No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
1.	**MNEMO COLOMBIA SAS** 14/11/2025 4:51:29 PM Referencia del mensaje: CO1.MSG.8770756	**Observación 1:** Se solicita amablemente a la entidad modificar el numeral 3.1.11 de la siguiente manera “Deberá contar con escaneos predefinidos para análisis rápidos de ciberhigiene, incluyendo una plantilla específica para 'Configuración SSL/TLS' que detecte cifrados débiles y problemas de certificados, y una plantilla de 'Auditoría de Configuración' para **encabezados** de seguridad web”. Con el propósito de clarificar la razón por las cuales son necesarias las plantillas indicadas.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que la solicitud busca dotar al IDU de capacidades robustas para la identificación proactiva de vulnerabilidades y malas configuraciones en sus aplicaciones web y RestAPI. La observación recibida, sugiere especificar la necesidad de contar con plantillas de escaneo predefinidas para 'Configuración SSL/TLS' y 'Auditoría de Configuración' lo cual puede sesgar el proceso a características puntuales de un fabricante determinado. Por tal razón y con el fin de garantizar la pluralidad de oferentes, **no se acoge la observación.**
2.	**MNEMO COLOMBIA SAS** 14/11/2025 4:51:29 PM	**Observación 2:** Se solicita amablemente a la entidad modificar el numeral 4.1.6 de la siguiente manera “La categorización deberá basarse en más de 200 campos de metadatos, y la plataforma deberá proveer una razón de atribución clara para cada activo descubierto, explicando por qué se considera que pertenece a la organización”. Lo	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que el requerimiento de una solución de "Seguridad de Superficie de Ataque Externa", tiene como objetivo proporcionar una visibilidad completa y precisa de todos los

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
	Referencia del mensaje: CO1.MSG.8770756	anterior con el propósito de destacar la profundidad del análisis y la transparencia de los resultados.	activos de la organización expuestos a Internet, incluyendo aquellos que pudieran ser desconocidos o no gestionados. Una simple lista de IPs o dominios sin contexto no es suficiente; la herramienta debe justificar porqué el equipo de seguridad debe tomar acciones y de esta manera reducir la carga de trabajo manual de verificación. Por ende, se acoge la observación, ajustando la redacción del numeral 4.1.6. de la ficha técnica, en los siguientes términos: 4.1.6 (Texto ajustado): La solución ofertada deberá categorizar los activos descubiertos con base en un modelo de datos enriquecido (más de 200 campos de metadatos). De manera fundamental, la plataforma deberá proporcionar, para cada activo, una razón de atribución clara y auditable que explique la evidencia por la cual se le vincula a la organización, permitiendo así una validación rápida y transparente de los resultados.
3	**MNEMO COLOMBIA SAS**	**Observación 3:** Se solicita amablemente a la entidad modificar el numeral 5.1.11 (sic) de la siguiente manera “La solución ofertada deberá Gestionar las Vulnerabilidades de todas las cargas de trabajo (CWPP), Gobierno y Cumplimiento de la infraestructura nube (CSPM), Gobierno	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La observación recibida, solicita que todos los componentes de la solución CNAPP (CWPP, CSPM, CIEM, etc.) sean provistos por un

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
	14/11/2025 4:51:29 PM Referencia del mensaje: CO1.MSG.8770756	de Identidades (CIEM), Análisis e Identificación de Comportamiento Malicioso (CDR) y Gobierno de Infraestructura como Código (IaC / DevSecOps) de la entidad, bajo una arquitectura CNAPP unificada y provista por el mismo fabricante; y provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades, La cual cuente con una cobertura para 50 activos por un periodo de 12 meses). Con el fin de garantizar que la solución CNAPP esté en la capacidad de correlacionar la información de cada uno de los módulos que lo componen y permitan una identificación cruzada de amenaza que al interactuar de manera conjunta aumentan el impacto del riesgo identificado.	único fabricante y bajo una arquitectura unificada. Este requisito busca evitar la complejidad operativa, los silos de información y los costos ocultos asociados a la integración de múltiples herramientas dispares. Con el fin de garantizar la adquisición de una plataforma CNAPP integrada y evitar la fragmentación tecnológica, se acepta la sugerencia del observador, ajustando la redacción del numeral 5.1.1 de la ficha técnica, en los siguientes términos: 5.1.1 (Texto ajustado): La solución ofertada deberá proporcionar una Plataforma de Protección de Aplicaciones Nativas en la Nube (CNAPP) nativamente unificada y provista por un único fabricante. Dicha plataforma deberá integrar, como mínimo, las siguientes capacidades en una única consola y bajo un modelo de datos correlacionado: Gestión de la Postura de Seguridad en la Nube (CSPM), Protección de Cargas de Trabajo en la Nube (CWPP), Gestión de Derechos de Infraestructura en la Nube (CIEM) y Seguridad de Infraestructura como Código (IaC). La solución deberá demostrar la capacidad de correlacionar hallazgos entre estos distintos módulos para identificar y priorizar rutas de ataque complejas en el entorno de nube. La cobertura mínima requerida es de 50 activos por un periodo de 12 meses.

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
4.	**MNEMO COLOMBIA SAS** 14/11/2025 4:51:29 PM Referencia del mensaje: CO1.MSG.8770756	**Observación 4**: Solicitamos amablemente a la entidad con la presentación de la oferta se deba adjuntar: Datasheets y/o manuales públicos del o los fabricantes donde se evidencie el cumplimiento punto a punto de los requerimientos técnicos.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite informar que no acoge la observación, atendiendo a que los datasheets o manuales públicos deberán ser aportados por el contratista, tal como se indicó en el numeral 3.1.18 de la ficha.
5.	**MNEMO COLOMBIA SAS** 14/11/2025 4:51:29 PM Referencia del mensaje: CO1.MSG.8770756	**Observación 5:** Solicitamos amablemente a la entidad en el marco del proceso, se adjunten certificados del fabricante o fabricantes donde se indique la tecnología ofertada, cantidades y tiempo; esto con el fin de garantizar que el oferente esta alineado el fabricante y lo ofertado cumpla con las expectativas de la entidad.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que la presentación de la certificación del fabricante asegura que la oferta está alineada con las políticas comerciales del mismo, que las cantidades y vigencias de las licencias son correctas, y que el proponente es un canal autorizado para comercializar y soportar la solución. Con el fin de fortalecer la trazabilidad de la oferta y garantizar el respaldo del fabricante, se acoge en su totalidad la sugerencia del observador, para lo cual se modifica el ítem Certificación del Fabricante del numeral 6.3, aspectos técnicos del Estudio Previo, el cual quedará así:

