	PREVISORA SEGUROS	**CONSOLIDADO RESPUESTA A OBSERVACIONES INVITACIÓN ABIERTA 023-2025**		
CONSECUTIVO	**OFERENTE**	**OBSERVACIÓN**	**REQUIERE ADENDA?**	**RESPUESTA DEFINITIVA**
1	NEWNET SAS	OBSERVACIÓN 1. Retiro del requisito de 'dos máximos niveles de membresía' por ser un filtro comercial restrictivo y no necesario: Causa legal/técnica: El requisito impone una jerarquía comercial propia de cada fabricante y ajena al mérito técnico exigible, lo cual afecta la pluralidad de oferentes y la selección objetiva al limitar la concurrencia a canales 'top tier'. El propio pliego ya exige ISO/IEC 27001:2022, perfiles habilitantes, ANS de disponibilidad (99,5%) y penalidades, controles que garantizan idoneidad y continuidad sin necesidad de un 'nivel máximo' de canal. Texto a reemplazar (extracto del pliego): 'Deberá adjuntar con su propuesta la certificación expedida por el fabricante, mayorista o representante oficial en Colombia, que lo acredite como canal autorizado en cualquiera de los dos máximos niveles de membresía, con una vigencia no mayor a dos (2) meses.' Propuesta de reemplazo: 'Carta de respaldo del fabricante o del distribuidor oficial que garantice suministro legítimo, acceso a parches/actualizaciones y soporte; acreditación vigente como partner autorizado sin limitar a niveles máximos; en consorcios/UT, la acreditación podrá aportarla el miembro responsable del componente técnico.' Argumento de la solicitud: Desde la perspectiva legal, el filtro comercial desproporcionado vulnera los principios de igualdad y pluralidad que informan el procedimiento de invitación abierta, pudiendo configurar direccionamiento. Desde la técnica, la entrega de parches y soporte se garantiza por contrato y por respaldo del fabricante, no por el 'tier'. Las obligaciones de seguridad y continuidad están consagradas en los ANS y en las penalidades de la minuta; establecer niveles máximos no añade garantías jurídicas ni técnicas adicionales, pero sí restringe el mercado.	NO	1) ISO/IEC 27001 (no se modifica): No procede su supresión ni ajuste: por tratarse de una solución SaaS/nube, la Circular Básica Jurídica de la SFC instruye que la entidad verifique que el proveedor en la nube cuente y mantenga vigente, al menos, la certificación ISO27001; es un requisito regulatorio para servicios cloud. 2) Niveles altos del cuadrante/ranking (se mantienen): Se conserva la exigencia de que la solución sea "líder" en al menos uno de los rankings (Gartner, Forrester Wave, GigaOm Radar o SC Media), tal como está en el pliego, porque asegura madurez, capacidad de ejecución y hoja de ruta, claves para cumplir el objeto, la disponibilidad 99,5% y la remediación/actualización continua. Los modelos de analistas definen públicamente qué implica ser líder (alta capacidad de ejecutar y visión en Magic Quadrant; metodología transparente en Forrester Wave; comparación de capacidades en GigaOm Radar), aportando un criterio técnico independiente y verificable.
2	NEWNET SAS	OBSERVACIÓN 2. Modulación de la 'vigencia máxima de dos meses' de la acreditación (actualidad razonable sin afectar concurrencia) La exigencia de una vigencia de dos (2) meses resulta excesivamente rígida y puede excluir proveedores con acreditaciones válidas que por ciclos administrativos del fabricante tengan emisión superior a dos meses, sin que ello implique pérdida de validez. El control de actualidad puede satisfacerse con verificación directa al fabricante o mayorista y con el contrato de soporte adjunto, evitando sacrificar pluralidad. *Texto a reemplazar (extracto del pliego):* '…con una vigencia no mayor a dos (2) meses.' Propuesta de reemplazo: 'Acreditación vigente del fabricante o verificación documental emitida por el fabricante/mayorista dentro de los últimos seis (6) meses, o certificación de soporte activa; en su defecto, confirmación electrónica del fabricante durante la etapa de verificación.' Argumento de la solicitud: Legalmente, el estándar de 'actualidad razonable' debe armonizarse con la realidad del mercado para no transformar un control de vigencia en una barrera de entrada. Técnicamente, la continuidad del soporte y la legitimidad del licenciamiento se acreditan por contratos activos y cartas del fabricante, no por una ventana temporal rígida de dos meses.'	NO	No se acoge; se mantiene la exigencia de acreditación como canal autorizado con vigencia no mayor a dos (2) meses. Es un requisito habilitante expreso (Cap. III, 3.2(b)) . La ventana uniforme de 2 meses garantiza actualidad verificable y homogeneidad para todos los oferentes, preserva la selección objetiva y asegura que el nivel de membresía y las facultades del canal estén vigentes al cierre; contratos de soporte o verificaciones externas no sustituyen el estándar habilitante definido en el Documento.

3	NEWNET SAS	OBSERVACIÓN 3. Protección de la pluralidad y selección objetiva frente a jerarquías comerciales heterogéneas Los 'niveles máximos' de membresía son conceptos no estandarizados: cada fabricante los define con criterios propios, por lo que su comparación entre oferentes y su relación con la calidad es discutible. Impulsar un criterio heterogéneo como habilitante puede generar ventaja indebida y limitar la participación de integradores con respaldo oficial pero sin 'top tier'. Texto a reemplazar Exigencia de 'dos máximos niveles de membresía' como habilitante. *Propuesta de reemplazo:* 'Aceptar respaldo oficial del fabricante/distribuidor y evidencia de soporte/actualizaciones (SLA, plan de parches) como criterios habilitantes objetivos, sin jerarquías comerciales.' Argumento de la solicitud: Legalmente, la selección objetiva reclama criterios verificables y comparables; las jerarquías comerciales no aseguran mayor seguridad ni mejor prestación. Técnicamente, los riesgos operativos se mitigan por la arquitectura, cifrado, integración, SAST/EH y ANS, todos ya exigidos en el pliego; el 'nivel máximo' no es un control de seguridad, sino un emblema comercial.	NO	No se acoge; se mantiene la exigencia de acreditación como canal autorizado en cualquiera de los dos máximos niveles de membresía. Es un requisito habilitante expreso (Cap. III, 3.2(b)) . Aunque los fabricantes definen jerarquías comerciales propias, el umbral de "dos máximos niveles" uniforma el estándar dentro de cada fabricante y garantiza capacidad de ejecución y rutas de escalamiento directo para cumplir obligaciones de gestión técnica, cifrado, actualización, remediación y continuidad del servicio (6.1(b), 6.3(b–d), 6.8(a–d)). Los controles invocados por el oferente (ISO 27001, ANS, SAST/EH) son complementarios, no sustitutivos del respaldo operativo derivado del nivel de membresía.
4	NEWNET SAS	OBSERVACIÓN 4. Claridad para proponentes plurales (consorcios/UT) y complementariedad técnica Causa: El pliego contempla la participación plural, pero no precisa expresamente que las certificaciones y respaldos puedan ser aportados por el integrante que ejecuta el componente técnico, lo cual desalienta la asociación y restringe el aprovechamiento de capacidades complementarias. Propuesta de reemplazo: Página 3 'En proponente plural (consorcio/UT), las certificaciones y respaldos requeridos podrán ser aportados por el miembro que ejecuta el alcance técnico relacionado; la verificación se realizará sobre el conjunto de la oferta y la matriz de responsabilidades.' Argumento de la solicitud (enfoque legal y técnico): Desde el plano legal, esta precisión protege la pluralidad y evita barreras indirectas; en lo técnico, favorece la suficiencia del equipo sin relajar controles de soporte ni seguridad establecidos en ANS/minuta.	NO	No se acoge la modificación propuesta; se mantiene el esquema habilitante vigente. El Documento ya regula la participación plural y la asignación de responsabilidades técnicas dentro del documento de constitución del consorcio/UT, exigiendo identificar actividades por miembro, porcentajes y reglas internas, lo que permite evaluar la oferta como conjunto sin alterar requisitos habilitantes (Cap. III, 1.1.5). En consecuencia, las certificaciones y respaldos exigidos deben estar vigentes y ser aportados por el PROPONENTE; en el caso de proponente plural, podrán estar en cabeza del integrante que ejecuta el componente técnico siempre que ello quede expresamente consignado en la matriz de responsabilidades del consorcio/UT y se acredite conforme al pliego (Cap. III, 3.2(a–b)).
