTING

Las actividades de Threat Hunting ejecutadas por Intrust Security consisten en la búsqueda proactiva e iterativa de amenazas que hayan evadido los controles de seguridad existentes del cliente. A diferencia de la detección reactiva (alertas de SIEM/IDS), el Threat Hunting parte de hipótesis formuladas por el equipo de analistas y se ejecuta conforme al siguiente enfoque:

- Formulación de hipótesis basadas en inteligencia de amenazas, indicadores de compromiso (IOCs) y TTPs de actores de amenaza relevantes para el sector del cliente.
- Análisis de logs, telemetría de red, eventos de endpoints y registros de autenticación en busca de patrones anómalos o indicadores de actividad maliciosa.
- Correlación de eventos mediante técnicas de análisis de datos para identificar movimientos laterales, persistencia, exfiltración de datos y otras técnicas de post-explotación.
- Validación o descarte de hipótesis con documentación de hallazgos y recomendaciones de contención cuando se confirma actividad maliciosa.
- Mejora continua de las capacidades de detección del cliente, proponiendo nuevas reglas de correlación, alertas y casos de uso para el SIEM/EDR basados en los resultados del Threat Hunting.

Los ejercicios de Threat Hunting se mapean contra la matriz MITRE ATT&CK, cubriendo las tácticas de mayor interés según el perfil de riesgo del cliente: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control y Exfiltration.

CUARTO – ADVERSARY EMULATION

La Adversary Emulation (Emulación de Adversarios) es una actividad avanzada de seguridad ofensiva en la que el equipo de Intrust Security replica las tácticas, técnicas y procedimientos (TTPs) de actores de amenaza reales documentados en la base de conocimiento MITRE ATT&CK. El objetivo es evaluar la capacidad de la organización para detectar, contener y responder ante un ataque que siga los patrones de un adversario específico.

Proceso de ejecución:

- Selección del adversario: se identifica el actor de amenaza (APT o grupo criminal) más relevante para el sector, región geográfica y perfil de riesgo del cliente, con base en inteligencia de amenazas actualizada.
- Diseño del plan de emulación: se construye un plan de ataque que replica las TTPs documentadas del adversario seleccionado, mapeando cada paso contra la matriz MITRE ATT&CK (Técnicas T-ID específicas).
- Ejecución controlada: el equipo ejecuta el plan de emulación en el entorno real del cliente, documentando cada paso, las herramientas utilizadas, los resultados obtenidos y los controles que fueron evadidos o que detectaron la actividad.
- Evaluación de capacidades de detección: se analiza cuáles técnicas del adversario fueron detectadas por los controles existentes (SIEM, EDR, IDS/IPS, SOC) y cuáles pasaron desapercibidas.
- Reporte y recomendaciones: se entrega un informe detallado con el mapeo ATT&CK del ejercicio, las brechas de detección identificadas y recomendaciones priorizadas para cerrar dichas brechas.

QUINTO – RED TEAMING

Los ejercicios de Red Teaming constituyen la evaluación de seguridad ofensiva más completa e integral que ejecuta Intrust Security. A diferencia de las pruebas de penetración convencionales, el Red Teaming evalúa la postura de seguridad global de la organización, incluyendo personas, procesos y tecnología, con el objetivo de medir la capacidad real de detección y respuesta ante un adversario sofisticado y persistente.

Componentes del ejercicio de Red Teaming:

Componente	Descripción
Penetración técnica	Explotación de vulnerabilidades en infraestructura, aplicaciones, servicios de red y entornos cloud, combinando técnicas de caja negra y caja gris.
Ingeniería social	Campañas de phishing dirigido (spear phishing), vishing (llamadas telefónicas), smishing (mensajes de texto) y pretexting para evaluar la concienciación del personal y la efectividad de los controles anti-phishing.
Acceso físico	Cuando el alcance contractual lo contempla, se ejecutan pruebas de acceso físico a instalaciones, evaluando controles de acceso, vigilancia y seguridad perimetral.
Movimiento lateral	Una vez obtenido acceso inicial, se ejecutan técnicas de post-explotación para escalar privilegios, moverse lateralmente y alcanzar activos críticos (Domain Controllers, bases de datos, servidores de archivos, sistemas financieros).
Evasión de controles	El equipo de Red Team busca evadir activamente los controles de detección (EDR, SIEM, IDS/IPS) para evaluar su efectividad real frente a un adversario que adapta sus técnicas.
Evaluación del Blue Team	Se mide la capacidad del equipo de seguridad del cliente (Blue Team/SOC) para detectar, investigar, contener y responder a las actividades del Red Team, documentando tiempos de detección y respuesta.

SEXTO – MARCOS DE REFERENCIA APLICADOS

Todas las actividades de seguridad ofensiva descritas se ejecutan alineadas con los siguientes marcos y estándares internacionales:

Marco / Estándar	Aplicación
MITRE ATT&CK	Mapeo de todas las técnicas utilizadas y hallazgos identificados contra la matriz ATT&CK para Enterprise
NIST SP 800-115	Estructura de ejecución de las evaluaciones técnicas: Planificación, Descubrimiento, Ataque, Reporte
OWASP Testing Guide v4.2	Metodología de pruebas de seguridad para aplicaciones web
OWASP Top 10 (2021)	Clasificación de vulnerabilidades web identificadas
PTES (Penetration Testing Execution Standard)	Estándar de ejecución de pruebas de penetración: pre-engagement, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, reporting
OSSTMM (Open Source Security Testing Methodology Manual)	Metodología complementaria para evaluaciones de seguridad de infraestructura y comunicaciones
CVSS v3.1	Clasificación de severidad de todas las vulnerabilidades identificadas
ISO/IEC 27001:2022	Alineación de controles evaluados con el Anexo A del estándar

SÉPTIMO – ENTREGABLES Y SEGUIMIENTO

Al finalizar cada ejercicio de seguridad ofensiva, Intrust Security entrega los siguientes productos:

- Informe ejecutivo dirigido a la alta dirección con resumen de hallazgos críticos, nivel de riesgo global y recomendaciones estratégicas.
- Informe técnico detallado con la descripción completa de cada vulnerabilidad, evidencias de explotación, clasificación CVSS, categorización OWASP (cuando aplica), mapeo MITRE ATT&CK y recomendaciones de remediación priorizadas.
- Registro de todos los hallazgos en la plataforma ALTAIR para gestión, seguimiento y cierre verificado de vulnerabilidades por parte del cliente.
- Sesión de presentación de resultados al equipo técnico y directivo del cliente.
- Ejecución de retest de verificación posterior a la remediación, con alertas automáticas desde ALTAIR.

OCTAVO – DECLARACIÓN

En virtud de lo expuesto, certifico y confirmo que Intrust Security S.A.S.:

- Ejecuta pruebas de penetración en modalidad de caja negra y caja gris de manera secuencial para todos sus clientes, realizando primero la evaluación sin información (caja negra) y posteriormente, con la entrega de credenciales y contextualización por parte del cliente, la evaluación en caja gris.
- Ejecuta actividades de Threat Hunting como búsqueda proactiva de amenazas basada en hipótesis e inteligencia de amenazas.
- Ejecuta actividades de Adversary Emulation replicando las TTPs de actores de amenaza reales mapeados contra MITRE ATT&CK.



- Ejecuta ejercicios de Red Teaming como evaluación integral de la postura de seguridad que combina penetración técnica, ingeniería social, movimiento lateral y evaluación de capacidades de detección y respuesta.
- Todas las actividades anteriores forman parte del alcance estándar de los servicios de seguridad ofensiva de Intrust Security y se ejecutan conforme a los marcos de referencia internacionales mencionados en esta certificación.