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
			El oferente deberá adjuntar una certificación emitida por el fabricante, con una vigencia no mayor a 30 días calendario anteriores a la fecha del cierre del proceso, donde se indique la tecnología ofertada y vigencia de las licencias.
6.	**IN TECH SAS** 14/11/2025 4:59:54 PM Referencia del mensaje: CO1.MSG.8770808	**Observación 6:** 1) Solicitamos a la entidad aclarar si la solución de seguridad en Nube Publica debe ser del tipo CNAPP y si esta debe tener las capacidades de DSPM.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que la solución requerida es una Plataforma de Protección de Aplicaciones Nativas en la Nube (CNAPP), unificada y provista por un único fabricante, la cual debe incluir la capacidad de gestionar la postura de seguridad de los datos (DSPM).
7	**IN TECH SAS** 14/11/2025 4:59:54 PM Referencia del mensaje: CO1.MSG.8770808	**Observación 7:** 2) Solicitamos a la entidad aclarar para las capacidades de conectores de terceros cuantos activos y que tipo de activos desde que fuente requiere conectar a la plataforma. ¿Entendemos que requieren unificar el riesgo?	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que requiere una solución que pueda actuar como el sistema central y autosuficiente para el descubrimiento, análisis y gestión de la ciber-exposición. Las capacidades de integración con conectores de terceros, descritas, no tienen como fin delegar el análisis a herramientas externas, sino enriquecer con contexto adicional el motor de riesgo de la propia plataforma.

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
			De la misma forma, no se especifica un número o tipo de activos a conectar, ya que la capacidad de integración requerida debe permitir la ingesta de datos de otras herramientas del ecosistema de seguridad de la Entidad (ej. EDR, SIEM, CMDB), tanto actuales como futuras. El detalle de las tecnologías específicas que conforman el ecosistema actual será compartido con el adjudicatario del contrato.
8	**IN TECH SAS** 14/11/2025 4:59:54 PM Referencia del mensaje: CO1.MSG.8770808	**Observación 8:** 3) La solución requerida de exposición de dominios requiere TakeDown? Tienen algún alcance requerido para la cantidad de takedown a realizar?	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite informar que sí se requiere que la solución tenga capacidad de Take Down, mediante créditos, los cuales sólo pueden ser consumidos hasta que el Take Down sea efectivo, esto debe estar soportado por el datasheet del fabricante. De otra parte, se aclara que el fabricante de la tecnología de exposición de dominios deberá ser diferente a la del firewall y WAF de la Entidad.
9	**IN TECH SAS**	**Observación 9:**	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:**

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
	14/11/2025 4:59:54 PM Referencia del mensaje: CO1.MSG.8770808	4) La solución requerida de exposición de dominios deberá ser implementada por personal en español directo de fabricante? Los servicios son remotos o presenciales?	La Entidad se permite aclarar que es un requisito que la implementación, configuración y transferencia de conocimiento de la solución sean ejecutadas directamente por el equipo de Servicios Profesionales del fabricante en idioma español. Asimismo, se confirma que los servicios pueden ser prestados de forma remota.
10	**IN TECH SAS** 14/11/2025 4:59:54 PM Referencia del mensaje: CO1.MSG.8770808	**Observación 10:** 5) Recomendamos amablemente que con el servicio se considere automatizar las capacidades de análisis mediante un servicio de autorespuesta para el personal de la entidad el cual sea basado en Inteligencia Artificial y garantize la rápida respuesta mediante canales como whastapp para consultas de estados actuales de ciberseguridad provenientes de las tecnologías consideradas. Esto permitira optimizar los tiempos de respuesta de los analistas internos de la entidad en un 99% ya que tendrán respuestas rápidas provenientes de datos consultados directos de las plataformas.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La entidad se permite indicar respecto a la observación que pretende que la misma esté inmersa en la solución, ya que lo que se busca con el servicio es incluir una solución basada en inteligencia artificial, la cual permita automatizar las consultas hacia la plataforma de gestión de exposición, donde a través vía WhatsApp se puedan consultar el estado actual de la ciberseguridad en la entidad.

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
11	**INGENIUM COLOMBIA SAS** 14/11/2025 5:33:05 PM Referencia del mensaje: CO1.MSG.8771229	**Observación 11:** 1. Se solicita amablemente a la entidad modificar el numeral 1.1.4 de la siguiente manera "La priorización de riesgos deberá basarse en un modelo de machine learning que analice más de 150 variables y la amenaza en tiempo real, generando un puntaje de riesgo dinámico para enfocar los esfuerzos de remediación y prevenir ataques". Lo anterior con el propósito de dotar a la herramienta de capacidades de última tecnología que no dependan de diccionarios y/o bases de datos estáticas, esta característica es básica en cualquier herramienta líder del mercado y permitirá a la entidad contar con última tecnología sin costos adicionales.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que el objetivo de la funcionalidad es anticipar riesgos por ende se requieren modelos de priorización basado en machine learning y/o IA que analice un amplio espectro de variables y el panorama de amenazas actual. Con el fin de garantizar que la herramienta adquirida cuente con capacidades de priorización inteligentes y predictivas, se acoge la observación y se modifica el numeral 1.1.4 de la Ficha Técnica, en los siguientes términos: 1.1.4 (Texto ajustado): La priorización de riesgos deberá basarse en un modelo de machine learning que analice por lo menos 150 variables y la amenaza en tiempo real, generando un puntaje de riesgo dinámico para enfocar los esfuerzos de remediación y prevenir ataques.
12	**INGENIUM COLOMBIA SAS**	**Observación 12:**	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:**

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
	14/11/2025 5:33:05 PM Referencia del mensaje: CO1.MSG.8771229	2. Se solicita amablemente a la entidad modificar el numeral 1.1.5 de la siguiente manera “Con el fin de garantizar la adquisición de una solución tecnológicamente madura, con una visión estratégica de mercado y una ejecución operacional comprobada, el fabricante de la solución ofertada deberá demostrar su liderazgo en el cuadrante de Gartner o Forrester a nivel de Vulnerability Management o Unified Vulnerability management en su ultima versión. El proponente deberá adjuntar la documentación o evidencia pública que certifique la posición de 'Líder' en ambos informes. El incumplimiento de este doble requisito de liderazgo”. Esto permitira tener una herramienta líder de mercado y con las condiciones minimas de reconocimiento y desarrollo que la entidad reuiere.(sic)	La Entidad se permite aclarar que la selección de un fabricante líder en la industria es un criterio objetivo que busca garantizar la adquisición de una solución tecnológicamente madura, con una visión estratégica de mercado consolidada y una capacidad de ejecución operacional comprobada por analistas de terceros imparciales. Con el fin de asegurar que la solución seleccionada represente la vanguardia del mercado y cumpla con las condiciones mínimas de reconocimiento y desarrollo que la Entidad requiere, se acoge la observación y se modifica el numeral 1.1.5 de la Ficha Técnica en los siguientes términos: 1.1.5 (Texto ajustado): Con el fin de garantizar la adquisición de una solución tecnológicamente madura, con una visión estratégica de mercado y una ejecución operacional comprobada, el fabricante de la solución ofertada deberá demostrar su liderazgo simultáneo en las evaluaciones más recientes de Gartner y Forrester para las tecnologías relevantes. Específicamente, deberá estar posicionado como 'Líder' en: • Gestión del Riesgo de Vulnerabilidades. • Gestión Unificada de Vulnerabilidades.