5	NEWNET SAS	OBSERVACIÓN 5. Solicitud de Adenda: sustitución del criterio comercial por controles de licenciamiento y soporte verificables: Para blindar el proceso frente a riesgos operativos (licencias ilegítimas, falta de parches/soporte), se propone reemplazar el 'nivel máximo' por una combinación de controles objetivos: (i) carta de respaldo del fabricante; (ii) contrato de soporte activo; (iii) plan de gestión de parches y actualizaciones; (iv) verificación documental durante evaluación; (v) penalidades específicas por incumplimiento de soporte y seguridad ya previstas. Propuesta de reemplazo: 'Incluir en Adenda el paquete de controles (i–v) como habilitantes/obligatorios, eliminando la exigencia de jerarquía comercial.' Legalmente, se privilegian criterios objetivos y no discriminatorios alineados con selección objetiva; técnicamente, se fortalecen garantías directas de seguridad y continuidad sin restringir la participación. Conclusión y petición: Solicitamos la expedición de Adenda que elimine la exigencia de 'dos máximos niveles de membresía' y module la vigencia de la acreditación, sustituyéndolas por controles objetivos de licenciamiento y soporte que no restrinjan la concurrencia, y que se precise la aportación de certificaciones en consorcios/UT. Soporte	NO	No se acoge la solicitud de Adenda; se mantiene la exigencia habilitante de acreditación como canal autorizado en cualquiera de los dos máximos niveles de membresía y la vigencia no mayor a dos (2) meses, por tratarse de condiciones mínimas del pliego (Cap. III, 3.2(b)) , los controles objetivos propuestos (carta de respaldo, contrato de soporte activo, plan de parches, verificación documental y penalidades) ya se encuentran exigidos y verificables dentro de las obligaciones específicas de gestión técnica, cifrado, actualización y remediación (6.1–6.3, 6.8–6.11), los ANS y penalizaciones (Cap. III, 3.6), y las garantías del contrato (Cap. I, 8), por lo que no sustituyen el umbral de capacidad y ruta de escalamiento directo que acredita el nivel de membresía. Respecto de proponentes plurales, la aportación de certificaciones por el miembro responsable del componente técnico se evalúa conforme al documento de constitución y matriz de responsabilidades del consorcio/UT (Cap. III, 1.1.5), sin necesidad de modificación del texto
6	MULTISOFT	Observación No. 2: Respetuosamente solicitamos a la Entidad que, para los factores de calificación, de factor Trabajadores en condición de discapacidad y el factor Emprendimiento y empresa de mujeres, tenga la misma calificación, es decir; 6.25 cada uno, con el fin de asegurar que el proceso sea transparente y objetivo, garantizando la igualdad y libre participación a la contratación pública.	NO	No se acoge; la ponderación no puede igualarse porque los incentivos están regulados por ley y decreto con tratamientos distintos: (i) para emprendimientos y empresas de mujeres, la Ley 2069 de 2020 (art. 32) y su reglamentación en el Decreto 1860 de 2021 (que adiciona los arts. 2.2.1.2.4.2.14 y 2.2.1.2.4.2.15 al Decreto 1082) prevén requisitos diferenciales y puntajes adicionales hasta el 0,25% del total de puntos.

7	MULTISOFT	Observación No. 3: Respetuosamente solicitamos a LA PREVISORA, aclarar si el tiempo de antigüedad es contado a partir de la fecha de terminación de contrato.	NO	Para efectos de este proceso, el tiempo de antigüedad de la experiencia se computará a partir de la fecha de terminación efectiva del contrato acreditado lo definido de conformidad con el documento de condiciones definitivas.
8	MULTISOFT	Observación No. 4: Solicitamos gentilmente a la entidad dentro de la capacidad y experiencia del proponente en el servicio del presente proyecto, sea requerida la certificación MIEMBRO FIRST con el fin de ofrecer un servicio certificado en la detección y respuesta de amenazas bajo indicadores de compromisos y equipos enlazados a nivel global. teniendo en cuenta los siguientes aspectos, importancia y beneficios que brinda para la ejecución del presente proyecto. Acceso a Mejores Prácticas y Herramientas: FIRST reúne a equipos de respuesta ante incidentes de seguridad informática de todo el mundo. Al unirse, las organizaciones tienen acceso a las mejores prácticas, herramientas y recursos para mejorar su capacidad de respuesta ante amenazas. Cooperación y Coordinación: FIRST fomenta la cooperación y coordinación entre los equipos de seguridad. Esto incluye compartir información sobre amenazas, técnicas de mitigación y estrategias de respuesta. La colaboración entre miembros ayuda a fortalecer la seguridad global. Capacidad de Anticipar, Detectar y Responder: Diseñados para anticipar, detectar y responder a amenazas avanzadas. Inteligencia Colectiva: Ser parte de FIRST permite compartir información geográficamente y beneficiarse de la inteligencia colectiva. Los miembros pueden aprender de las experiencias de otros y colaborar en la lucha contra las ciber amenazas.	NO	No se acoge la solicitud; t no se incorpora "Miembro FIRST" como requisito habilitante. FIRST es una asociación global de equipos de **respuesta a incidentes** (CSIRT) basada en membresía voluntaria, y para este proceso no es una necesidad de la compañía.
9	MULTISOFT	6. Obligaciones específicas de EL OFERENTE y/o PROVEEDOR 6.1. Disponibilidad y entrega del servicio b) Garantizar una disponibilidad mínima del 99.5% del servicio, la cual debe ser reportada mensualmente. Observación No. 5: Respetuosamente solicitamos a la Entidad, indicar si se debe presentar un certificado de disponibilidad de la plataforma SaaS a ofertar para validar la disponibilidad mencionada, y aclarar si a nivel de servicio se deben establecer SLA para medir la disponibilidad del servicio	NO	Sí, el ANS de disponibilidad (99,5%) debe medirse mediante un SLA contractual y reportarse mensualmente por el proveedor; la Circular Básica Jurídica de la SFC exige que en servicios cloud/SaaS se garantice al menos 99,5% de disponibilidad y que ello quede pactado en el contrato dentro de las condiciones de servicio (capacidad, disponibilidad, tiempos de recuperación y resolución de incidentes).
10	MULTISOFT	d) Incluir e implementar un PLAN DE CONTINUIDAD Y RECUPERACIÓN DE DESASTRES medidas de contingencia para garantizar la continuidad operativa, PROBADO SEMESTRALEMNTE Observación No. 6: Respetuosamente solicitamos a la Entidad aclarar, si el oferente debe de diseñar e implementar el plan de continuidad de negocio y DRP sobre toda la infraestructura tecnológica. Si es así, por favor indicar sobre que activos o plataformas se requiere. Para diseñar estos planes, requerimos conocer: • Procesos críticos • Dependencias e impacto considerado • Definición de tiempos (RTO, RPO) • Estrategia de continuidad • Indicar Cumplimiento normativo (ISO 22301, NIST, etc.)., el plan de continuidad y el DRP	NO	El Plan de Continuidad del Negocio y el Plan de Recuperación de Desastres (BCP/DRP) requerido deberá diseñarse, implementarse y probarse únicamente sobre las soluciones ofertadas en el marco del presente proceso, y no sobre la totalidad de la infraestructura tecnológica de la Entidad.
11	MULTISOFT	6.5. Capacidades de descubrimiento y análisis a) Descubrimiento de activos mediante escaneo pasivo, activo (autenticado y no autenticado) así como a través de agente instalado. Observación No. 7: Respetuosamente solicitamos a la Entidad aclarar, si permiten la instalación de uno o varios sensores sobre la infraestructura de cliente, para ejecutar a cumplimiento los escaneos solicitados	NO	Se permite la instalación de uno o varios sensores sobre la infraestructura del cliente dentro del alcance del contrato y bajo los controles anteriores; el oferente deberá proveer el plan de despliegue y operación (roles, ventanas, evidencias) y embebido en el SLA el esquema de medición y reporte de descubrimiento/escaneo, sin embargo, dicho sensores deben ser solamente activados para el descubrimiento y mantenimiento de la infraestructura de manera periódica y previo visto bueno de los miembros de la reunión de cambios de la Gerencia de TI.