La presente certificación se expide en cumplimiento de los requisitos establecidos en el proceso de evaluación y a solicitud de la entidad interesada. La información contenida es veraz y verificable.

Se expide a los nueve (9) días del mes de mayo de 2026, en la ciudad de Medellín, Colombia.

A handwritten signature in black ink, appearing to read "Sergio Mauricio Barón Vera", written over a horizontal line.

Sergio Mauricio Barón Vera

Representante Legal

Intrust Security S.A.S.

NIT: 901380604-6

CC: 91'286.268 de Bucaramanga



Outlook

Informe de Documentos para Subsanaciones

Desde Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>**Fecha** Mar 12/05/2026 16:38**Para** Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>**CC** Sergio Andres Velez Upegui <coordinacion.mesa@valormas.gov.co>

1 archivo adjunto (52 KB)

INFORME DE RESPUESTA TÉCNICA A DOC PRESENTADA POR PROPONENTE VULNERABILIDADES.docx;

Buena tarde, envié documento de validación aprobando las subsanaciones enviadas de los documentos requeridos.

Gracias por su atención.

**Carlos Arturo Correa Correa**

Profesional Universitario

carlos.correa@valormas.gov.coCalle 42 # 52-27, Edificio Edstel, Piso 3, Sector A/pujarra,
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) es dirigido.
Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución
o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos
notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

INFORME DE RESPUESTA TÉCNICA A DOCUMENTACIÓN

PRESENTADA POR EL PROPONENTE

INTRUST SECURITY S.A.S.

En atención a la revisión de los documentos allegados por el **INTRUST SECURITY S.A.S.**, y en el marco del proceso contractual correspondiente a la Convocatoria Abreviada N° 012-2026, se procede a emitir las siguientes consideraciones técnicas.

1. Sobre la aclaración técnica del desarrollo

Tras la evaluación de la aclaración presentada por el proponente, se determina que la propuesta **CUMPLE** con los requerimientos técnicos del desarrollo establecidos en la convocatoria.

A continuación, se describen los puntos en los cuales el proponente aporta la información necesaria de acuerdo con el informe preliminar y a los documentos faltantes que debían de ser entregados por parte de **INTRUST SECURITY S.A.S.** con el fin realizar las subsanaciones de los puntos donde cumplía parcialmente o se requería más aclaración y especificidad de lo preguntado y requerido.

1.1. Verificación jurídica: cumple luego de aportar los documentos faltantes de:

- Certificado de antecedentes Disciplinarios.
- Certificado bancario Vigente
- Certificado de lavado de activos y financiación del territorio.

1.2. Verificación técnica: cumple luego de aportar los documentos faltantes de:

- Entrega de documento con las precisiones de la plataforma a emplear y la descripción de su funcionalidad y alcance. Intrust Security S.A.S. certifica que para la prestación de servicios de Vigilancia Tecnológica (Threat Intelligence) utiliza la plataforma propietaria denominada VektCore, desarrollada internamente por el equipo de ingeniería de la empresa con capacidades nativas de Inteligencia Artificial. Ver: **CERT-VKC-2026-001_VektCore**
- Envía documento donde manifiesta la aplicación de estándares y buenas prácticas solicitadas en la gestión de vulnerabilidades. Intrust Security S.A.S., en el ejercicio de sus servicios profesionales de ciberseguridad, aplica de manera sistemática los siguientes estándares y marcos de referencia internacionales en todos sus procesos de identificación, evaluación, priorización, remediación y seguimiento de vulnerabilidades. Ver. **CERT-GTV-2026-001_Gestion_Tratamiento_Vulnerabilidades**

- Documento aportado señalando que ejecuta actividades descritas en alcance garantizando cumplimiento de estándares técnico, normativos y buenas prácticas de ciberseguridad. . Intrust Security S.A.S., en el ejercicio de sus servicios profesionales de ciberseguridad, aplica de manera sistemática los siguientes estándares y marcos de referencia internacionales en todos sus procesos de identificación, evaluación, priorización, remediación y seguimiento de vulnerabilidades. Ver. **CERT-GTV-2026-001_Gestion_Tratamiento_Vulnerabilidades**
- Documento suscrito por el representante legal donde indica que en el desarrollo del objeto contractual y en cumplimiento de esta gestión desarrollara ejercicios especializados como pruebas de penetración sobre los activos. Intrust Security S.A.S., en el ejercicio de sus servicios profesionales de ciberseguridad, aplica de manera sistemática los siguientes estándares y marcos de referencia internacionales en todos sus procesos de identificación, evaluación, priorización, remediación y seguimiento de vulnerabilidades. Ver. **CERT-ALTAIR-2026-001_Gestion_Vulnerabilidades**

 CERT-ALTAIR-2026-001_Gestion_Vulnerabilidades

 CERT-GTV-2026-001_Gestion_Tratamiento_Vulnerabilidades

 CERT-VKC-2026-001_VektCore

Conclusión: Cumple ya que envía la documentación requerida de subsanación

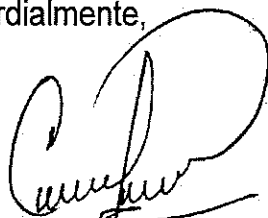
2. Conclusión General

Tras la revisión integral de la propuesta y sus documentos aclaratorios, se concluye que el proveedor:

- Presenta una propuesta técnicamente sólida en materia de seguridad.
- Cumple con los documentos que validan la experiencia y conocimientos técnicos con sus respectivos soportes y certificaciones requeridos.

En consecuencia, el proponente subsana de acuerdo con **las observaciones señaladas** para dar cumplimiento integral a las condiciones del proceso.

Cordialmente,



Carlos Arturo Correa Correa
Profesional Universitario
Valor+ S.A.S



Código: E003 DE CCM
Versión: 1.0
Fecha: 20/07/2018

OBJETO: ""												
Contratante	Contratista	Objeto del Contrato	Valor	Plazo	Estado: (en ejecución, ejecutado o terminado)	Proponentes						
						Proponente 1	Proponente 2	Proponente 3	Proponente 4	Proponente 5	Proponente 6	Proponente 7
						Intrusit Security S.A.S.						
						Cumple / No cumple	Cumple / No cumple	Cumple / No cumple	Cumple / No cumple	Cumple / No cumple	Cumple / No cumple	Cumple / No cumple
Modussoftware	Intrusit Security S.A.S.	Prestar el servicio profesional de auditoría para evaluar el cumplimiento frente a las buenas prácticas: ISO 27032 (Cybersecurity Framework) y Cybersecurity Framework NIST (National Institute of Standard and Technology) y realizar una verificación de los controles establecidos por el cliente de MODUSSOFTWARE en ese caso la CCB, para mitigar los riesgos de ciberseguridad, a través de la emisión de recomendaciones que permitan tomar acciones para mejorar el programa de gobierno de la ciberseguridad y de los controles implementados.	\$ 139.200.000	3 meses	Ejecutado	Cumple						
Distribuciones AXA	Intrusit Security S.A.S.	Fortalecer la postura de ciberseguridad de las organizaciones mediante la evaluación continua, gestión proactiva y acompañamiento especializado en la identificación, análisis y reducción de riesgos tecnológicos.	\$ 71.100.120	12 meses	Ejecutado	No Cumple (Pq no tiene certificado)						
Modussoftware	Intrusit Security S.A.S.	Evaluar y fortalecer la postura de seguridad de los activos tecnológicos de ALDEAMO mediante ejercicios avanzados de Red Team y Ethical Hacking, con el fin de identificar vulnerabilidades críticas, validar controles existentes y proponer medidas de mitigación alineadas a estándares internacionales y necesidades estratégicas de la organización.	\$ 65.000.000	1 mes	Ejecutado	Cumple						
TCC	Intrusit Security S.A.S.	Servicios de Ciberseguridad	\$ 110.384.400	12 meses	Ejecutado	Cumple						
Valor +	Intrusit Security S.A.S.	Prestación de servicios especializados de seguridad informática para los diferentes proyectos de Valor+ y sus clientes	\$ 128.674.700	4 meses	Ejecutado	No Cumple (Pq no tiene certificado)						

**Versionamiento Formato**

Código: FO16-DE-GCYN
Versión: 1.0
Fecha actualización: 8/11/2023

Medellín, 13 de mayo de 2026

Convocatoria Abreviada N° 012 - 2026

Objeto: “Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet.”