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
			El contratista deberá adjuntar la documentación o evidencia pública que certifique la posición de 'Líder' en ambos informes en su versión más reciente disponible antes de la suscripción del acta de inicio.
13	**INGENIUM COLOMBIA SAS** 14/11/2025 5:33:05 PM Referencia del mensaje: CO1.MSG.8771229	**Observación 13:** 3. Se solicita amablemente a la entidad modificar el numeral 1.3.1 de la siguiente manera “La plataforma deberá ser capaz de visualizar gráficamente las rutas de ataque que combinan vulnerabilidades, misconfiguraciones y problemas de identidad en activos de TI, nube y Directorio Activo, identificando los 'choke points' o activos críticos que interrumpen más rutas de ataque si son remediados, basado en un análisis de riesgo utilizando el framework de MITRE ATT&CK”. L Lo anterior con el propósito de garantizar que la herramienta esté en la capacidad de analizar la información de todos los módulos requeridos y no	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que el Análisis de Ruta de Ataque es una capacidad crítica requerida en este proceso. Su propósito es ir más allá de una simple lista de vulnerabilidades aisladas y proporcionar una visión contextualizada de cómo un atacante podría moverse a través de la infraestructura de la Entidad, combinando diferentes debilidades para alcanzar activos críticos. Con el fin de garantizar que la herramienta seleccionada posea las capacidades analíticas y de correlación necesarias para una gestión de riesgo contextualizada, **se acoge la observación** y se modifica numeral 1.3.1 de la Ficha Técnica, en los siguientes términos: 1.3.1.(texto ajustado) La plataforma deberá ser capaz de visualizar gráficamente las rutas de ataque que combinan vulnerabilidades, '*misconfiguraciones*' y

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
		únicamente de las capacidades para gestionar vulnerabilidades.	problemas de identidad en activos de TI, nube y Directorio Activo, identificando los '*choke points*' o activos críticos que interrumpen más rutas de ataque si son remediados, basado en un análisis de riesgo utilizando el framework de MITRE ATT&CK
14	**INGENIUM COLOMBIA SAS** 14/11/2025 5:33:05 PM Referencia del mensaje: CO1.MSG.8771229	**Observación 14:** 4. Se solicita amablemente a la entidad modificar el numeral 2.2.3 de la siguiente manera "Monitoreo pasivo: La tecnología de monitoreo pasivo deberá estar patentada y ser capaz de descubrir activos gestionados y no gestionados, incluyendo la detección de cambios en servicios y aplicaciones en tiempo real mediante el análisis de red de un puerto espejo". Lo anterior con el fin de clarificar las capacidades de monitoreo pasivo.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que el descubrimiento de activos es la base fundamental de cualquier programa de gestión de vulnerabilidades y ciber-exposición. Para lograr una visibilidad completa, es indispensable contar con múltiples métodos de descubrimiento. Dicha observación solicita características específicas que pueden sesgar el proceso a un fabrícate determinado. Por tal razón **no se acoge la observación.**
15	**INGENIUM COLOMBIA SAS**	**Observación 15:**	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:**

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
	14/11/2025 5:33:05 PM Referencia del mensaje: CO1.MSG.8771229	5. Se solicita amablemente a la entidad modificar el numeral 2.2.11 de la siguiente manera “El etiquetado deberá poder realizarse de forma manual y dinámica, basado en atributos del activo (ej. Sistema Operativo, software instalado) o en reglas de negocio (ej. criticidad del activo). La plataforma deberá contar con una métrica de Criticidad de Activos (ACR) que se ajuste automáticamente según reglas configurables”. Lo anterior con el fin de ampliar las capacidades de la herramienta únicamente a las capacidades de organización de resultados y orientarlas a una gestión granular de la plataforma.	La Entidad se permite aclarar que una gestión de vulnerabilidades eficaz va más allá de la simple identificación de hallazgos; requiere una organización granular y contextual de los activos para permitir una priorización y asignación de tareas eficientes. Con el fin de garantizar que la herramienta seleccionada ofrezca capacidades avanzadas de organización y contextualización de activos, se acoge la observación y se modifica el numeral 2.2.11. de la Ficha Técnica, en los siguientes términos: 2.2.11 (Texto ajustado): Poder etiquetar los activos por grupos en función de las necesidades de la organización para poder categorizar los resultados y asignar las tareas correspondientes. El etiquetado deberá poder realizarse de forma manual y dinámica, basado en atributos del activo (ej. Sistema Operativo, software instalado) o en reglas de negocio (ej. criticidad del activo). La plataforma deberá contar con una métrica de Criticidad de Activos (ACR) que se ajuste automáticamente según reglas configurables.
16	**INGENIUM COLOMBIA SAS**	**Observación 16:** 6. Se solicita amablemente a la entidad modificar el numeral 2.2.13 de la siguiente manera “La	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:**

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
	14/11/2025 5:33:05 PM Referencia del mensaje: CO1.MSG.8771229	solución deberá contar con una bóveda de credenciales interna y, además, integrarse de forma nativa con soluciones PAM líderes del mercado (ej. CyberArk, BeyondTrust) para realizar escaneos autenticados sin almacenar credenciales directamente en la plataforma". Lo anterior con el fin de dotar a la herramienta de capacidades que permitan generar automatismos y no dependan de librerías y/o credenciales quemadas de manera estática, las cuales pueden ser un punto de riesgo en la infraestructura.	La Entidad se permite aclarar que la gestión de las credenciales utilizadas para estos escaneos debe realizarse siguiendo las más estrictas prácticas de seguridad para evitar que la propia herramienta de gestión de vulnerabilidades se convierta en un punto de riesgo. La observación recibida, que propone especificar que la solución debe contar tanto con una bóveda de credenciales interna y segura como con la capacidad de integrarse de forma nativa con soluciones de Gestión de Acceso Privilegiado (PAM) líderes del mercado, solicita características específicas que pueden sesgar el proceso a un fabrícate determinado. Por tal razón **no se acoge la observación.**
17	**NEVITECH S.A.S** 14/11/2025 5:37:41 PM Referencia del mensaje: CO1.MSG.8771297	**Observación 17:** **1. Requerimiento Técnico:** El fabricante de la solución de ciber-exposición deberá estar como líder en Gartner, Forrester o IDC wave para tecnologías de ciber-exposición o Vulnerability Management.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que, si bien se valora y promueve la pluralidad de oferentes, es un deber fundamental de este proceso de contratación asegurar la adquisición de una solución que no solo cumpla con los requisitos técnicos punto por punto, sino que también demuestre una madurez, estabilidad y visión estratégica de mercado comprobadas.