12	MULTISOFT	6.11. Análisis de código a) Realizar análisis de código estático (SAST) con informe técnico, enfocado en identificar malas prácticas, vulnerabilidades, errores de sintaxis, entre otros. b) Cubrir aplicaciones propias (hasta 20 mil líneas en Java) y hasta dos análisis anuales de aplicaciones a demanda. Observación No. 8: Respetuosamente solicitamos a la Entidad realizar las siguientes precisiones respecto al numeral 6.11, referente a análisis de código (SAST): • 9a. Aclarar la cantidad de códigos que desean sean analizados y la cantidad de líneas promedio por código, con el fin de contar con un alcance detallado que permita dimensionar correctamente el servicio. • 9b. Indicar si tienen un aproximado de la cantidad de códigos que podrían llegar a requerir de manera a demanda, así como confirmar si este costo debe considerarse únicamente bajo la modalidad de servicio a consumo, o si se debe incluir en la oferta base.	NO	De conformidad con el documento de condiciones definitivas , Capítulo VI – Obligaciones específicas, numeral 6.11, literales (a) y (b).el SAST cubre una (1) aplicación propia de hasta 20.000 LOC en Java y hasta dos (2) análisis anuales a demanda incluidos en la oferta; cualquier excedente (más LOC o más análisis) se atiende a consumo. El conteo de LOC se hace sobre código fuente (sin dependencias/binaries/comentarios).
13	MULTISOFT	3.4.3. Seguridad, gestión y reportes en idioma español 4) El servicio deberá incluir acciones de remediación basadas en la criticidad de las vulnerabilidades detectadas, el estado de los controles existentes y el nivel de obsolescencia tecnológica, permitiendo a través de la plataforma funcionalidades adicionales como la aplicación de parches y/o la ejecución de acciones de remediación temporales o definitivas para vulnerabilidades críticas o de alto impacto. Estas acciones deberán estar respaldadas por informes detallados que evidencien el tratamiento de cada hallazgo, su evolución y el estado actual de mitigación. Observación No. 9: Respetuosamente solicitamos a la Entidad reconsiderar este requerimiento, de modo que se pueda realizar la remediación mediante la integración nativa o modular con herramientas de remediación y/o parcheo (ej. SCCM, Ansible, para gestionar de forma automatizada o semiautomatizada la mitigación de vulnerabilidades críticas.	NO	No se modifica el requerimiento: la remediación “a través de la plataforma” puede cumplirse de forma nativa o mediante orquestación/integración certificada (API/connector) con herramientas de parcheo y automatización como SCCM, Ansible, Intune/WSUS, BigFix, siempre que: (i) se mantenga gobierno de cambios (aprobaciones, ventanas, rollback), (ii) controles de mínimo privilegio y trazabilidad, y (iii) informes en español que evidencien tratamiento, evolución y estado de mitigación por hallazgo, tal como exige el pliego.
14	MULTISOFT	3.6. Acuerdo de Nivel de Servicio (ANS). 2) El PROPONENTE debe garantizar una disponibilidad del 99.5% de la solución, en caso de que durante el servicio se presente alguna indisponibilidad, el porcentaje respectivo será descontado sobre el costo en la factura correspondiente a la siguiente vigencia de facturación. a) Entre el 99.5% y 99% penalización de 2%. b) Entre el 98.99 % y 98% penalización del 5%. c) Inferior al 98% penalización del 10% Observación No. 10: Respetuosamente solicitamos a la Entidad, confirmar si estos ANS están estipulados a la disponibilidad solo de la solución o también a la disponibilidad del servicio. También considerar los porcentajes de penalización por disponibilidad de la solución. a) Entre el 99.5% y 99% penalización de 1%. b) Entre el 98.99 % y 98% penalización del 3%. c) Inferior al 98% penalización del 5%	NO	El ANS de disponibilidad (99,5%): Aplica al uptime de la solución/plataforma SaaS (módulos, APIs y componentes bajo responsabilidad del proveedor). El servicio operativo (soporte, atención, remediación) se evalúa con SLA de respuesta y resolución, no con porcentaje de disponibilidad. Esto se pacta en el contrato para servicios en nube (condiciones de servicio, continuidad y monitoreo). [nist.gov] Penalizaciones: No se acoge la modificación; se mantienen los porcentajes previstos en el pliego (2%, 5%, 10%) sobre la factura de la siguiente vigencia, como mecanismo proporcional al impacto de indisponibilidad en procesos misionales. La CBJ de la SFC exige, además, que la disponibilidad mínima SaaS sea ≥ 99,5% y que el contrato contenga niveles de servicio y medidas de continuidad

15	MULTISOFT	Observación No. 11: Respetuosamente solicitamos a la Entidad confirmar, cuando se hace referencia a la contención o mitigación en tiempo real y a la implementación de la postura de seguridad (hardening) sobre los activos tecnológicos de La Previsora, cuáles son los criterios que deben tenerse en cuenta para su ejecución.	NO	Contención/mitigación en tiempo real: aislamiento de activos, bloqueo de IOC/TTP y segmentación, con acciones preautorizadas y trazabilidad en playbooks. Hardening: aplicar CIS Benchmarks (perfil L1/L2), mínimo privilegio (AC-6) y remediación de fallos (SI-2) con pruebas y registro en gestión de configuración. Parches de emergencia: priorizar, instalar y verificar actualizaciones o mitigaciones compensatorias según NIST SP800-40 Rev.4. Gobierno y alcance: cambios controlados, canales cifrados y continuidad; aplica sobre la solución SaaS y activos integrados definidos en el contrato/SLA, conforme CBJ SFC. lo anterior, conforme al Documento de Condiciones, los criterios para la contención/mitigación en tiempo real y el hardening se encuentran en Cap. 3.4.3(4), Cap. VI 6.3, y el ANS en Cap. III 3.6(2); y para hardening en Cap. VI 6.8–6.9 y Cap. VI 6.11. Estos numerales establecen remediación por criticidad, gobierno de cambios, evidencia en español, pruebas y verificación sobre los activos en alcance.
16	MULTISOFT	Observación No. 12: Respetuosamente solicitamos a la Entidad confirmar los requisitos de la solución y el porcentaje de crecimiento proyectado, dado que en el numeral 3.4.1 Requisitos a nivel de la solución, ítem 8, se indica un crecimiento anual del 5%, mientras que en el numeral 6.4 Cobertura de licenciamiento, se señala un crecimiento anual del 10%.	NO	Se confirma que los dos porcentajes aplican a aspectos distintos del alcance, por lo cual no hay contradicción: 3.4.1, ítem 8 (5%): crecimiento técnico de la solución (capacidad/escala de la plataforma: rendimiento, almacenamiento, eventos, activos monitoreados). y 6.4 Cobertura de licenciamiento (10%): crecimiento para dimensionamiento y cobertura de licencias/usuarios/activos (headroom contractual), a fin de evitar desabastecimiento de licencias en la operación. Regla de aplicación: dimensionar capacidad con 5% anual y licenciamiento con 10% anual, ambos calculados sobre la línea base del año anterior.
17	MULTISOFT	Observación No. 13: Respetuosamente solicitamos a la Entidad aclarar, de acuerdo con lo establecido en el numeral 6.7 Alertas e integración, si en caso de realizarse algún cambio en la plataforma SIEM se informará oportunamente al oferente, con el fin de validar la viabilidad de la integración o, en su defecto, confirmar si se continuará utilizando el SIEM Elastic.	NO	Cualquier cambio de la plataforma SIEM será informado oportunamente al proveedor para validar la viabilidad técnica de la integración y ajustar los conectores si aplica. Mientras no medie comunicación oficial, el SIEM de referencia es Elastic
18	MULTISOFT	Observación No. 14: Respetuosamente solicitamos a la Entidad aclarar, de acuerdo con lo establecido en el numeral 3.3 Recurso humano mínimo habilitante, en el cual se señala que “el proponente debe permitir realizar los cambios de personal que La Previsora S.A., por intermedio del supervisor del contrato y de manera motivada, le solicite, reservándose el derecho de exigir el reemplazo de cualquier persona vinculada al proyecto”, cuáles serán los criterios que La Previsora tendrá en cuenta para solicitar dichos cambios de personal.	NO	En atención al numeral 3.3 (Recurso humano mínimo habilitante), LA PREVISORA S.A. podrá solicitar cambios de personal de manera motivada cuando se evidencie: (i) incumplimiento del perfil mínimo o de las certificaciones exigidas para el rol; (ii) bajo desempeño o incumplimiento de entregables/cronograma/ANS; (iii) vulneración de políticas institucionales (seguridad de la información, confidencialidad, ética y SARLAFT); (iv) indisponibilidad o ausencias que afecten la continuidad operativa; (v) conflicto de interés sobreviniente; o (vi) conductas que pongan en riesgo la calidad del servicio. La solicitud se formalizará por escrito por el supervisor del contrato y el oferente deberá asignar un reemplazo con perfil igual o superior en un plazo máximo de cinco (5) días hábiles, conforme al ANS previsto en el numeral 3.6 (incisos 3 y 4), sin afectar la operación del servicio.