Valor+ S.A.S.

INFORME DE EVALUACIÓN DEFINITIVO

De conformidad con el cronograma de la “Convocatoria Abreviada N° 012-2026”, el día 28 de abril de 2026, se envió el documento Condiciones de la Contratación con todos sus anexos a cinco (05) personas jurídicas y se publicó en plataforma Web (Página Web de la empresa), en el cual se informaron todos los requisitos y exigencias para participar en el proceso.

#	Proponente	Nit	Medio de Comunicación
1	3 POINTECH S.A.S.	900.131.823	gerencia@3pointech.net , compras@3pointech.net
2	INTRUST SECURITY S.A.S.	901.380.604	sbaron@intrustsecurity.co
3	CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.	900.096.184	procesoscomerciales@ccd.com.co
4	GAMMA INGENIEROS S.A.S.	891.501.783	natalia.molina@gammaingenieros.com
5	HEIMCORE S.A.S.	900.425.697	yvasquez@heimcore.com.co , larodriguez@heimcore.com.co

Hasta las 18:00 horas del día 29 de abril de 2026, se estableció el plazo para la presentación de observaciones y/o solicitud de aclaraciones a las condiciones de la contratación.

Se presentaron observaciones y/o solicitud de aclaraciones a las condiciones de la contratación por parte de las siguientes empresas: (Ver Adjunto Observaciones)

#	Proponente	Fecha y Hora	Medio de Comunicación
1	INCOCREDITO	29/04/2026 a las 16:51 horas	chenao@incocredito.com.co
2	GAMMA INGENIEROS S.A.S.	29/04/2026 a las 15:02 horas	natalia.molina@gammaingenieros.com

Posterior a esto, se generó de acuerdo con lo establecido en el cronograma, la respuesta a las observaciones presentadas, lo cual tenía plazo hasta el 04 de mayo de 2026 a las 17:00 horas. (Ver adjunto Respuesta Observaciones)

La empresa 3 POINTECH S.A.S., el día 28 de abril de 2026 estando dentro del plazo establecido, manifestó lo siguiente: “(...)encontramos que no se encuentra dentro de nuestro portafolio esa solución”. También la empresa GAMMA INGENIEROS S.A.S. el día 06 de mayo de 2026 indicó a través de correo electrónico lo siguiente: “(...)en este caso NO es posible participar, el motivo es NO poder llegar al presupuesto asignado,(...)”

El plazo establecido para la presentación de las propuestas fue hasta el día 06 de mayo de 2026, hasta las 17:00 horas y se presentó el siguiente proponente, tal y como consta en el acta de recepción:

Proponente	Nit	Fecha y hora de Recepción	Valor Propuesta	Medio de recibo de la propuesta	# Folios
INTRUST SECURITY S.A.S.	901.380.604-6	06/05/2026 16:12 horas	\$55.800.000	compras2@valormas.gov.co	Se recibe por medio digital



El día 08 de mayo de 2026 dentro del plazo establecido de acuerdo con cronograma, se envió a los proponentes el Informe Preliminar de Evaluación y se publicó en plataforma Web (Página Web de la empresa); en el cual consta la participación de la empresa **INTRUST SECURITY S.A.S.** Dentro del referido informe, se concedió a la empresa plazo para presentación de observaciones al informe de evaluación preliminar y/o aclaraciones y/o subsanaciones de la oferta hasta el día 11 de mayo de 2026 hasta las 18:00 horas.

1. OBSERVACIONES Y/O ACLARACIONES

Dentro del término establecido se recibió subsanación al informe preliminar de evaluación por parte del proponente **INTRUST SECURITY S.A.S.**

2. SUBSANACIONES PRESENTADAS POR EL PROPONENTE

Se recibieron las subsanaciones por parte del proponente **INTRUST SECURITY S.A.S.**, mediante correo allegado a la dirección electrónica compras2@valormas.gov.co de acuerdo con lo señalado en el informe de evaluación preliminar y que corresponden a los requisitos: **Capacidad Jurídica:** Certificado Antecedentes Disciplinarios de la Persona Jurídica); Certificación Bancaria a la fecha; y Certificación de Lavado de Activos y Financiación del Terrorismo debidamente diligenciada. **Capacidad Técnica:** **Alcance:** Documento indicando cual es la plataforma o plataformas para utilizará el proveedor y la sustentación desde lo técnico, lo funcional y la cobertura. **Certificaciones:** Certificado señalando que aplica estándares internacionales, tales como el modelo CVSS (Common Vulnerability Scoring System); Certificado señalando que ejecuta las actividades garantizando el cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad (ISO 27001, NIST, MITRE ATT&CK, OWASP, entre otros); adicional, certificado o documento señalando que realizará ejercicios especializados tales como pruebas de penetración (caja negra y/o caja gris) sobre los activos críticos definidos por la entidad, así como actividades de Threat Hunting, Adversary Emulation y Red Teaming, orientadas a fortalecer la capacidad de detección y respuesta frente a amenazas avanzadas, tal y como se describe a continuación:

2.1. REQUERIMIENTOS:

2.1.1. VERIFICACIÓN CAPACIDAD JURÍDICA:

➤ Atendiendo a las "Condiciones de la Contratación Convocatoria Abreviada N° 012-2026", numeral "2.1 Capacidad Jurídica", el proponente debía subsanar lo siguiente:

- "10. Certificado Antecedentes Disciplinarios (Representante legal y persona jurídica). **Debe aportar certificado de la persona jurídica.**"

El proponente aporta certificado de antecedentes disciplinarios de la persona jurídica fechado del 11 de mayo de 2026. Este documento fue evaluado, concluyendo que **CUMPLE** con lo solicitado.

- "14. Certificación Bancaria. **Debe aportar certificado vigente,** ya que como se determinó en las condiciones de la contratación: "La expedición de los certificados no podrá tener una anterioridad superior a treinta (30) días calendario, contado a partir de la fecha de cierre del proceso."

El proponente aporta certificado bancario generado por BANCOLOMBIA, fechado al 11 de mayo de 2026. Este documento fue evaluado, concluyendo que **CUMPLE** con lo solicitado.

- “17. Formato Certificación de lavado de activos y financiación del terrorismo diligenciado. **Debe aportar certificado debidamente diligenciado.**”

El proponente aporta certificación de lavado de activos y financiación del terrorismo debidamente diligenciado, fechado al 08 de mayo de 2026. Este documento fue evaluado, concluyendo que **CUMPLE** con lo solicitado.