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
		Observación: Se recomienda ajustar este requisito para no restringir la participación únicamente a fabricantes clasificados como “líderes” en Gartner, Forrester o IDC, ya que estas designaciones se basan en criterios comerciales y de mercado que no necesariamente representan el desempeño técnico real, la eficacia en la gestión de vulnerabilidades o la madurez funcional de la solución. En su lugar, es más adecuado solicitar evidencias objetivas y verificables de capacidades técnicas, tales como: • Cobertura de activos y alcance de descubrimiento. • Capacidades de priorización basada en riesgo. • Integraciones nativas con SIEM, SOAR, CMDB o scanners existentes. • Certificaciones, evaluaciones independientes o cumplimiento de estándares. • Arquitectura, escalabilidad y mecanismos de actualización continua. Esto garantiza pluralidad, evita sesgos de mercado y permite evaluar soluciones técnicamente robustas e innovadoras que pueden no estar clasificadas como	La observación recibida, que recomienda eliminar la exigencia de que el fabricante sea clasificado como 'Líder' por analistas como Gartner o Forrester, y sustituirlo por la evaluación de capacidades técnicas individuales, no es acogida por la entidad. Por las siguientes razones fundamentales: • El liderazgo como criterio objetivo de calidad integral • Coherencia con la naturaleza de la solución requerida • Los requisitos técnicos ya están detallados En consecuencia, la Entidad considera que eliminar la exigencia de liderazgo debilitaría significativamente los criterios de calidad y expondría a la organización al riesgo de adquirir una solución de nicho, con una hoja de ruta incierta o una capacidad limitada para evolucionar al ritmo del panorama de amenazas. Por lo tanto, no se acoge la observación y se mantiene la redacción del numeral 1.1.5 tal como fue ajustada en observación previa.

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
		"líderes" pero sí cumplir o superar los requerimientos tecnológicos del proyecto.	
18	**NEVITECH S.A.S** 14/11/2025 5:37:41 PM Referencia del mensaje: CO1.MSG.8771297	**Observación 18:** **2. Requerimiento técnico** Se requiere una solución de escaneo de vulnerabilidades, con el fin de visibilizar y priorizar todas las brechas de seguridad sobre la infraestructura. La cual cuente con una cobertura para 2200 activos por un periodo de 12 meses. **Observación:** Solicitamos a la entidad aclarar a qué hace referencia el término "activos": Es decir, si corresponde a sistemas operativos o dispositivos físicos, máquinas virtuales o aplicaciones o cualquier otro tipo de recurso, con el fin de dimensionar el impacto económico y costeo de la solucion.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que la pregunta sobre la definición del término "activo", el mismo debe ser entendido en su sentido más amplio, abarcando cualquier entidad tecnológica que posea una superficie de ataque y pueda ser evaluada por la solución. Esto incluye, pero no se limita a: Activos de TI tradicionales: Dispositivos físicos o virtuales con una dirección IP (servidores, estaciones de trabajo, dispositivos de red, impresoras, etc.). Recursos en la nube pública: Instancias de computación (ej. EC2, Azure VM), bases de datos gestionadas, funciones serverless y otros recursos IaaS/PaaS. Aplicaciones web: Identificadas por su nombre de dominio completamente cualificado (FQDN).

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
			Sistemas de IDENTIDAD: Usuarios activos dentro del Directorio Activo monitoreado. Contenedores: Imágenes de contenedores o contenedores en ejecución.
19	**NEVITECH S.A.S** 14/11/2025 5:37:41 PM Referencia del mensaje: CO1.MSG.8771297	**Observación 19:** **3. Requerimiento técnico** El fabricante de la solución deberá estar como líder en Gartner, Forrester o IDC wave para tecnologías de Ciberexposición o Vulnerability Management. **Observación:** Se solicita a la entidad ajustar el requisito para que el fabricante no deba estar exclusivamente en la categoría de “Líder” en Gartner, Forrester o IDC, sino que pueda encontrarse en cualquiera de las categorías evaluadas (Líder, Visionario, Retador o Nicho) dentro de los reportes para tecnologías de Ciberexposición o Vulnerability Management. La razón técnica es que estos análisis clasifican a los fabricantes según múltiples dimensiones — como estrategia, innovación, madurez del portafolio y enfoque de mercado—, y no todas ellas corresponden directamente al desempeño técnico o a la	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar, que la participación de fabricantes ubicados en cualquier otra de las categorías de los informes de analistas (Visionario, Retador o Nicho) No es aceptada por las razones que se exponen a continuación: El Liderazgo como sello de calidad integral y sostenibilidad: La designación de 'Líder' en los informes de analistas como Gartner y Forrester no es un criterio arbitrario ni puramente comercial. Representa la intersección indispensable entre una alta "Capacidad de Ejecución" y una alta "Integridad de la Visión". Mientras que otras categorías representan fortalezas parciales, también implican compromisos inaceptables para un proyecto de esta envergadura:

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
		capacidad real de cobertura, escalabilidad o automatización de la solución. Fabricantes ubicados en otras categorías pueden ofrecer capacidades técnicas igual de robustas o incluso más adecuadas para los requerimientos del proyecto, especialmente en entornos donde se valoran innovación, flexibilidad, integración o especialización. Permitir cualquier categoría garantiza pluralidad, competencia técnica equilibrada y mayor alineación con las necesidades reales de la solución, sin sacrificar la calidad tecnológica y a su vez dar apertura a la libre concurrencia y participación efectiva.	Un 'Visionario' puede ser innovador, pero carece de la capacidad de ejecución probada a escala. Un 'Retador' puede ejecutar bien, pero su visión estratégica es limitada, lo que genera incertidumbre sobre su evolución futura. Un 'Nicho' está demasiado especializado y no puede cumplir con el requisito de una plataforma integral y unificada. La capacidad de desarrollar, mantener y evolucionar una plataforma tan compleja y correlacionada es precisamente una de las características distintivas que los analistas reconocen en los líderes del mercado. Relajar este requisito sería contradictorio con el objetivo técnico principal del proceso. Por ende, **no se acoge la observación**
20	**NEVITECH S.A.S** 14/11/2025 5:37:41 PM Referencia del mensaje: CO1.MSG.8771297	**Observación 20:** **4. Requerimiento técnico** La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que ha recibido la observación que argumenta que el requisito de liderazgo del fabricante podría contravenir los principios de pluralidad de oferentes y selección objetiva. Dicha observación, que aborda el mismo principio fundamental discutido en las respuestas a las Observaciones 17 y