19	NEXTDATA	Observación 1 Solicitud sobre posibilidad de solución en modalidad SaaS Muy respetuosamente solicitamos a la entidad confirmar si es viable ofrecer la solución en modalidad cloud tipo SaaS, alojada en la nube del fabricante. Esta modalidad evitaría a la entidad incurrir en costos asociados a colocation y, adicionalmente, podría estar exenta de IVA según la normativa aplicable.	NO	La entidad confirma la viabilidad de ofrecer la solución en modalidad cloud tipo SaaS alojada en la nube del fabricante, en concordancia con lo previsto en el Cap. I, numeral 6.1 a) y el Cap. III, numeral 3.4.1 (1) que contemplan la entrega como servicio (SaaS); bajo esta modalidad no se requerirán recursos de colocation en el Datacenter de LA PREVISORA, por lo que no aplican los costos del numeral 6.2 salvo que el proponente incluya componentes on-prem. En cuanto al IVA, su tratamiento se sujetará a la normatividad tributaria vigente y a la naturaleza del servicio, conforme al Cap. II, numeral 6 (Impuestos); el oferente deberá discriminar y soportar la condición tributaria de su oferta (p. ej., "servicios de licenciamiento sin IVA" ya previstos en el presupuesto oficial – Cap. II, numeral 4), y la entidad procederá con las retenciones/causaciones que correspondan. En todo caso, la solución SaaS debe cumplir con los requisitos de seguridad, integración y ANS establecidos en el documento de condiciones.
20	NEXTDATA	Observación 2 Aclaración sobre el alcance funcional solicitado Respecto del Anexo N.° 7 –Condiciones Técnicas Obligatorias, solicitamos a la entidad confirmar si es correcto nuestro entendimiento: La entidad requiere una solución de análisis de vulnerabilidades que permita monitorear los activos integrados y entregar un análisis de la exposición del activo.	NO	Su entendimiento es parcialmente correcto: además de monitorear activos y analizar su exposición, la solución solicitada debe descubrir, validar, evaluar y priorizar vulnerabilidades en tiempo real, mantener inventario actualizado, clasificar por criticidad, detectar obsolescencia y fin de soporte, generar dashboards y reportes ejecutivos/técnicos, emitir alertas e integrarse con el SIEM; así mismo, debe incluir acciones de remediación (parcheo/mitigación y re-tests), pruebas de Ethical Hacking semestrales y puntuales sobre hallazgos críticos, análisis de código (SAST), apoyo en gestión de riesgos y capacitación (ver Cap. III, 3.4.1–3.4.6; Cap. I, 6.5–6.13; Cap. I, 6.8–6.9; Cap. IV, 1.2.3).
21	NEXTDATA	Observación 3 Solicitud de eliminación del requisito de análisis de día cero En relación con el Anexo N.° 7 – Condiciones Técnicas Obligatorias, solicitamos amablemente eliminar el requisito de análisis de día cero, dado que esta funcionalidad corresponde a soluciones de tipo Sandbox, las cuales no hacen parte del objeto de una solución de análisis de vulnerabilidades.	NO	Respuesta del Comité Evaluador Técnico: No procede eliminar el requisito. El análisis de día cero solicitado no implica la incorporación de soluciones sandbox; se entiende como la capacidad de la plataforma de gestión de vulnerabilidades para detectar tempranamente, correlacionar, priorizar y proponer acciones de mitigación/contención frente a amenazas sin parche disponible mediante fuentes de inteligencia y correlación con CVE/CWE/NVD, así como la ejecución de re-tests y medidas de hardening (ver Cap. III, 3.4.1 (3); Cap. I, 6.8–6.9; Cap. IV, 1.2.3). En consecuencia, el requisito se mantiene para garantizar cobertura ante vulnerabilidades emergentes sin exigir sandbox, y el oferente puede cumplirlo través de inteligencia de amenazas, priorización (CVSS temporal), virtual patching y controles de configuración seguros, conforme a las Condiciones Técnicas Obligatorias.
22	NEXTDATA	Observación 4 Aclaración sobre el crecimiento anual Frente al Anexo N.° 7 – Condiciones Técnicas Obligatorias, solicitamos confirmar si nuestro entendimiento es correcto en el sentido de que el crecimiento anual aplica únicamente a las 50 aplicaciones web	NO	SE ACLARA que el crecimiento anual del cinco por ciento (5%) aplica de manera integral a todas las soluciones y componentes ofertados (IP/host, servicios/aplicaciones web, agentes, integraciones y módulos de la plataforma), no exclusivamente a las 50 aplicaciones web. En consecuencia, dicho porcentaje deberá incorporarse en el dimensionamiento, licenciamiento y proyección de la totalidad de las soluciones incluidas en la oferta, conforme a lo establecido en el Anexo N.° 7 – Condiciones Técnicas Obligatorias.

23	NEXTDATA	Observación 5 Corrección del formato económico Respecto del Anexo N.° 8 – Formato de Propuesta Económica, solicitamos a la entidad verificar la información contenida en la hoja denominada “Hoja 1”, ya que no corresponde al formato requerido y podría generar errores en la presentación de las propuestas	SI	Gracias por la observacion y se modifica mediante adenda
24	NEXTDATA	Observación 6 Diferencias sobre capacidades y crecimiento anual entre documento En el Documento de Condiciones Definitivas se establece la inclusión de licencias para al menos 500 IP/Host y 50 servicios web, con un crecimiento anual del 10%, sin incremento proporcional de la tarifa. No obstante, en el Anexo N.° 7 solo se menciona el crecimiento para las 50 aplicaciones web. Solicitamos a la entidad confirmar el porcentaje real de crecimiento anual y unificar la información, dado que ambos documentos hacen referencia a valores distintos.	NO	SE ACLARA que el crecimiento anual será del cinco por ciento (5%) y aplicará de forma integral a todas las capacidades y componentes ofertados (≥500 IP/Host y 50 servicios/aplicaciones web, agentes, integraciones y módulos), sin incremento proporcional de la tarifa. Para unificar la información, la referencia al 10% del cuerpo del documento se ajustará mediante adenda y se alineará con el Anexo N.° 7 – Condiciones Técnicas Obligatorias; en consecuencia, se actualizarán los textos de Cap. I, numeral 6.4 a) y Cap. III, numeral 3.4.1 (8 a–b). Los oferentes deberán dimensionar, licenciar y proyectar toda la solución con el 5% anual durante la vigencia, manteniendo los topes presupuestales establecidos.
25	NEXTDATA	Observación 7 Alcance del monitoreo y escaneo continuo De acuerdo con el Documento de Condiciones Definitivas, solicitamos confirmar si es correcto nuestro entendimiento: Cuando se indica que la solución debe escanear y monitorear activos en IPv4 e IPv6 de manera continua, esto aplica para los 500 activos contemplados en la capacidad total.	NO	SE ACLARA que el requerimiento de “escanear y monitorear activos en IPv4 e IPv6 de manera continua” aplica a la totalidad de los activos cubiertos por el licenciamiento mínimo (≥500 IP/Host) y a los que se incorporen por el crecimiento anual del cinco por ciento (5%), sin incremento proporcional de la tarifa; ello incluye servidores, dispositivos de red y seguridad, periféricos y servicios integrados, usando los métodos de descubrimiento definidos (escaneo pasivo, activo autenticado/no autenticado y por agente), conforme a Cap. I, 6.10 a; Cap. III, 3.4.1 (8 a–e) y Cap. III, 3.4.6 (6 d), ejecutándose bajo ventanas de mantenimiento y políticas operativas que garanticen los ANS establecidos.