CONCLUSIÓN: En este sentido, se entienden subsanados estos requisitos por parte del proponente **INTRUST SECURITY S.A.S.** **Capacidad Jurídica:** certificado de antecedentes disciplinarios persona jurídica; certificación bancaria a la fecha; y certificación de lavado de activos y financiación del terrorismo debidamente diligenciado, por lo tanto, **CUMPLE** con las condiciones previamente señaladas (Requisitos Jurídicos)

2.1.2. VERIFICACIÓN CAPACIDAD TÉCNICA:

- Respecto a lo señalado en las “Condiciones de la Contratación Convocatoria Abreviada N° 012-2026”, específicamente para el numeral “**Alcance y/o Condiciones y/o Especificaciones Técnicas del Bien o Servicio a Contratar**”, en el “**Servicio de Vigilancia Tecnológica, Gestión de Vulnerabilidades y Superficie de Ataque**”, **en los ejes fundamentales**, se tiene para **los ejes** lo siguiente:

1. “**Vigilancia Tecnológica: (...) Para el cumplimiento de esta obligación, el Proveedor deberá emplear plataformas especializadas de inteligencia de amenazas (Threat Intelligence), cuya selección deberá estar debidamente sustentada mediante criterios técnicos, funcionales y de cobertura.**”; si bien, en el documento “Propuesta” se menciona lo anterior, no se indica cual es la plataforma o plataformas para utilizar por el proveedor y la sustentación desde lo técnico, lo funcional y la cobertura. **Para poder evaluarlo correctamente, se requiere que el proponente realice las precisiones respecto a la plataforma o plataformas a emplear y su descripción y alcance,** con el fin de asegurar que la oferta cumple con todas las especificaciones técnicas y se eviten riesgos en la ejecución.

El proponente presenta documento “**Certificación y sustentación técnica de la plataforma de vigilancia tecnológica (Threat Intelligence)**”, a través del cual certifica que para la prestación de servicios de Vigilancia Tecnológica (Threat Intelligence) utiliza la plataforma propietaria denominada VektCore, desarrollada internamente por el equipo de ingeniería de la empresa con capacidades nativas de Inteligencia Artificial, y detalla el alcance, propiedades y beneficios.

Este documento fue evaluado, concluyendo que **CUMPLE** con lo solicitado.

- Frente a la **gestión de vulnerabilidades** y de acuerdo con lo establecido en las “Condiciones de la Contratación Convocatoria Abreviada N° 012-2026”, se solicitó que el proveedor presentara certificado manifestando que aplica los estándares internacionales, tales como el modelo CVSS (Common Vulnerability Scoring System). En el caso de aplicaciones web, deberá adoptar las buenas prácticas establecidas por OWASP (Open Web

Application Security Project), y para la ejecución de pruebas técnicas, deberá alinearse con lo establecido en el marco metodológico NIST SP 800-115. Asimismo, las actividades deberán estar articuladas con el marco MITRE ATT&CK, incorporando enfoques como Adversary Emulation, Red Teaming y Threat Hunting, orientados a fortalecer la capacidad de detección y respuesta ante amenazas avanzadas.

Con el fin de subsanar lo requerido, el proponente INTRUST SECURITY S.A.S. aporta **"Certificación de aplicación de estándares y buenas prácticas en Gestión de Vulnerabilidades (CVSS, OWASP, NIST SP 800-115, MITRE ATT&CK)"** donde manifiesta que aplica de manera sistemática los siguientes estándares y marcos de referencia internacionales en todos sus procesos de identificación, evaluación, priorización, remediación y seguimiento de vulnerabilidades:



Estándar / Marco	Descripción	Aplicación en Intrust Security
CVSS (Common Vulnerability Scoring System)	Sistema estándar de la industria para evaluar la severidad de las vulnerabilidades de seguridad informática mediante una puntuación numérica de 0.0 a 10.0, mantenido por el FIRST (Forum of Incident Response and Security Teams).	Todas las vulnerabilidades identificadas son clasificadas utilizando CVSS v3.1 como sistema de scoring primario. La priorización de remediación se establece según los rangos.
OWASP (Open Worldwide Application Security Project)	Proyecto de código abierto dedicado a mejorar la seguridad del software. Su marco de referencia OWASP Top 10 establece las categorías de vulnerabilidades más críticas en aplicaciones web.	Las evaluaciones de seguridad de aplicaciones web siguen la metodología OWASP Testing Guide (OTG) v4.2 y clasifican hallazgos conforme al OWASP Top 10 (versión 2021).
NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment)	Guía técnica del Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos que establece las directrices para la planificación, ejecución y reporte de evaluaciones de seguridad de la información.	Las evaluaciones técnicas de seguridad (pentesting, análisis de vulnerabilidades, auditorías) se ejecutan conforme a las fases definidas por NIST.
MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)	Base de conocimiento mantenida por MITRE Corporation que documenta las tácticas, técnicas y procedimientos (TTPs) utilizados por actores de amenaza reales, organizada en matrices por plataforma.	Los hallazgos de seguridad se mapean contra la matriz MITRE ATT&CK para Enterprise, identificando las técnicas específicas (T-ID) explotadas o explotables, lo que permite contextualizar el riesgo frente a amenazas reales y documentadas.

Adicional, indica que han desarrollado internamente la plataforma denominada ALTAIR, la cual constituye el eje central del ciclo de vida de gestión de vulnerabilidades de sus servicios.

Este documento fue evaluado, concluyendo que **CUMPLE** con lo solicitado.

- En el alcance del documento "Condiciones de la Contratación Convocatoria Abreviada N° 012-2026", se estableció lo siguiente: **"Gestión y tratamiento de vulnerabilidades (...)** El proveedor deberá ejecutar las actividades descritas, garantizando el cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad (ISO 27001, NIST, MITRE

ATT&CK, OWASP, entre otros). Por lo anterior, se solicitó al proponente subsanar y aportar certificado manifestando que garantiza lo anterior.”

Al respecto, el proponente **INTRUST SECURITY S.A.S.** con el fin de subsanar lo solicitado, presentó documento **“Certificación de cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad en Gestión y Tratamiento de Vulnerabilidades.”**, a través del cual señala que cumple a cabalidad con los estándares técnicos, normativos y buenas prácticas de ciberseguridad solicitados, aplicados de manera integral en todos los servicios de gestión y tratamiento de vulnerabilidades.

Este documento fue evaluado, concluyendo que **CUMPLE** con lo solicitado.

- Adicional a lo anterior, el proponente debía indicar como se estableció en el alcance del documento **“Condiciones de la Contratación Convocatoria Abreviada N° 012-2026”**, si en el desarrollo del objeto contractual y en cumplimiento de esa gestión, desarrollará **“(…) ejercicios especializados tales como pruebas de penetración (caja negra y/o caja gris) sobre los activos críticos definidos por la entidad, así como actividades de Threat Hunting, Adversary Emulation y Red Teaming, orientadas a fortalecer la capacidad de detección y respuesta frente a amenazas avanzadas.”**

El proponente subsana lo solicitado, aportando documento **“Certificación de alcance de actividades de Red Team, Pruebas de Penetración, Threat Hunting y Adversary Emulation”**, mediante el cual confirma que en desarrollo del objeto contractual ejecuta la totalidad de las siguientes actividades de seguridad ofensiva:



Actividad	Se ejecuta	Descripción del alcance
Pruebas de Penetración (Caja Negra)	SÍ	Evaluación de seguridad sin información previa del entorno objetivo. Se ejecuta como primera fase de toda evaluación, simulando un atacante externo sin conocimiento interno de la organización.
Pruebas de Penetración (Caja Gris)	SÍ	Evaluación con credenciales y contextualización proporcionada por el cliente. Se ejecuta como segunda fase, posterior a la caja negra, permitiendo profundizar en vectores de ataque internos y validar controles de acceso.
Threat Hunting	SÍ	Búsqueda proactiva de amenazas activas o latentes dentro de la infraestructura del cliente, utilizando hipótesis basadas en inteligencia de amenazas y análisis de comportamiento anómalo.
Adversary Emulation	SÍ	Simulación de las tácticas, técnicas y procedimientos (TTPs) de actores de amenaza reales y documentados, utilizando la matriz MITRE ATT&CK como referencia para replicar escenarios de ataque específicos del sector del cliente.
Red Teaming	SÍ	Ejercicio integral de seguridad ofensiva que combina pruebas de penetración, ingeniería social, acceso físico (cuando aplica) y explotación de vulnerabilidades técnicas para evaluar la capacidad real de detección y respuesta de la organización frente a un adversario sofisticado.