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
		El requisito que establece que la solución debe ser provista por un fabricante ubicado en el cuadrante de líderes de Gartner o Forrester para tecnologías de Vulnerability Risk Management, sumado a la exigencia de integración con múltiples categorías, limita la pluralidad de oferentes, ya que son muy pocos fabricantes los que cumplen simultáneamente con estas condiciones. Esto contraviene los principios de pluralidad de oferentes y selección objetiva establecidos en la Ley 80 de 1993 y la Ley 1150 de 2007. **Observación:** Se solicita modificar el criterio para permitir la participación de fabricantes reconocidos en informes de analistas en categorías afines o que demuestren capacidades equivalentes (integración, dashboards, gestión de exposición), garantizando así competencia y transparencia en el proceso.	19, no es acogida por las razones técnicas y de principio que se exponen a continuación: No Contravención de los principios de contratación: Los principios de pluralidad de oferentes y libre competencia no implican que la Entidad deba sacrificar la idoneidad y calidad técnica de la solución requerida. Inviabilidad de aceptar "capacidades equivalentes" subjetivas: Aceptar la sugerencia de evaluar "capacidades equivalentes" o el liderazgo en "categorías afines" introduciría un alto grado de subjetividad en el proceso de evaluación, lo cual sí podría contravenir el principio de selección objetiva. Por ende, **no se acoge la observación.**
21	**NEVITECH S.A.S** 14/11/2025 5:37:41 PM	**Observación 21:** 5. Experiencia requerida El proponente o el oferente deberá acreditar experiencia en al menos una de las dos viñetas: - Venta y/o renovación licenciamiento para gestión de Ciberexposición. -	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La entidad se permite informar que acoge parcialmente su observación para lo cual se modificará el ítem **Experiencia**

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
	Referencia del mensaje: CO1.MSG.8771297	Actualización y/o mantenimiento y/o soporte y/o licenciamiento y/o suscripción de sistemas y/o herramientas de Ciberexposición. Nota 1: Los Proponentes podrán acreditar experiencia proveniente de contratos ejecutados con particulares o Entidades Estatales de acuerdo con lo definido en el modelo tipo. Nota 2: No se requiere desagregar la experiencia en actividades. **Observación:** El término "ciberexposición" no corresponde a una categoría estandarizada en los marcos internacionales de ciberseguridad (ISO/IEC 27000, NIST CSF, ENISA). Por el contrario, ha sido un concepto de mercado acuñado por fabricantes, dentro de los cuales se encuentra TENABLE. Dicho concepto describe la visibilidad y gestión del riesgo asociado a los activos tecnológicos. No obstante, la gestión de ciberexposición se compone de capacidades reconocidas por la industria de la ciberseguridad, tales como la gestión de vulnerabilidades (Vulnerability Management), la gestión de superficie de ataque (ASM) y la evaluación de riesgo cibernético, las	**Habilitante** del numeral 6**.3. de Carácter Técnico** del Estudio Previo, el cual quedará así: El proponente deberá acreditar experiencia en contratos cuyo objeto sea igual o similar al objeto de la presente contratación. Para tales efectos, se entenderá como similar todo contrato que, dentro de su alcance, haya incluido una o varias de las siguientes actividades: GESTIÓN DE VULNERABILIDADES Y/O ANÁLISIS DE VULNERABILIDADES; Y/O, ADQUISICIÓN O IMPLEMENTACION DE SOFTWARE PARA LA CIBERSEGURIDAD; Y/O, PLATAFORMA DE ANÁLISIS DE VULNERABILIDADES; Y/O, HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES; Y/O, SOLUCIÓN DE ANÁLISIS DE VULNERABILIDADES Y/O GESTION DE SUPERFICIE DE ATAQUE Y/O GESTION DE CIBEREXPOSICION

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
		cuales son cubiertas por diversos fabricantes que implementan mecanismos equivalentes de identificación, priorización y mitigación de exposición cibernética. Por tanto, solicitamos a la entidad que la experiencia solicitada sea sobre estas capacidades reconocidas en la industria y no sea solicitadas certificaciones con terminología propia de un solo fabricante. La redacción que sugerimos se circunscribe a OBJETO, ALCANCE O ACTIVIDADES de: Venta y/o renovación licenciamiento para gestión de vulnerabilidades y/o gestión de superficie de ataque y/o evaluación de riesgo cibernético. • Actualización y/o mantenimiento y/o soporte y/o licenciamiento y/o suscripción de sistemas y/o herramientas de gestión de vulnerabilidades y/o gestión de superficie de ataque y/o evaluación de riesgo cibernético. Esta terminología sugerida comparte capacidades fundamentales, tales como descubrimiento de activos, priorización basada en riesgo, gestión de vulnerabilidades, visibilidad de superficies de ataque y monitoreo de exposición continua. Por lo tanto, reconocerlas como	

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
		equivalentes garantiza pluralidad, coherencia técnica y alineación con la terminología actual del mercado y la experiencia que hoy registran en sus certificados los diferentes oferentes del sector de la ciberseguridad.	
22	**Olimpia IT** 14/11/2025 5:49:36 PM Referencia del mensaje: CO1.MSG.8771394	**Observación 22:** **Ficha Técnica. Texto Observado: Numeral 1.** El fabricante de la solución de ciber-exposición deberá estar como líder en Gartner, Forrester o IDC wave para tecnologías de ciber-exposición o Vulnerability Management." **Observación/Solicitud:** Se solicita a la entidad modificar este criterio para permitir la participación de fabricantes reconocidos en informes de analistas en categorías relacionadas (como NDR, XDR o Exposure Management) o que demuestren validación tecnológica y casos de éxito, incluyendo tecnologías avanzadas basadas en Inteligencia Artificial (IA), garantizando así pluralidad de marcas innovadoras y fomentando la competencia en el proceso.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que ha recibido la observación que solicita ampliar el criterio de liderazgo del fabricante para incluir categorías de analistas relacionadas como Detección y Respuesta de Red (NDR), Detección y Respuesta Extendida (XDR) o tecnologías basadas en Inteligencia Artificial. Dicha observación, que nuevamente aborda el principio fundamental del criterio de liderazgo discutido en las respuestas a las Observaciones 17, 19 y 20, no es acogida por las siguientes razones técnicas. Incompatibilidad con el Objeto Técnico Central: El objeto del presente proceso es la adquisición de una plataforma de gestión de ciber-exposición y vulnerabilidades. El objetivo es anticipar, identificar, priorizar y gestionar las debilidades en la superficie de ataque de manera proactiva. La Innovación y la IA son Evaluadas dentro de la Categoría Correcta: Los informes de analistas para "Gestión Unificada de