26	NEXTDATA	Observación 8 Aclaración sobre el perfil profesional solicitado En el Documento de Condiciones Definitivas, solicitamos confirmar si es correcto interpretar que, cuando se menciona el término “profesional”, se refiere a las carreras clasificadas como tales por el Sistema Nacional de Información de la Educación Superior (SNIES), incluyendo: Ingeniería eléctrica, electrónica, sistemas, telecomunicaciones y/o afines, así como las licenciaturas en las mismas áreas.	NO	SE ACLARA que el término “profesional” al que alude el Documento de Condiciones Definitivas corresponde a título universitario de pregrado reconocido por el SNIES en áreas afines al rol exigido (p. ej., Ingeniería de Sistemas, Electrónica, Eléctrica y afines), según los perfiles definidos para Analista de seguridad y Gerente de proyecto; en caso de títulos obtenidos en el exterior, se aceptan convalidaciones ante el Ministerio de Educación Nacional. Adicionalmente, para profesiones de la ingeniería es obligatoria la tarjeta profesional y el certificado de antecedentes del Consejo Profesional de Ingeniería, conforme a la nota prevista en el Cap. III, numeral 3.3 (Recurso humano mínimo habilitante). Los niveles técnico/tecnólogo no suplen el requisito cuando el perfil exige formación profesional.

27	NEXTDATA	Observación 9 Solicitud sobre posibilidad de solución en modalidad SaaS Muy respetuosamente solicitamos a la entidad confirmar si es viable ofrecer la solución en modalidad cloud tipo SaaS, alojada en la nube del fabricante. Esta modalidad evitaría a la entidad incurrir en costos asociados a colocation y, adicionalmente, podría estar exenta de IVA según la normativa aplicable. En caso de ser aceptada esta modalidad, la entidad podría suministrar los recursos necesarios para virtualizar una sonda, con los siguientes parámetros promedio: 4 vCPU, 4 GB RAM y 125 GB de almacenamiento	NO	SE ACLARA que la entidad sí admite la oferta en modalidad cloud tipo SaaS alojada en la nube del fabricante, conforme a Cap. I, 6.1 a y Cap. III, 3.4.1 (1); bajo esta modalidad no se requerirán recursos de colocation en el Datacenter de LA PREVISORA ni los costos del numeral 6.2, salvo que el proponente incluya componentes on-prem específicos. Respecto del IVA, su tratamiento se realizará según la normatividad vigente y la naturaleza del servicio, de acuerdo con Cap. II, 6 (Impuestos) y los rubros del presupuesto oficial (Cap. II, 4); en tal sentido, el oferente debe discriminar y soportar tributariamente su oferta (p. ej., servicios de licenciamiento sin IVA cuando aplique), y la entidad efectuará las retenciones correspondientes. En todo caso, la solución SaaS deberá cumplir integralmente los requisitos de seguridad, integración y ANS establecidos en el documento.
28	GL5	Observación 1 Documento: "Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf" Tema: “Limitación de Responsabilidad en Infraestructura”. Texto: 6.2. Responsabilidad sobre infraestructura a) Asumir todos los costos de aprovisionamiento […] de la infraestructura requerida en el Datacenter de LA PREVISORA S.A. b) Garantizar y asumir costos de la migración en caso de cambio de proveedor… Esta cláusula es muy favorable para la Entidad, pero jurídicamente puede ser considerada de difícil cumplimiento si no se acota. Exigir al proveedor asumir costos de migración "en caso de cambio de proveedor de Datacenter" (decisión de la Entidad) sin límites, podría generar desequilibrio económico del contrato a futuro, lo que habilitaría al contratista a reclamaciones posteriores. Acotar la obligación. Sugiero añadir: "limitado a los costos directos de la migración de la solución de seguridad contratada y hasta por un monto de [X]% del valor del contrato". Esto cierra la puerta a futuras demandas de restablecimiento del equilibrio económico contractual, haciendo la cláusula más robusta y	NO	SE ACLARA que la obligación prevista en el numeral 6.2 (Responsabilidad sobre infraestructura) aplica únicamente cuando la oferta incluya componentes on-prem de la solución (p. ej., appliances/VMs requeridos para el servicio); bajo modalidad SaaS (Cap. I, 6.1 a; Cap. III, 3.4.1), no se generan costos de colocation ni migración en el Datacenter de LA PREVISORA. En todo caso, la obligación de asumir costos de migración se acota a los costos directos, necesarios y verificables asociados exclusivamente a la solución de seguridad contratada, previa aprobación del plan de transición por el supervisor del contrato y sin incluir sistemas/servicios ajenos al alcance. Adicionalmente, se incorporará por adenda un tope porcentual (calculado sobre el valor del contrato y respetando los topes por vigencia) para dichos costos, con el fin de evitar desequilibrios económicos y mantener la robustez jurídica de la cláusula, sin desmejorar el objeto ni los ANS establecidos.
29	GL5	Observación 2 Documento: ANEXO No. 9 Matriz de riesgos precontractuales contractuales (003).xlsx. Tema: “Insuficiencia en la Tipificación del Riesgo de Fuga de Información (Confidencialidad). Texto: "Riesgos Operacionales: "Demoras en la entrega de la información necesaria…", "Incumplimiento del tiempo y alcance del proyecto…". (Snippet de Matriz)." La matriz de riesgos actual se enfoca excesivamente en el cumplimiento de cronogramas (riesgos típicos de obra o suministro). En un contrato de Gestión de Vulnerabilidades, el riesgo operativo/jurídico más grave no es el retraso, sino la fuga de información (Data Leakage) o el uso indebido de los hallazgos por parte del personal del contratista. El proveedor tendrá acceso a las "llaves del reino" (vulnerabilidades críticas). La matriz actual no parece ponderar este riesgo con la severidad adecuada. Agregar un Riesgo Específico en la etapa Contractual clasificado como: Riesgo: Divulgación no autorizada, copia o uso indebido de la información sobre vulnerabilidades de la Entidad. Consecuencia: Materialización de ciberataques por terceros, daño reputacional severo y sanciones de la SIC/Superfinanciera. Tratamiento: Exigencia de firma de Acuerdos de Confidencialidad (NDA) individuales por cada ingeniero del proveedor, implementación de controles DLP (Data Loss Prevention) en los equipos del proveedor y constitución de pólizas con amparo específico para responsabilidad civil por violación de datos	NO	SE ACLARA que la Entidad incorporará en la Matriz de Riesgos (Anexo N.º 9, versión actualizada) un riesgo específico contractual denominado: “Divulgación no autorizada, copia o uso indebido de información sobre vulnerabilidades”, con probabilidad media/alta y impacto catastrófico (afecta disponibilidad, integridad y confidencialidad), y tratamiento basado en: (i) NDA individuales firmados por cada ingeniero del proveedor; (ii) controles técnicos obligatorios en equipos del proveedor (cifrado de disco, DLP, bloqueo de puertos/transferencias, registro y auditoría de accesos, segregación de ambientes, principio de menor privilegio, transmisión por canales cifrados); (iii) integración con SIEM y reporte inmediato de incidentes conforme al ANS; (iv) refuerzo de cláusulas de confidencialidad, seguridad de la información y Habeas Data (Cap. I, 12; Cap. V – Minuta: Información confidencial, Seguridad de la información, Protección de datos personales); y (v) póliza con amparo específico de responsabilidad civil por violación de datos, además de los amparos de Cumplimiento y Calidad del servicio. Este ajuste quedará tipificado, ponderado y con responsable de seguimiento en la etapa contractual, sin modificar los topes ni el objeto del proceso. Envía tus comentarios en BizChat¿Cómo se implementan los controles DLP?¿Qué incluye la póliza de responsabilidad civil?