Este documento fue evaluado, concluyendo que **CUMPLE** con lo solicitado.

CONCLUSIÓN: En este sentido, se entienden subsanados estos requisitos por parte del proponente **INTRUST SECURITY S.A.S. Capacidad Técnica:** Precisiones respecto a la plataforma o plataformas a emplear y su descripción y alcance; Aportar certificado manifestando que aplica los estándares y buenas prácticas solicitadas para Gestión de Vulnerabilidades; Aportar certificado donde señale que ejecutará las actividades descritas en el alcance, garantizando el cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad (ISO 27001, NIST, MITRE ATT&CK, OWASP, entre otros); Indicar a través de documento suscrito por el Representante Legal si en el desarrollo del objeto contractual y en cumplimiento de esta gestión, desarrollará "(...) *ejercicios especializados tales como pruebas de penetración (caja negra y/o caja gris) sobre los activos críticos definidos por la entidad, así como actividades de Threat Hunting, Adversary Emulation y Red Teaming, orientadas a fortalecer la capacidad de detección y respuesta frente a amenazas avanzadas.*", por lo tanto, **CUMPLE** con las condiciones previamente señaladas (Requisitos Técnicos)

3. VERIFICACIÓN REQUISITOS HABILITANTES DESPUES DE OBSERVACIONES Y/O SUBSANACIONES

Los requisitos habilitantes serán objeto de verificación, por lo tanto, únicamente se considera (n) habilitado (s) aquello (s) oferente (s) que cumpla (n) con todos los requisitos solicitados en el documento Condiciones de la Contratación. Se evaluará (n) como "Cumple", en caso contrario, se evaluarán como "No cumple" y, por tanto, no será objeto de evaluación en los requisitos de evaluación, sin perjuicio de la subsanación que el o los oferentes puedan realizar en el término que otorgue Valor+.

3.1. Capacidad Jurídica:

Nº	DOCUMENTO	INTRUST SECURITY S.A.S. CUMPLE / NO CUMPLE	OBSERVACIÓN
1	Carta de presentación de la propuesta debidamente diligenciada.	Cumple	Aporta carta de presentación de la propuesta debidamente diligenciada y suscrita por el Representante Legal, fechada a 06 de mayo de 2026.
2	Certificado de existencia y representación legal del proponente, con fecha de expedición no mayor a treinta (30) días anteriores a la fecha de presentación de la oferta.	Cumple	Presentado con fecha del 06/05/2026.
3	Acta de la Junta o Asamblea que autoriza al representante legal del Proponente a presentar la oferta, cuando se trate de persona jurídica (Si aplica).	N/A	De conformidad con el certificado de existencia y representación legal, el proponente no tiene restricciones de contratación por razón de la naturaleza ni de la cuantía de los actos que celebre! Adicional, el Certificado señala: "REPRESENTACION LEGAL. El Gerente General será el Representante Legal de la sociedad y tendrá a su cargo la inmediata dirección y administración de los negocios

			<i>sociales con sujeción a las disposiciones legales y estatutarias y a las decisiones de la asamblea general de accionistas. Todos los funcionarios y empleados de la sociedad, con excepción de los nombrados por la asamblea general, estarán subordinados a él y bajo su dirección e inspección inmediata."</i>
4	Certificado de estar a paz y salvo con el sistema de seguridad social integral (salud, pensión, riesgos profesionales y ARL) y aportes parafiscales (ICBF, Sena y Cajas de Compensación Familiar), expedido por el representante legal y/o contador o revisor fiscal (adjuntando copia de la cédula, copia de la tarjeta profesional y certificado de antecedentes disciplinarios expedido por la junta central de contadores del contador) o Planilla integrada de autoliquidación de aportes a la seguridad social integral y aportes parafiscales.	Cumple	Aporta certificado con fecha del 06 de mayo de 2026, suscrito por el Representante Legal y el Contador. También aporta: -Copia de la cédula del contador. -Copia de la tarjeta profesional del contador. -Certificado de antecedentes disciplinarios expedido por la junta central de contadores del 24 de abril de 2026 con vigencia de tres (3) meses contados a partir de la fecha de su expedición.
5	Copia del documento de identidad del representante legal o apoderado.	Cumple	Aporta cédula de ciudadanía
6	Copia del Registro Único Tributario (RUT)	Cumple	Aporta el documento actualizado con fecha de generación del 06/05/2026.
7	Certificado Registro de Deudores Alimentarios Morosos – REDAM	Cumple	Aporta certificado del 05/05/2026 del representante legal, sin reporte de antecedentes y valido hasta el 04/08/2026.
8	Certificado de la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST, emitido por la ARL o el Ministerio del Trabajo, con vigencia no mayor a noventa (90) días antes de la presentación de la oferta.	Cumple	Aporta certificado emitido por Sura con fecha del 19 de marzo de 2026.
9	Certificado Antecedentes fiscales (Representante legal y persona jurídica).	Cumple	Aporta certificados del Representante Legal y de la Persona Jurídica del 05/05/2026 sin reporte de antecedentes.
10	Certificado Antecedentes Disciplinarios (Representante legal y persona jurídica).	<u>Cumple</u>	Aporta certificado del 05/05/2026 del Representante Legal sin reportes de antecedentes. Aporta certificado del 11/05/2026 de la persona jurídica sin reportes de antecedentes.
11	Certificado Antecedentes judiciales del Representante legal.	Cumple	Aporta certificado del 06/05/2026 del representante legal, sin reporte de antecedentes.
12	Certificado Antecedentes Medidas correctivas del Representante legal.	Cumple	Aporta certificado del 06/05/2026 del representante legal, sin reporte de antecedentes.

13	Certificado Antecedentes de delitos sexuales cometidos contra menores de 18 años del Representante legal.	Cumple	Aporta certificado del 06/05/2026 del representante legal, sin reporte de antecedentes.
14	Certificación Bancaria.	<u>Cumple</u>	Aporta certificado del 11/05/2026 expedida por Bancolombia.
15	Formato Inhabilidades e Incompatibilidades Persona Jurídica diligenciado.	Cumple	Debidamente diligenciado y suscrito por el representante legal con fecha del 06/05/2026.
16	Formato Autorización tratamiento de datos diligenciado.	Cumple	Debidamente diligenciado y suscrito por el representante legal con fecha del 06/05/2026.
17	Formato Certificación de lavado de activos y financiación del terrorismo diligenciado.	<u>Cumple</u>	Aporta formato debidamente diligenciado y suscrito por el Representante Legal, fechado al 08/05/2026.
18	Garantía de seriedad de la oferta.	Cumple	Póliza emitida por Seguros del Estado S.A. Vigencia desde el 06/05/2026 hasta el 20/08/2026. Valor Asegurado de \$5.721.520 (10% del valor del presupuesto oficial). Aporta comprobante de pago de la prima.
19	Registro Único de Proponentes – RUP renovado y en firme. Los proponentes deberán estar inscritos y clasificados en el Registro Único de Proponentes de la Cámara de Comercio de su jurisdicción, de acuerdo con las condiciones establecidas en el Título VI Registro Único de Proponentes –RUP del Decreto 1082 de 2015. La expedición de dicho certificado no podrá tener una anterioridad superior a treinta (30) días calendario, contado a partir de la fecha de cierre del proceso. En caso de no contar con el RUP renovado en firme, se deberán aportar Balances o Estados Financieros aprobados del año inmediatamente anterior.	Cumple	Aporta Estados Financieros 2025, elaborados el 24 de febrero de 2026, aprobados por el Representante Legal y Contador de la empresa.
20	Manifestación Juramentada de Ausencia de Multas y/o Sanciones: El proponente deberá hacer manifestación juramentada de ausencia o presencia de multas y/o sanciones impuestas por entidades públicas en los cinco (5) últimos años anteriores al cierre de esta convocatoria.	Cumple	Aporta Manifestación Juramentada de Ausencia de Multas y/o Sanciones con fecha del 06/05/2026 suscrita por el representante legal.