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
			Vulnerabilidades" ya evalúan rigurosamente la innovación y el uso de tecnologías avanzadas como la Inteligencia Artificial y el Machine Learning por parte de los fabricantes. Necesidad de Mantener un Criterio de Comparación Homogéneo: Permitir que los proponentes presenten liderazgos en categorías funcionalmente diferentes haría imposible una evaluación objetiva y equitativa. Por ende, **no se acoge la observación.**
23	**Olimpia IT** 14/11/2025 5:49:36 PM Referencia del mensaje: CO1.MSG.8771394	**Observación 23:** **Ficha Técnica Numeral 2.1.1 Texto Observado:** Se requiere una solución de escaneo de vulnerabilidades, con el fin de visibilizar y priorizar todas las brechas de seguridad sobre la infraestructura. La cual cuente con una cobertura para 2200 activos por un periodo de 12 meses. **Observación/Solicitud:** Solicitamos a la entidad aclarar a qué hace referencia el término “activos”: si corresponde a sistemas operativos, dispositivos físicos, máquinas virtuales, aplicaciones o cualquier otro tipo de recurso, ya que esta definición impacta directamente la dimensionamiento, alcance y costos de la solución. Esta	La Entidad se permite aclarar que la definición y el modelo de licenciamiento del término "activo" ya han sido detallados en la respuesta proporcionada a la Observación 18. A modo de resumen y para mayor claridad, se reitera que, en el contexto de una plataforma de ciber-exposición unificada, el término "activo" se define como una entidad tecnológica única y abarca, entre otros, Activos de TI tradicionales (IPs), Recursos en la Nube, Aplicaciones Web (FQDNs) y Sistemas de Identidad (usuarios de Directorio Activo).

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
		precisión es fundamental para garantizar la correcta preparación de la oferta.	
24	**Olimpia IT** 14/11/2025 5:49:36 PM Referencia del mensaje: CO1.MSG.8771394	**Observación 24:** **Ficha Técnica Numeral 2.1.2. Texto Observado: "**El fabricante de la solución deberá estar como líder en Gartner, Forrester o IDC wave para tecnologías de Ciberexposición o Vulnerability Management. **Observación/Solicitud:** Mantener el liderazgo como condición única limita el proceso a unos pocos fabricantes y excluye tecnologías que ofrecen funcionalidades superiores y diferenciadoras, vulnerando los principios de pluralidad de oferentes y selección objetiva consagrados en el artículo 24 de la Ley 80 de 1993 y el artículo 5 de la Ley 1150 de 2007, que exigen reglas claras y objetivas para garantizar igualdad y competencia. Se solicita a la entidad modificar este criterio para permitir la participación de fabricantes reconocidos en informes de analistas en categorías afines o que demuestren innovación tecnológica y casos de éxito, asegurando así la pluralidad y fomentando la competencia en el proceso, en	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que la observación recibida, relacionada con el requisito de liderazgo del fabricante, aborda el mismo principio fundamental y los mismos argumentos legales ya discutidos en detalle en las respuestas proporcionadas a las Observaciones 12, 17, 19, 20 y 22. En aras de la brevedad y la coherencia, se remite al observador a dichas respuestas y se reitera la posición de la Entidad: El Criterio es Objetivo y Proporcional: La exigencia de liderazgo en los informes de analistas como Gartner y Forrester no es una barrera subjetiva ni desproporcionada. No Contravención de los Principios de Contratación: Tal como se justificó previamente, la normativa de contratación pública permite y fomenta el establecimiento de criterios de calidad exigentes que aseguren la idoneidad del proponente y la solución.

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
		cumplimiento de los principios de transparencia y eficiencia establecidos en la normativa aplicable	Inconsistencia con el Objeto Técnico: Permitir la participación de fabricantes líderes en "categorías afines" pero funcionalmente distintas (como NDR o XDR) desvirtuaría el objeto central del proceso. Por ende, **no se acoge la observación.**
25	**Olimpia IT** 14/11/2025 5:49:36 PM Referencia del mensaje: CO1.MSG.8771394	**Observación 25:** **Ficha Técnica Numeral 3.1.8Texto Observado:** El fabricante de la solución deberá estar como líder en Gartner, Forrester o IDC wave para tecnologías de Ciberexposición o Vulnerability Management. **Observación/Solicitud:** Esto limita la pluralidad de oferentes, debido a que son muy pocos los fabricantes que cumplen con esta condición, lo que restringe la competencia y contraviene los principios de pluralidad de oferentes y selección objetiva consagrados en el artículo 24 de la Ley 80 de 1993 y el artículo 5 de la Ley 1150 de 2007. Se solicita modificar este criterio para permitir la participación de fabricantes reconocidos en informes de analistas en categorías afines o que demuestren innovación tecnológica y casos de éxito, garantizando así transparencia y competencia en el proceso.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que la observación recibida para el numeral 3.1.8 aborda, una vez más, el requisito de liderazgo del fabricante, un principio que ha sido objeto de múltiples consultas y ha sido extensamente justificado. Como se ha detallado en las respuestas a las Observaciones 12, 17, 19, 20, 22 y 24, la exigencia de que el fabricante sea calificado como 'Líder' por analistas reconocidos es un criterio técnico objetivo, idóneo y proporcional al objeto contractual. Dicho requisito garantiza la adquisición de una solución tecnológicamente madura, con una visión estratégica y una capacidad de ejecución comprobadas, lo cual es de interés fundamental para la Entidad y está en pleno cumplimiento de los principios de la contratación pública. Por ende, **no se acoge la observación.**