30	GL5	Observación 3 Documento: “Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf” Tema: “Criterios de Calificación vs. Requisitos Habilitantes (Servicio Forense).”. Texto: "Ítem 10: "Entrega de información técnica errada al contratista por parte de la Entidad" | Consecuencia: "se retrasa el proyecto" Aunque el riesgo está correctamente asignado a la ADRES, el tratamiento propuesto ("Control de calidad") es preventivo pero no correctivo. Legalmente, si la ADRES entrega información errada que causa retraso, esto no solo implica ajustar el cronograma, sino que podría generar reclamaciones por mayores permanencias (costos administrativos de personal ocioso) por parte del contratista. Agregar en la columna de "Tratamiento" o "Consecuencia" que, ante la materialización de este riesgo, se procederá a la suspensión del plazo o prórroga automática del cronograma por el tiempo equivalente al retraso, para blindar a la entidad de demandas por incumplimiento de plazos que no son culpa del contratista.	NO	SE ACLARA que en la Matriz de Riesgos (Anexo N.º 9) se incorporará tratamiento correctivo para el riesgo “Entrega de información técnica errada por parte de la Entidad”: suspensión del plazo o prórroga automática del cronograma por el tiempo equivalente al retraso, con reprogramación de hitos y sin aplicación de penalidades ni afectación de ANS al proveedor por causa atribuible a la Entidad. Este ajuste se formalizará por escrito mediante comunicación del supervisor del contrato, con acta de suspensión y/o otrosí, en armonía con la Minuta (p. ej., Cláusula Décima – Suspensión y Cláusula Cuarta – Plazo), de modo que se prevengan reclamaciones por mayores permanencias y se preserve el equilibrio contractual sin reconocimiento económico adicional, salvo que así se determine por el procedimiento contractual aplicable.
31	GL5	Observación No. 4 Documento: Proyecto de Pliego de Condiciones Tema: Indeterminación en la remuneración (Pago por horas vs. Pago por producto). Texto: "1.2.1. Se otorgarán 80 puntos al proponente que incluya en su propuesta un servicio especializado de Análisis Forense, el cual deberá garantizar la disponibilidad de personal especializado..." (Página 57).". Desde la óptica de la gestión del riesgo jurídico, existe una inconsistencia. Si el Análisis Forense es necesario para responder a incidentes de seguridad (cuyo impacto legal y reputacional es altísimo), no debería ser un factor opcional que otorga puntos ("calificable"), sino un requisito técnico mínimo ("habilitante"). Al dejarlo como puntaje, la Entidad asume el riesgo de adjudicar el contrato a un proveedor que no tenga capacidad forense, quedando desprotegida ante un incidente real. Reevaluar la matriz de contratación. Si la Entidad considera crítico tener capacidad de respuesta forense ante un incidente, este ítem debe moverse a los Requisitos Técnicos Habilitantes (Obligatorios). Si se mantiene como puntaje, se sugiere incluir una obligación contractual para que, en caso de que el adjudicatario no tenga este servicio in-house, deba demostrar un convenio de respaldo con un tercero para emergencias forenses, sin costo adicional para la entidad	NO	SE ACLARA que el servicio de análisis forense se mantiene como aspecto calificable (Cap. IV, 1.2.1) para incentivar diferenciación y valor agregado; sin embargo, para blindar la capacidad mínima de respuesta ante incidentes, se incorporará vía adenda una obligación contractual en la Minuta: el adjudicatario deberá garantizar atención forense mediante servicio propio o convenio de respaldo con tercero especializado, activable 24x7, sin costo adicional para la Entidad, con tiempo máximo de activación (p. ej., ≤ 4 horas), personal certificado (p. ej., CCE/CFCE/CHFI/GCFA o equivalentes) y procedimiento de preservación de evidencias; su incumplimiento dará lugar a correctivos conforme ANS. Este ajuste no modifica el objeto, los topes presupuestales ni la estructura de puntajes, y garantiza la capacidad operativa aun cuando el proponente no ofrezca el módulo forense como ítem calificable.
32	GL5	Observación No. 5. Documento:Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf Tema: Requisito de que la solución sea “Líder” en rankings (Gartner, Forrester, GigaOm, SC Media) Página: Cap. III (Certificaciones del Proponente): Texto del documento: “confirmación de que la solución... está como Líder en al menos uno de los siguientes rankings: Gartner, Forrester Wave, GigaOm Radar o SC MEDIA Awards.” Observación y Sustento Técnico: Solicitud 1: Agradecemos a la Entidad nos confirme si se acepta que la solución sea Líder o Strong Performer en cualquiera de los listados mencionados o bien que el oferente presente evidencia de evaluación analítica (brief de analista, datasheet y referencias de clientes) en lugar de exclusivamente la posición 'Líder' Solicitud 2: Solicitamos aclarar si se aceptan combinaciones (p. ej. plataforma base no líder + módulo de gestión de vulnerabilidades líder) y documentación que acredite integración y	NO	SE ACLARA que, manteniendo íntegramente las condiciones del documento, el requisito del Cap. III – Certificaciones del Proponente (numeral 3.2.c) exige que la solución ofertada esté como “Líder” en al menos uno de los listados indicados (Gartner, Forrester Wave, GigaOm Radar o SC Media Awards en las categorías de Vulnerability Management/Assessment), conforme a la edición más reciente publicada; no se aceptan equivalencias tales como Strong Performer, Challenger, Outperformer u otras categorías distintas a “Líder”. Respecto a combinaciones, solo serán admisibles cuando el módulo de gestión de vulnerabilidades que efectivamente se entrega a LA PREVISORA S.A. sea el reconocido como “Líder”, con integración nativa y soportada por el fabricante, y se anexe brochure/datasheet junto con carta firmada por el representante legal que detalle el cumplimiento funcional y la responsabilidad única de soporte; en caso contrario, el requisito se calificará NO CUMPLE. Esta respuesta no modifica el objeto, los puntajes ni los topes del proceso.

33	GL5	Observación No. 6. Documento: Tema: Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf. Página:Cap. 6.1 / 3.6 ANS Texto del documento: “Garantizar una disponibilidad mínima del 99.5%... penalizaciones: 99.5–99% = 2%; 98.99–98% = 5%; <98% = 10% (descuento sobre factura).” Observación y Sustento Técnico: Solicitud 1: Agradecemos a la Entidad nos confirme el método de cálculo de disponibilidad (fórmula), periodo de medición (mensual o calendario) y si existen ventanas programadas de mantenimiento excluidas (frecuencia, duración máxima por mes y aviso previo requerido). Solicitud 2: Solicitamos aclarar procedimiento de disputa de mediciones (evidencias a aportar) y si existen métricas de disponibilidad por componente (UI, API, escaneos) o sólo disponibilidad global	NO	SE ACLARA que la disponibilidad se mide mensualmente (período de facturación) con: Disponibilidad (%) = [Horas del mes – indisponibilidad atribuible al proveedor] / [Horas del mes] × 100; se excluyen mantenimientos programados y aprobados (máx. 2 al mes, ≤4 h acumuladas, aviso ≥72 h), fuerza mayor, cambios solicitados por la Entidad y fallas de terceros fuera del control del proveedor. Las disputas se presentan con evidencias dentro de 5 días hábiles y se cotejan con registros de la Entidad; de persistir diferencias, prevalecen los de la Entidad. La penalización aplica sobre la disponibilidad global del servicio; el proveedor reportará submétricas (UI, API, motor de escaneo, agentes) sin penalidad individual salvo impacto en la disponibilidad global
34	GL5	Observación No. 7. Documento: Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf Tema: Plan de Continuidad y Recuperación de Desastres Página: Cláusula 6.1.d / cláusulas de continuidad Texto del documento: “deberá incluir e implementar PLAN DE CONTINUIDAD Y RECUPERACIÓN DE DESASTRES ... PROBADO SEMESTRALEMNTE.” Observación y Sustento Técnico: Solicitud 1: Agradecemos a la Entidad nos confirme el tipo de pruebas exigidas (tabletop, simulacros, failover parcial o completo), el alcance mínimo (componentes incluidos) y si la Entidad coordina ventanas de pruebas o las define el proveedor. Solicitud 2: Solicitamos aclarar los RTO/RPO objetivo exigidos para los ejercicios y si las pruebas semestrales implican penalidades en caso de fallo en la ejecución del plan de PCN o si se requiere solo evidencias y mejoras	NO	SE ACLARA que el Plan de Continuidad y Recuperación de Desastres (Cap. I, 6.1.d) deberá probarse semestralmente mediante al menos: (i) ejercicio tabletop (de escritorio) y (ii) simulacro técnico con failover parcial o total sobre los componentes críticos de la solución (UI, API, motor de escaneo, agentes, integraciones –p. ej., SIEM– y repositorios de configuración), en ventanas coordinadas con el supervisor del contrato, definidas por el proveedor y aprobadas por la Entidad (preferiblemente fuera de horario hábil y con aviso ≥72 h), en armonía con el ANS (Cap. III, 3.6). Los RTO/RPO se proponen por el adjudicatario en el PCN y se aprueban por la Entidad (ver Minuta, Cláusula Cuadragésima Tercera – PCN); cada prueba debe entregar evidencias (plan, bitácora, resultados y mejoras). El fallo del ejercicio no genera penalidad por sí mismo; solo si impacta la disponibilidad efectiva del servicio en producción se aplican las penalidades del ANS (Cap. I, 6.1.b / Cap. III, 3.6), debiéndose re-ejecutar el ejercicio y cerrar hallazgos dentro del plazo acordado.