CONCLUSIÓN: De acuerdo con lo anterior, el proponente **INTRUST SECURITY S.A.S.** **CUMPLE** con los requisitos jurídicos habilitantes.

3.2. Capacidad Técnica:

Atendiendo a las “Condiciones de la Contratación Convocatoria Abreviada N° 012-2026”, en lo respectivo a la capacidad técnica, y específicamente a que el proponente realizara o precisara lo siguiente: “*Precisiones respecto a la plataforma o plataformas a emplear y su descripción y alcance; Aportar certificado manifestando que aplica los estándares y buenas prácticas solicitadas para Gestión de Vulnerabilidades; Aportar certificado donde señale que ejecutará las actividades descritas en el*

alcance, garantizando el cumplimiento de estándares técnicos, normativos y buenas prácticas de ciberseguridad (ISO 27001, NIST, MITRE ATT&CK, OWASP, entre otros); Indicar a través de documento suscrito por el Representante Legal si en el desarrollo del objeto contractual y en cumplimiento de esta gestión, desarrollará "(...) ejercicios especializados tales como pruebas de penetración (caja negra y/o caja gris) sobre los activos críticos definidos por la entidad, así como actividades de Threat Hunting, Adversary Emulation y Red Teaming, orientadas a fortalecer la capacidad de detección y respuesta frente a amenazas avanzadas; se evidencia que cumplió a cabalidad con lo solicitado.

CONCLUSIÓN: De acuerdo con lo anterior, el proponente **CUMPLE** con los requisitos técnicos habilitantes.

Adicionalmente y de acuerdo con los requisitos de capacidad técnica establecidos en el documento condiciones de la contratación "(...) el proponente **deberá acreditar la cuantía en máximo dos (2) contratos relacionados con el objeto del presente proceso, en ejecución, ejecutados o terminados a la fecha de cierre de la convocatoria y cuya sumatoria sea igual o superior al presupuesto oficial establecido para esta contratación.**

Las certificaciones deberán contener por lo menos la siguiente información:

- Contratante.
- Contratista.
- Objeto.
- Valor.
- Plazo.
- Estado: (en ejecución, ejecutado o terminado)

Los certificados de experiencia deben ser en idioma español.

Para los contratos en ejecución, adicionalmente se deberá certificar cual es el valor ejecutado a la fecha."

Nº	CONTRATANTE	OBJETO DEL CONTRATO	VALOR EN SMMLV/PESOS	CUMPLE/ NO CUMPLE	OBSERVACIONES
1	MODUSOFTWARE	Evaluar y fortalecer la postura de seguridad de los activos tecnológicos de ALDEAMO mediante ejercicios avanzados de Red Team y Ethical Hacking, con el fin de identificar vulnerabilidades críticas, validar controles existentes y proponer medidas de mitigación alineadas a estándares internacionales y	\$65.000.000	Cumple	Plazo: Desde el 01/09/2025 hasta el 05/10/2025 45,66 SMMLV



		necesidades estratégicas de la organización			
2	MODUSOFTWARE	Prestar el servicio profesional de auditoría para evaluar el cumplimiento frente a las buenas prácticas: ISO 27032 (Cybersecurity Framework) y Cybersecurity Framework NIST (National Institute of Estandar and Technology) y realizar una verificación de los controles establecidos por el cliente de MODUSOFTWARE en ese caso la CCB, para mitigar los riesgos de ciberseguridad, a través de la emisión de recomendaciones que permitan tomar acciones para mejorar el programa de gobierno de la ciberseguridad y de los controles implementados.	\$139.200.000	Cumple	Plazo: Desde el 29/07/2024 hasta el 27/10/2024 107, 07 SMLV

Nota: La sumatoria de los contratos que se acreditan como experiencia habilitante, cumple con lo solicitado en este criterio.

CONCLUSIÓN: De acuerdo con lo anterior, el proponente **CUMPLE** con los requisitos habilitantes de carácter técnico, ya que tanto la propuesta económica, como la experiencia cumplen con lo solicitado.

3.3. Capacidad Financiera:

“Los requisitos financieros para participar en el presente proceso serán verificados a partir de la información que deberán aportar el o los proponentes en el correspondiente Registro Único de Proponentes – RUP debidamente actualizado y renovado y/o Balances o Estados Financieros aprobados del año inmediatamente anterior.”

Para validar la capacidad financiera, el oferente deberá aportar los siguientes indicadores:

INDICADOR	FÓRMULA	INDICADOR	INDICADOR PROPONENTE	CUMPLE/NO CUMPLE
Índice de Liquidez	$\frac{\text{Activo corriente}}{\text{Pasivo Corriente}}$	Mayor o igual a 1.3	2.18	Cumple
Índice de endeudamiento	$\frac{\text{Activo Total}}{\text{Pasivo Total}}$	Menor o igual al 60%	39%	Cumple
Razón de Cobertura de Intereses	$\frac{\text{Utilidad operacional}}{\text{Gasto de Intereses}}$	Mayor o igual a 2.0	16	Cumple

3.4. Capacidad organizacional:

"Para validar la capacidad organizacional se tomará la información que aparezca en el Registro Único de Proponentes (RUP) y/o Balances o Estados Financieros aprobados del año inmediatamente anterior."

Para validar la capacidad organizacional, el oferente deberá aportar los siguientes indicadores:

FACTOR EVALUACIÓN	FORMULA	CRITERIO	INDICADOR PROPONENTE	CUMPLE/NO CUMPLE
Indicadores de Rentabilidad				
ROE	$\frac{\text{Utilidad Operacional}}{\text{Patrimonio}}$	Mayor o igual al 5%	13.46%	Cumple
ROA	$\frac{\text{Utilidad Operacional}}{\text{Activo Total}}$	Mayor o igual al 2%	8%	Cumple

De acuerdo con la revisión de los indicadores financieros exigidos en la convocatoria abreviada, se evidencia que el proponente **cumple** con los requisitos establecidos.

En relación con el índice de liquidez, la entidad registra un valor de 2.18, superior al mínimo requerido de 1.3, lo que evidencia una sólida capacidad para atender sus obligaciones de corto plazo, así como un adecuado respaldo de sus pasivos corrientes. Además, el índice de endeudamiento se sitúa en 39%, por debajo del límite máximo establecido de 60%; este resultado refleja una menor dependencia de recursos de terceros en la financiación de los activos, lo que reduce la exposición al riesgo financiero sin afectar la percepción de solvencia de la entidad.

En cuanto a la razón de cobertura de intereses, la entidad alcanza un valor de 16, superior al mínimo exigido de 2, lo que demuestra una capacidad holgada para cubrir los gastos financieros derivados de sus obligaciones, evidenciando estabilidad operativa.

Adicionalmente, la rentabilidad del patrimonio (ROE) se ubica en 13.46% superior al mínimo exigido de 5%, lo que refleja una alta eficiencia en la generación de utilidades a partir de los recursos propios. De manera complementaria, la rentabilidad del activo (ROA) alcanza un valor de 8% superior al mínimo exigido del 2%, evidenciando una gestión eficiente de los activos y una sólida capacidad de generación de beneficios.

Los indicadores analizados evidencian que la entidad presenta fortalezas significativas en liquidez, rentabilidad y capacidad de cobertura financiera, respaldando una posición financiera sólida y estable.