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
26	**Olimpia IT** 14/11/2025 5:49:36 PM Referencia del mensaje: CO1.MSG.8771394	**Observación 26:** **Ficha Técnica Numeral 8.1.2. Texto observado:** La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management). **Observación/Solicitud:** El requisito que establece que la solución debe ser provista por un fabricante ubicado en el cuadrante de líderes de Gartner o Forrester para tecnologías de Vulnerability Risk Management, sumado a la exigencia de integración con múltiples categorías, limita la pluralidad de oferentes, ya que son muy pocos fabricantes los que cumplen simultáneamente con estas condiciones. Esto contraviene los principios de pluralidad de oferentes y selección objetiva establecidos en la Ley 80 de 1993 y la Ley 1150 de 2007. Se solicita modificar el criterio para permitir la participación de fabricantes reconocidos en informes de analistas en categorías afines o que demuestren capacidades equivalentes (integración, dashboards, gestión de exposición), garantizando así competencia y transparencia en el proceso.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite informar que la observación recibida para el numeral 8.1.2 es idéntica en su argumentación a múltiples consultas anteriores que cuestionan el requisito de liderazgo del fabricante (ver, entre otras, las respuestas a las Observaciones 12, 17, 19, 20, 22, 24 y 25). El requisito de liderazgo es un criterio técnico objetivo y no negociable, diseñado para asegurar la calidad, madurez y visión estratégica de la solución a adquirir, en total conformidad con los principios de la contratación pública. Por ende, **no se acoge la observación.**

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
27	**Olimpia IT** 14/11/2025 5:49:36 PM Referencia del mensaje: CO1.MSG.8771394	**Observación 27:** **Matriz 1 – Experiencia. Texto observado:** El proponente o el oferente deberá acreditar experiencia en al menos una de las dos viñetas:: • Venta y/o renovación licenciamiento para gestión de Ciberexposición • Actualización y/o mantenimiento y/o soporte y/o licenciamiento y/o suscripción de sistemas y/o herramientas de Ciberexposición Nota 1: Los Proponentes podrán acreditar experiencia proveniente de contratos ejecutados con particulares o Entidades Estatales de acuerdo con lo definido en el modelo tipo. Nota 2: No se requiere desagregar la experiencia en actividades." **Observación/Solicitud:** El término “ciberexposición” no corresponde a una categoría estandarizada en los marcos internacionales de ciberseguridad (ISO/IEC 27000, NIST CSF, ENISA), sino a un concepto de mercado introducido por algunos fabricantes —principalmente Tenable— para describir la visibilidad y gestión del riesgo asociado a los activos tecnológicos. No obstante, la gestión de ciberexposición se compone de capacidades reconocidas por la industria, tales como la gestión de vulnerabilidades (Vulnerability Management), la	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La entidad se permite informar que acoge parcialmente su observación para lo cual se modificará el ítem **Experiencia Habilitante** del numeral 6**.3. de Carácter Técnico** del Estudio Previo, el cual quedará así: El proponente deberá acreditar experiencia en contratos cuyo objeto sea igual o similar al objeto de la presente contratación. Para tales efectos, se entenderá como similar todo contrato que, dentro de su alcance, haya incluido una o varias de las siguientes actividades: GESTIÓN DE VULNERABILIDADES Y/O ANÁLISIS DE VULNERABILIDADES; Y/O, ADQUISICIÓN O IMPLEMENTACION DE SOFTWARE PARA LA CIBERSEGURIDAD; Y/O, PLATAFORMA DE ANÁLISIS DE VULNERABILIDADES; Y/O, HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES; Y/O, SOLUCIÓN DE ANÁLISIS DE VULNERABILIDADES Y/O GESTION DE SUPERFICIE DE ATAQUE Y/O GESTION DE CIBEREXPOSICION

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
		gestión de superficie de ataque (ASM) y la evaluación de riesgo cibernético, las cuales son cubiertas por diversos fabricantes que implementan mecanismos equivalentes de identificación, priorización y mitigación de exposición cibernética. Por tanto, solicitamos comedidamente que la experiencia solicitada sea sobre estas capacidades reconocidas en la industria y no sea solicitadas certificaciones con terminología propia de un solo fabricante. La redacción sugerida es la siguiente: Venta y/o renovación licenciamiento para análisis y/o gestión de vulnerabilidades y/o gestion de superficie de ataque y/o evaluaion de riesgo cibernético. • Actualización y/o mantenimiento y/o soporte y/o licenciamiento y/o suscripción de sistemas y/o herramientas y/o servicios de analisis y/o gestión de vulnerabilidades y/o gestion de superficie de ataque y/o evaluaion de riesgo cibernético."	
28	**O4IT** 14/11/2025 7:15:44 PM	**Observación 28:** Ficha Técnica y Pliego de Condiciones Requisitos funcionales y técnicos generales **Observación:** Solicitamos aclarar si es obligatorio que todas las capacidades descritas en la ficha técnica (gestión de	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que es un requisito obligatorio, fundamental y no negociable donde todas las capacidades solicitadas en la ficha técnica —incluyendo, pero no limitándose a,

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
	Referencia del mensaje: CO1.MSG.8771944	vulnerabilidades, escaneo de aplicaciones web, gestión de superficie de ataque externa, seguridad en la nube, auditoría de directorio activo, gestión de actualizaciones y monitoreo de credenciales expuestas) estén integradas nativamente en una única plataforma del mismo fabricante, o si se permite cumplir mediante la integración de soluciones especializadas de diferentes fabricantes, siempre que se garantice administración centralizada, reporting unificado y cumplimiento funcional.	la gestión de vulnerabilidades, escaneo de aplicaciones web, gestión de superficie de ataque externa, seguridad en la nube (CNAPP), auditoría de Directorio Activo y demás funcionalidades — estén nativamente integradas en una única plataforma, desarrollada y soportada por un único fabricante. Esta decisión estratégica se ha fundamentado y reforzado a lo largo de este proceso (ver, entre otras, las respuestas a las aclaraciones sobre los numerales 1.3.1, 5.1.1 y sobre conectores de terceros), y se basa en los siguientes principios técnicos irrenunciables: • Eliminación de Silos de Información • Necesidad de un Único Motor de Análisis de Riesgo • Eficiencia Operativa y Reducción de la Complejidad.
29	**O4IT** 14/11/2025 7:15:44 PM Referencia del mensaje: CO1.MSG.8771944	**Observación 29:** Ficha Técnica y Pliego de Condiciones Integración y administración de la solución **Observación:** ¿Se aceptan propuestas en las que la integración entre módulos se realice mediante APIs, conectores certificados o integración con plataformas SIEM (por ejemplo, IBM QRadar), aunque los módulos sean de diferentes fabricantes?	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** En coherencia con la respuesta proporcionada a la Observación 28, no se aceptan propuestas basadas en este modelo de integración. Es un requisito fundamental que todas las capacidades solicitadas en la ficha técnica sean componentes nativos de una única plataforma, desarrollada y soportada por un único fabricante.