35	GL5	Observación No. 8. Documento: Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf Tema: Cobertura de licenciamiento: 500 IP/HOST y 50 servicios web; crecimiento anual y “Sin incremento proporcional de tarifa Página: Cap. 6.4 / 3.4.2 Texto del documento: “Incluir licencias para al menos 500 IP/HOST y 50 servicios web, con crecimiento anual del 10%/5%. Sin incremento proporcional de tarifa.” Observación y Sustento Técnico: Solicitud 1: Agradecemos a la Entidad nos confirme la definición operativa de 'IP/HOST' (servidor virtualizado, contenedor, IP pública/privada) y cuál fórmula se utilizará para el cómputo mensual/reportado. Solicitud 2: Solicitamos aclarar la discrepancia de crecimiento anual indicada en distintas secciones (10% vs. 5%) y si la Entidad acepta un mecanismo de ajuste en caso de crecimiento excepcional o cambios tecnológicos que incrementen el conteo de activos >15% anua	NO	SE ACLARA que, manteniendo las condiciones del documento, por IP/HOST se entiende cada activo único gestionado por la plataforma (servidor físico/virtual, dispositivo de red/seguridad, periférico), contabilizado una sola vez aunque tenga múltiples IP (pública/privada); los contenedores solo se cuentan cuando poseen IP propia y son gestionados individualmente. El cómputo mensual se realizará sobre el número de activos distintos que registren al menos una interacción (escaneo, telemetría o hallazgo) en el período, de duplicados por identificadores (hostname/MAC/agentID); para servicios web, se contará la URL/aplicación distinta escaneada. Respecto al crecimiento, se unifica en cinco por ciento (5%) anual y aplica de forma integral a la cobertura (≥500 IP/HOST y 50 servicios/aplicaciones web), sin incremento proporcional de tarifa; la referencia al 10% se ajustará por adenda. Ante crecimientos extraordinarios (>15%) por cambios tecnológicos, se requerirá autorización previa y plan de ajuste, enmarcados en los topes por vigencia; la Entidad podrá priorizar/diferir activos o tramitar licencias adicionales mediante el mecanismo contractual correspondiente, sin afectar la regla de crecimiento ordinario del 5%.

36	GL5	Observación No. 9. Documento: Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf. Tema: Pruebas de Ethical Hacking — alcance y número de activos (2 pruebas anuales, hasta 10 activos por prueba). Página: Cap. 6.9 / 3.4.2 Texto del documento: “Realizar dos pruebas de Ethical Hacking (una por semestre), tipo caja gris, sobre hasta 10 activos.” Observación y Sustento Técnico: Solicitud 1: Agradecemos nos confirme la definición de 'activo' para las pruebas (IP, dominio, aplicación, subdominio, endpoint) y el criterio para selección (la compañía selecciona o se acuerda lista conjunta) Solicitud 2: Solicitamos aclarar la política de re-test (plazos, ejemplos de evidencia) y si los retests se consideran dentro de las dos pruebas anuales o se realizan a demanda sin costo adicional	NO	SE ACLARA que, para efectos de las pruebas de Ethical Hacking tipo caja gris, el término “activo” comprende hosts y servicios identificables y escaneables por la solución: servidores físicos/virtuales, aplicaciones/URL (dominio/subdominio), endpoints/dispositivos de red/seguridad y bases de datos (conforme Cap. I, 6.9 y Cap. III, 3.4.4). La selección de hasta 10 activos por prueba será definida por LA PREVISORA S.A. (internos o externos) y podrá acordarse técnicamente con el proveedor, manteniendo la decisión final en cabeza de la Entidad (Cap. III, 3.4.6, 6 a). Los re-tests se ejecutan a demanda hasta confirmar la remediación y no se contabilizan como una de las dos pruebas semestrales; deben entregar evidencias (bitácora, reporte comparativo, cierre de hallazgos en la plataforma y/o prueba técnica) dentro del plazo acordado en el plan de acción (Cap. I, 6.9 b; Cap. III, 3.4.6, 6 c; Cap. III, 3.5 – Entregables, ítem 6), sin costo adicional distinto al servicio ofertado.
37	GL5	Observación No. 10. Documento: Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf. Tema: Análisis de código (SAST) — cobertura y acceso al repositorio (aplicaciones propias hasta 20k líneas Java; 2 análisis a demanda). Página: Cap. 6.11 / 3.4.2 Texto del documento: “Realizar análisis SAST… aplicaciones propias (hasta 20 mil líneas en Java) y hasta dos análisis anuales a demanda.” Observación y Sustento Técnico: Solicitud 1: Agradecemos nos confirme el nivel de acceso que LA PREVISORA habilitará al proponente (acceso a repositorios GitHub, ramas, pipelines CI/CD, o se entregarán artefactos compilados) para realizar SAST correctamente Solicitud 2: Solicitamos aclarar el alcance de análisis a demanda (tipos de lenguaje admitidos) y si existe alguna restricción legal o de terceros para el escaneo de repositorios administrados por	NO	Solicitud 1 (acceso para SAST): LA PREVISORA habilitará acceso de solo lectura al código fuente mediante repositorio GitHub institucional (rama(s) designadas) o entrega de snapshot cifrado (ZIP) por canal seguro, según el caso. No se otorga acceso a secretos, pipelines CI/CD ni credenciales; cualquier integración SAST en CI/CD, si se propone, será opcional, con tokens de servicio de mínimo privilegio y aprobación previa del supervisor (en línea con Confidencialidad, Seguridad de la Información y Protección de datos de la Minuta). Artefactos compilados (binarios) no son suficientes para SAST; el análisis exige código fuente. Solicitud 2 (alcance a demanda y restricciones): Los dos análisis anuales a demanda podrán cubrir Java y otros lenguajes comunes (C#/.NET, JavaScript/TypeScript, Python, PHP, Go, entre otros) siempre que el fabricante/herramienta soporte el lenguaje y se cumplan las Condiciones Técnicas. Si el repositorio es administrado por un tercero, se requiere autorización escrita del titular, NDA y acceso de lectura; alternativamente, el tercero puede entregar el informe SAST con evidencias (lista de hallazgos, mapeo CWE, severidad CVSS, recomendaciones y trazabilidad) para validación. En todos los casos, el proveedor deberá entregar informe técnico, proponer remediaciones y realizar re-test para confirmar cierre de hallazgos, conforme a Cap. I, 6.11 y Cap. III (Condiciones Técnicas/Entregables), sin costos distintos a los ofertados.