CONCLUSIÓN: De acuerdo con lo anterior, el proponente **CUMPLE** con los requisitos habilitantes de carácter financieros.

3.5. Personal Especializado:

*De acuerdo con lo establecido en el documento "Condiciones de la Contratación Convocatoria Abreviada N°012-2026", respecto del personal, "(...) El Proveedor deberá disponer de un **componente de personal especializado** para la gestión de vulnerabilidades, el cual será responsable de la operación continua del servicio. Este equipo deberá garantizar la gestión integral del ciclo de vida de las vulnerabilidades, desde su identificación hasta su cierre, incluyendo la validación de la remediación aplicada. De igual forma, deberá coordinar con las áreas técnicas de la entidad la implementación de controles correctivos, realizar seguimiento a los planes de acción y asegurar la trazabilidad de cada hallazgo.*

El personal asignado deberá contar con formación profesional en áreas afines a tecnologías de la información y ciberseguridad, así como certificaciones vigentes de reconocimiento internacional, tales como CEH, OSCP, CISA, CISSP o equivalentes. Adicionalmente, deberán acreditar experiencia comprobada en la ejecución de pruebas de seguridad, análisis de vulnerabilidades y gestión de riesgos tecnológicos. Deberá presentar certificado manifestando que cuenta con el equipo para garantizar la prestación del servicio y que cumple con las certificaciones y experiencia requerida

Documento aportado: "Certificación de idoneidad del personal, capacidad operativa y compromiso de confidencialidad.": Aporta certificación suscrita por el Representante Legal de la empresa, donde indican que cuentan con "el personal profesional asignado para la ejecución del contrato, que estos cuentan con formación académica en áreas afines a las tecnologías de la información y la ciberseguridad, así como con certificaciones vigentes de reconocimiento internacional, entre las que se incluyen CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), CISA, CISSP y/o sus equivalentes, según el perfil de cada profesional asignado.", lo anterior, con la finalidad de garantizar la adecuada prestación del servicio objeto del presente proceso de selección.

CONCLUSIÓN: De acuerdo con lo anterior, el personal requerido **CUMPLE** con los requisitos habilitantes de carácter técnico, toda vez que, se aportó por parte del proponente, certificado suscrito por el Representante Legal, donde manifiesta que cuenta con el equipo para garantizar la prestación del servicio.

3.6. Certificaciones solicitadas al proveedor:

Frente a lo requerido para garantizar la confidencialidad, integridad y disponibilidad de la información a la que tenga acceso en el desarrollo del contrato, así como del cumplimiento de las políticas de seguridad de la entidad y la normativa vigente aplicable, el proveedor presenta documento "**Certificación de idoneidad del personal, capacidad operativa y compromiso de confidencialidad.**", a través del cual manifiesta: "TERCERO – CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD Intrust Security S.A.S. se compromete a garantizar la confidencialidad, integridad y disponibilidad de toda la información a la que tenga acceso en desarrollo del contrato. En consecuencia: • Toda la información obtenida será

tratada como estrictamente confidencial y no será divulgada, cedida ni utilizada para fines distintos a los establecidos contractualmente. • El personal asignado suscribirá acuerdos individuales de confidencialidad antes del inicio de las actividades. • Se cumplirán en su totalidad las políticas de seguridad de la información de la entidad contratante, así como la normativa vigente aplicable, incluyendo la Ley 1581 de 2012 y demás disposiciones en materia de protección de datos personales y seguridad de la información.”

CONCLUSIÓN: De acuerdo con lo anterior, **CUMPLE** con los requisitos habilitantes de carácter técnico, toda vez que, se aportó por parte del proponente, certificado suscrito por el Representante Legal, donde manifiesta su compromiso de confidencialidad.

4. RESUMEN DE LA VERIFICACIÓN DE LOS REQUISITOS HABILITANTES

Los requisitos habilitantes son objeto de verificación, por lo tanto, únicamente se considera habilitado aquel oferente que cumpla con todos los requisitos solicitados. Se evaluarán como “Cumple”. En caso contrario, se evaluarán como “No Cumple” y, por tanto, no será objeto de evaluación en los requisitos de calificación, sin perjuicio de la subsanación que los oferentes puedan realizar en el término que otorgue Valor+ S.A.S.

N	Proponente	Verificación Jurídica	Verificación Técnica	Verificación Financiera	Verificación Organizacional	Verificación Equipo de Trabajo	Certificaciones solicitadas al proveedor
1	INTRUST SECURITY S.A.S.	CUMPLE	CUMPLE	CUMPLE	CUMPLE	CUMPLE	CUMPLE

5. CRITERIOS DE EVALUACIÓN:

Según lo establecido en el documento “Condiciones de la Contratación Convocatoria Abreviada N°012-2026 para el numeral 3. EVALUACIÓN DE PROPUESTAS”: (...) El criterio de selección que permita identificar la oferta más favorable para Valor+ S.A.S., será la ponderación de los siguientes criterios, siempre que haya cumplido con las especificaciones técnicas y requisitos habilitantes del proceso.

Lo anterior, de acuerdo con lo siguiente:

ÍTEMS DE EVALUACIÓN	PUNTOS
PRECIO: Oferta de menor valor	85
APOYO A LA INDUSTRIA NACIONAL	10
EMPRENDIMIENTO Y EMPRESAS DE MUJERES	5
TOTAL	100

(...)”

De acuerdo con lo señalado en el documento “Condiciones de la Contratación Convocatoria Abreviada N°012-2026 para el numeral 4. EVALUACIÓN DE PROPUESTAS”, se asigna puntaje de la siguiente manera:

5.1. Precio: Puntaje máximo 65 puntos

Se otorgarán **85 puntos** a la propuesta de menor valor. **Presenta propuesta técnica y económica por valor de \$55.800.000**

Ítem	Valor	Puntaje asignado
Precio	\$55.800.000	85

5.2. Apoyo a la Industria Nacional: Puntaje máximo 10 puntos

Se otorgarán **10 puntos** al proponente que aporte documento que demuestre que apoya a la Industria Nacional. **Aporta Camara de Comercio donde se evidencia que el domicilio principal es Medellín – Antioquia.**

N°	Proponente	Puntaje asignado
1	INTRUST SECURITY S.A.S.	10

5.3. Emprendimiento y Empresas de Mujeres: Puntaje máximo 5 puntos

Se otorgarán **5 puntos** al proponente que aporte documento que demuestre que apoya el Emprendimiento y Empresas de Mujeres. No aporta documento para este ítem.

N°	Proponente	Puntaje asignado
1	INTRUST SECURITY S.A.S.	0

6. RESUMEN DE PUNTAJE

Se relaciona el puntaje asignado al oferente, conforme con la propuesta y anexos presentados.

N°	Proponente	Criterio 1. Precio	Criterio 2. Apoyo a la industria nacional	Criterio 3. emprendimiento y empresas de mujeres	Puntaje	Observaciones
1	INTRUST SECURITY S.A.S.	85	10	0	<u>95</u>	No presenta documento que acredite el criterio 3

7. ORDEN DE ELEGIBILIDAD

Proponente	Orden de elegibilidad	Puntaje Total
INTRUST SECURITY S.A.S.	1	95

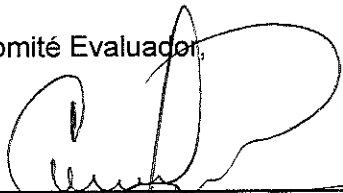
CONCLUSIÓN

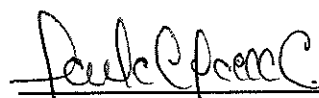
En conclusión, la propuesta presentada por la empresa **INTRUST SECURITY S.A.S.** alcanzó en la evaluación de los diferentes criterios establecidos un puntaje de **95 puntos**.