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
30	**O4IT** 14/11/2025 7:15:44 PM Referencia del mensaje: CO1.MSG.8771944	**Observación 30:** Ficha Técnica y Pliego de Condiciones Requisitos de experiencia **Observación:** ¿La experiencia requerida puede acreditarse con contratos ejecutados en los que se hayan prestado servicios de manera individual (por ejemplo, gestión de vulnerabilidades, ethical hacking, monitoreo de AD), o es obligatorio que la experiencia sea en la entrega de una solución integral como la que describe la ficha técnica?	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La entidad se permite informar que se modificará el ítem **Experiencia Habilitante** del numeral **6.3. de Carácter Técnico** del Estudio Previo, el cual quedará así: El proponente deberá acreditar experiencia en contratos cuyo objeto sea igual o similar al objeto de la presente contratación. Para tales efectos, se entenderá como similar todo contrato que, dentro de su alcance, haya incluido una o varias de las siguientes actividades: GESTIÓN DE VULNERABILIDADES Y/O ANÁLISIS DE VULNERABILIDADES; Y/O, ADQUISICIÓN O IMPLEMENTACION DE SOFTWARE PARA LA CIBERSEGURIDAD; Y/O, PLATAFORMA DE ANÁLISIS DE VULNERABILIDADES; Y/O, HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES; Y/O, SOLUCIÓN DE ANÁLISIS DE VULNERABILIDADES Y/O GESTION DE SUPERFICIE DE ATAQUE Y/O GESTION DE CIBEREXPOSICION
31	**O4IT** 14/11/2025 7:15:44 PM	**Observación 31:** Ficha Técnica y Pliego de Condiciones Módulo de monitoreo de credenciales expuestas y data leaks. Observación: ¿El componente de monitoreo de credenciales expuestas y data leaks debe ser nativo de la	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** Se acepta incluir una tecnologia/fabricante adicional a la tecnología de gestión de ciberexposicion siempre y cuando cumpla con las

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
	Referencia del mensaje: CO1.MSG.8771944	plataforma de ciberexposición, o se acepta la integración con servicios externos de Digital Risk Protection/Threat Intelligence, siempre que se garantice la gestión centralizada de incidentes?	características técnicas solicitadas y estas puedan ser verificables mediante documentación pública del fabricante.
32	**O4IT** 14/11/2025 7:15:44 PM Referencia del mensaje: CO1.MSG.8771944	**Observación 32:** Ficha Técnica y Pliego de Condiciones Módulo de gestión de actualizaciones. Observación: ¿La solución de gestión de actualizaciones debe ser del mismo fabricante de la plataforma de ciberexposición, o se acepta una solución OEM o integración con herramientas líderes del mercado?	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite confirmar que es un requisito obligatorio que el módulo de gestión de actualizaciones sea del mismo fabricante de la solución de ciber-exposición o un producto OEM de fábrica integrado nativamente en su portafolio. Las razones para esta exigencia son las siguientes: • Cierre del Ciclo de Remediación • Intercambio de Inteligencia de Riesgo • Evitar la Fragmentación Operativa.
33	**O4IT** 14/11/2025 7:15:44 PM	**Observación 33:** Ficha Técnica y Pliego de Condiciones Arquitectura y modalidad de prestación del servicio.	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** Se confirma que se requiere una arquitectura híbrida, sujeta a las siguientes condiciones específicas que garantizan la centralización,

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
	Referencia del mensaje: CO1.MSG.8771944	**Observación:** ¿Se permite una arquitectura híbrida (SaaS + on-premises) para cumplir con todos los módulos, o es obligatorio que toda la solución sea 100% SaaS?	la seguridad y la cobertura total del entorno tecnológico de la Entidad: • Plano de Gestión y Análisis Obligatoriamente en la Nube (SaaS) • Componentes de Recolección de Datos (Sensores) con Despliegue Local (On-Premises)
34	**O4IT** 14/11/2025 7:15:44 PM Referencia del mensaje: CO1.MSG.8771944	**Observación 34:** Ficha Técnica y Pliego de Condiciones Integración con servicios profesionales y SOC **Observación:** ¿Se valorará la integración con plataformas SIEM líderes y la capacidad de orquestar la respuesta a incidentes desde un SOC propio, aunque la plataforma de ciberexposición no incluya nativamente todos los módulos?	**RESPUESTA OBSERVACIÓN ÁREA ESTRUCTURADORA Y ORDENADORA DEL GASTO:** La Entidad se permite aclarar que la capacidad de la plataforma para integrarse con herramientas líderes de SIEM y SOAR es un requisito importante, pero secundario y unidireccional. El propósito de esta integración es que la plataforma de ciber-exposición envíe sus hallazgos priorizados y contextualizados al SIEM/SOC para que el equipo de respuesta a incidentes pueda actuar sobre ellos. Sin embargo, esta capacidad de exportación de datos no sustituye ni compensa la falta de capacidades de análisis nativas en la propia plataforma. No Aceptación de Modelos Fragmentados: Tal como se ha establecido en las respuestas a las Observaciones 28 y 29, no se aceptarán propuestas donde la funcionalidad central de la plataforma sea suplida por la integración de módulos de diferentes fabricantes. La orquestación realizada por un SOC o la correlación

No.	EMPRESA OBSERVANTE	TEMA	RESPUESTA
			dentro de un SIEM no se consideran equivalentes a una plataforma de ciber-exposición nativamente unificada. La integración con el ecosistema SIEM/SOC es una capacidad de exportación requerida, pero no se valorará ni aceptará como un mecanismo para cumplir con los requisitos fundamentales de una plataforma de único fabricante con todos sus módulos nativamente integrados.

Los funcionarios y contratistas suscriben el presente documento de acuerdo con las funciones asignadas a cada una de las dependencias y la estructura organizacional del Instituto de Desarrollo Urbano - IDU

Se expide en Bogotá D.C., el 25 de noviembre de 2025.

MARYID BETTY CASTAÑEDA ROMERO
Directora Técnica Administrativa y Financiera

V.B. respuestas DTPS:	Juan de Dios Duarte Sánchez – Director Técnico de Procesos Selectivos.
Revisó respuestas DTPS:	DTPS 150 DTPS 128 DTPS 188 DTPS 021 (Articuladores)
Consolidó y elaboró respuestas DTPS:	DTPS 174 DTPS208 DTPS 215 NAAC
Transcribió respuestas Área Estructuradora y ordenadora del Gasto	DTPS 174 DTPS 208 DTPS 215 NAAC
Viabilizó respuestas Área Estructuradora y ordenadora del Gasto:	MATRIZ DE RESPUESTAS – No. radicado 202553600351233 del 24 de noviembre de 2025