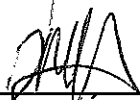
Teniendo en cuenta lo anterior, y en aplicación de lo establecido en el artículo 15 del Acuerdo de Junta Directiva N° 001 del 01 de octubre de 2022 “Manual Interno de Contratación de Valor+ S.A.S.”, modificado por el artículo segundo del Acuerdo de Junta Directiva N° 001 del 15 de abril de 2024, el

Acuerdo de Junta Directiva N° 002 del 26 de septiembre de 2024 y el Acuerdo de Junta Directiva N°001 del 17 de septiembre de 2025; a su vez, desarrollado por la Decisión Empresarial N° 048 del 31 de mayo de 2024 *"Instructivo del Manual de Contratación"*, modificada por la Decisión Empresarial N° 084 del 30 de septiembre de 2024 y la Decisión Empresarial N° 128 del 04 de noviembre de 2025; el comité evaluador recomienda suscribir con el proponente **INTRUST SECURITY S.A.S.** identificado con NIT. 901.380.604-6, el contrato que tiene por objeto: *"Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."*, en el marco del Contrato Interadministrativo N° 4600018598 cuyo objeto es: *"Servicios para la administración y operación de la mesa de servicios de la Gobernación de Antioquia, servicios de hosting corporativos y servicios de apoyo, para la apropiada operación de la plataforma tecnológica utilizada en la administración departamental."*

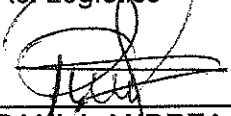
Comité Evaluador,



CARLOS ARTURO CORREA CORREA
Rol técnico

PAULA CRISTINA PARRA CARMONA
Rol jurídico

DANIELA MARIA LÓPEZ ANGULO
Rol Logístico

VERÓNICA RESTREPO ÁLVAREZ
Rol Financiero

PAULA ANDREA TORO TORRES
Rol Financiero



RE: Informe definitivo convocatoria abreviada N°12-2026

Desde Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

Fecha Mié 13/05/2026 9:25

Para Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

CC Sergio Andres Velez Upegui <coordinacion.mesa@valormas.gov.co>

Buen día Paula, Como has estado?

Se realiza validación y se aprueba el informe definitivo de la Convocatoria N° 12 -2026.

Gracias por tu atención y gestion.



Carlos Arturo Correa Correa

Profesional Universitario

carlos.correa@valormas.gov.co

Calle 42 # 52-27 Edificio Eoatel, Piso 3 Sector Alpujarra
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente del sistema.

De: Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

Enviado: Miércoles, 13 de Mayo de 2026 09:12

Para: Daniela Maria Lopez Angulo <daniela.lopez@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>; Sergio Andres Velez Upegui <coordinacion.mesa@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>

CC: Yeraldin Rua Pineda <yeraldin.rua@valormas.gov.co>; Hector Dario Yepes Vega <dir.contratacion@valormas.gov.co>

Asunto: Informe definitivo convocatoria abreviada N°12-2026

Cordial saludo,

Se comparte proyección del informe definitivo de la Convocatoria N° 12 -2026, la cual se construyo con el insumo enviado por cada uno de los participantes en el comité evaluador; se agradece validar y si es del caso aprobar o comentar con el fin de hacer los ajuste del caso.

Se agradece hacer esto antes de las 11 am, con el fin de revisar con el Director Jurídico Contractual y pasara a publicar antes de las 3:00 p.m.

Cordialmente,



Paula Cristina Parra Carmona

Profesional Especializada Grado I

paula.parra@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige.
Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución
o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos
notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.



Informe Definitivo - Convocatoria 012

Desde Compras Valor + 2 <compras2@valormas.gov.co>

Fecha Mié 13/05/2026 15:34

Para Sergio Mauricio Baron Vera <sbaron@intrustsecurity.co>

CC Compras Valor + <compras@valormas.gov.co>; Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>

📎 1 archivo adjunto (3 MB)

Informe definitivo Convocatoria Abreviada N°12-2026.pdf;

Cordial saludo,

Valor+ S.A.S. se encuentra adelantando el proceso de contratación cuyo objeto es **"Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."**

En este sentido, nos permitimos compartir el **Informe Definitivo** de conformidad con el cronograma establecido.

Quedamos atentos,



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.



Re: Informe Definitivo - Convocatoria 012

Desde Victor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

Fecha Mié 13/05/2026 15:52

Para Compras Valor + 2 <compras2@valormas.gov.co>

CC Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Compras Valor + <compras@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

Buenas tardes.

Dando respuesta a lo solicitado se carga documento al sitio web de la entidad.

Convocatoria Abreviada N°012-2026

Convocatoria Abreviada N°012-2026.

Objeto: "Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet"

1. Condiciones de la contratación
2. Cronograma Convocatoria Abreviada
3. CDP
4. Relación Experiencia Técnica
5. Formato Autorización de tratamiento de datos personales
6. Anexo Resolución de Injusticias
7. Formato Inhabilidades e Incompatibilidades
8. Formato Certificación de lavado de activos y financiación del Terrorismo - SARLAFT.
9. Formato Propuesta Económica
10. Respuesta a Observaciones - Convocatoria Abreviada N°012-2026.pdf
11. ACTA RECEPCIÓN DE PROPUESTAS.pdf
12. Informe Preliminar Convocatoria N°12-2026.pdf
13. Informe Definitivo Convocatoria Abreviada N°12-2026.pdf

Gracias por la atención prestada
Saludos.

**Victor Rodrigo Galvis Zuleta**

Contratista:
victor.galvis@valormas.gov.co
Carrera 53A #42-151, Torre B, Piso 6
Ed. Plaza de la Libertad
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

De: Compras Valor + 2 <compras2@valormas.gov.co>

Fecha: miércoles, 13 de mayo de 2026 a las 3:30 p.m.

Para: Victor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

CC: Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Compras Valor + <compras@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

Asunto: Informe Definitivo - Convocatoria 012

Cordial saludo,

Amablemente solicito tu ayuda por favor, para publicar el Informe Definitivo en la página web de la entidad.

Convocatoria Abreviada N°012-2026.

Objeto: “Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet.”

Quedo atenta,
Gracias.

**Daniela María López Angulo**

Profesional Universitaria
compras2@valormas.gov.co
Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra
Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.



Informe Definitivo - Convocatoria 012

Desde Compras Valor + 2 <compras2@valormas.gov.co>

Fecha Mié 13/05/2026 15:30

Para Víctor Rodrigo Galvis Zuleta <victor.galvis@valormas.gov.co>

CC Paula Cristina Parra Carmona <paula.parra@valormas.gov.co>; Compras Valor + <compras@valormas.gov.co>; Veronica Restrepo Alvarez <veronica.restrepo@valormas.gov.co>; Paula Andrea Toro Torres <gerencia.financiera@valormas.gov.co>; Carlos Arturo Correa Correa <carlos.correa@valormas.gov.co>

1 archivo adjunto (3 MB)

Informe definitivo Convocatoria Abreviada N°12-2026.pdf;

Cordial saludo,

Amablemente solicito tu ayuda por favor, para publicar el Informe Definitivo en la página web de la entidad.

Convocatoria Abreviada N°012-2026.

Objeto: "Prestación de servicios de vigilancia tecnológica en ciberseguridad para proteger a los diferentes proyectos de Valor + S.A.S mediante monitorización continua de internet y Darknet."

Quedo atenta,
Gracias.



Daniela María López Angulo

Profesional Universitaria

compras2@valormas.gov.co

Calle 42 # 52-27, Edificio Edatel, Piso 3 Sector Alpujarra,

Medellín - Colombia

Este correo electrónico es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.