38	GL5	Observación No. 11. Documento: Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf Tema: Propiedad intelectual y cesión de código fuente. Riesgo por cláusula amplia. Página: Cláusula cuadragésima séptima/tercera Texto del documento: "La propiedad intelectual de todo material creado… será de propiedad de LA PREVISORA S.A… suscripción del contrato de cesión de derechos será requisito para pago del último sprint." Observación y Sustento Técnico: Solicitud 1: Agradecemos confirmar si la cláusula de propiedad intelectual distingue entre software desarrollado ex-novo y software preexistente del proveedor, y si se aceptan licencias de uso para componentes preexistentes Solicitud 2: Solicitamos aclarar el mecanismo para la entrega de código fuente (formatos, repositorios, documentación) y si el pago final podrá condicionarse a entrega de documentación técnica en lugar de cesión total de IP de componentes preexistente	NO	SE ACLARA: (i) La propiedad intelectual distingue entre material creado ex-novo para el contrato (informes, guías, scripts, integraciones y/o desarrollos específicos), cuya cesión de derechos patrimoniales a LA PREVISORA S.A. procede conforme a la Minuta – Propiedad intelectual/Cesión (Cláusulas 40–41) y el Licenciamiento (Cláusula 42); y componentes preexistentes/comerciales del proveedor o fabricante, que no están sujetos a cesión ni entrega de código fuente y se usan bajo licencias de uso vigentes. (ii) La entrega de código fuente aplica solo a desarrollos ex-novo: se realizará en repositorio Git institucional (o paquete cifrado), con documentación técnica completa (README, arquitectura, instalación, dependencias, versionado, pruebas y manuales). El pago final se condiciona a la entrega de la documentación técnica y a la cesión de los desarrollos ex-novo; para componentes preexistentes, se exige evidencia de licencias, documentación de integración y compatibilidad, sin requerir cesión total de IP del software comercial. Esta precisión no modifica el objeto, puntajes ni topes del proceso y mantiene las condiciones del documento.
39	GLOBALTEK	1. Solicitud de ampliación del período de validez de experiencia: de 5 a 8 años El documento de la invitación limita la validez de las certificaciones de experiencia a contratos ejecutados en los últimos cinco (5) años. Sin embargo, en el sector de la ciberseguridad las metodologías base para ethical hacking, pruebas de penetración, análisis de vulnerabilidades, hardening, revisión de código seguro y simulación de incidentes mantienen continuidad técnica sustentada en estándares internacionales (OWASP, NIST, CIS, MITRE ATT&CK). Por esta razón, limitar la antigüedad a 5 años no representa una mejora en la selección objetiva, ni garantiza mayor idoneidad del contratista. Con fundamento en el principio de proporcionalidad (Ley 80, art. 24) y en el deber de no restringir irrazonablemente la participación (Ley 80, art. 25.1), solicitamos ampliar el período de experiencia al menos a 8 años, lo que permite reflejar de manera más precisa la trayectoria del mercado sin sacrificar calidad ni pertinencia técnica.	NO	SE ACLARA que, conforme al Cap. III, numeral 3.1 (Experiencia del Proponente), la antigüedad máxima de cinco (5) años para las certificaciones de experiencia se mantiene. Esta ventana garantiza pertinencia técnica frente a la rápida evolución de tecnologías, arquitecturas y amenazas, preserva la selección objetiva y la proporcionalidad del requisito (sin restringir irrazonablemente la participación, dado que admite hasta tres certificaciones y actualización por SMMLV/TRM según el documento). Los oferentes pueden adjuntar experiencias adicionales (≥5 años) a título informativo, pero la verificación habilitante se efectuará exclusivamente sobre contratos dentro del quinquenio establecido, sin modificación de las condiciones, puntajes ni topes del proceso.
40	GLOBALTEK	2. Solicitud de permitir hasta 4 certificaciones para las MiPymes El requisito actual limita el número de certificaciones a máximo tres (3), lo que genera una barrera desproporcionada para las MiPymes cuyo modelo de operación se caracteriza por contratos medianos distribuidos a lo largo del tiempo. La Ley 905 de 2004, en desarrollo de la Ley MiPymes, establece la obligación del Estado de promover su participación efectiva en procesos contractuales. Así mismo, el Decreto 1082/2015 (art. 2.2.1.1.2.1.4 y siguientes) promueve criterios diferenciales que faciliten el acceso de estas empresas. Por lo anterior, solicitamos autorizar la presentación de hasta cuatro (4) certificaciones para MiPymes, manteniendo intactas las demás exigencias (objeto similar, cuantía equivalente al 100% del presupuesto y duración mínima de 12 meses). Este ajuste no incrementa la carga evaluativa, pero sí fortalece la libre concurrencia (Ley 80, art. 24) y reduce el riesgo de limitar injustificadamente la participación de proveedores idóneos.	NO	SE ACLARA que, conforme al Cap. III, numeral 3.1 (Experiencia del Proponente), el límite de máximo tres (3) certificaciones para acreditar experiencia se mantiene para este proceso. La medida busca proporcionalidad y eficiencia evaluativa, sin restringir la participación de MiPymes, quienes conservan los demás mecanismos de promoción previstos en el documento: Requisitos habilitantes diferenciales (Cap. III, 1.1.21) y Factor de apoyo a la industria nacional (Cap. IV, 1.4), entre otros. En consecuencia, para esta invitación no se autoriza ampliar a cuatro certificaciones; cualquier cambio de dicho requisito requeriría adenda y, por tanto, no aplica en la etapa actual del proceso.

41	GLOBALTEK	3. Solicitud de aceptar contratos que finalicen antes de la publicación del Acta de Selección (16 de enero de 2026) El requisito de no admitir contratos en ejecución puede excluir experiencias ya ejecutadas en más del 90% y con entregables cumplidos, únicamente por el hecho de encontrarse pendientes de cierre administrativo al momento de presentación de la propuesta. De acuerdo con el principio de selección objetiva (Ley 80, art. 29), la Entidad debe valorar la capacidad real del proponente y no situaciones administrativas accidentales que no afectan el cumplimiento del objeto. Por ello, solicitamos que se acepten contratos cuya fecha de terminación ocurra antes del 16 de enero de 2026, fecha prevista para la publicación del Acta de Selección. Esto es coherente con el Decreto 1082/2015, el cual señala que la experiencia se acredita mediante certificaciones, sin limitar estrictamente el momento de terminación frente a la fecha de cierre del proceso, siempre que pueda verificarse la correcta ejecución contractual. Este ajuste evita excluir proveedores idóneos por motivos formales que no comprometen la calidad contractual.	NO	SE ACLARA que, conforme al Cap. III, numeral 3.1 (Experiencia del Proponente), solo se admiten certificaciones de contratos terminados (no en ejecución) a la fecha de cierre de presentación de ofertas (22 de diciembre de 2025, ver Cronograma). En consecuencia, no se aceptan para la verificación habilitante contratos cuya terminación ocurra después del cierre (p. ej., 16 de enero de 2026); dichos soportes podrán anexarse solo como información complementaria, sin efectos en la habilitación. Esta precisión mantiene las condiciones de la invitación, la selección objetiva y la pertinencia técnica del requisito, sin modificar puntajes ni topes del proceso.
42	GLOBALTEK	4. Los ajustes propuestos no disminuyen el rigor técnico Es importante resaltar que ninguna de las solicitudes modifica los estándares de calidad establecidos por la Entidad. Se mantienen plenamente: • El requisito de objeto igual o similar. • La exigencia de cuantía acumulada equivalente al 100% del presupuesto. • La duración mínima de 12 meses por contrato. • La obligación de presentar certificaciones verificables y completas. Los ajustes propuestos son razonables, proporcionados y compatibles con la jurisprudencia y principios del Estatuto General de Contratación, y permiten aumentar la pluralidad de oferentes sin disminuir la exigencia técnica.	NO	SE ACLARA que, aunque sus ajustes no disminuyen el rigor técnico, para este proceso se mantienen íntegramente las reglas vigentes de experiencia (objeto igual o similar, cuantía acumulada = 100%, duración ≥12 meses, y certificaciones verificables), conforme al Cap. III, 3.1 (Experiencia del Proponente) y al Cronograma (cierre 22 de diciembre de 2025). La pluralidad de oferentes ya se promueve mediante los requisitos habilitantes diferenciales (Cap. III, 1.1.21) y el Factor de apoyo a la industria nacional (Cap. IV, 1.4), entre otros. Cualquier modificación (ventana de antigüedad, número de certificaciones, contratos en ejecución) requeriría adenda y, para preservar la igualdad de condiciones, no procede en esta etapa del proceso.
43	GROWDATA	Se entiende que el servicio no incluye acompañamiento a juzgados o sitios de arbitramiento, o similares. Es correcto el entendimiento?	NO	SE ACLARA que su entendimiento es correcto: el alcance del servicio no incluye acompañamiento ante juzgados, tribunales de arbitramento u organismos similares. El objeto está limitado a la gestión técnica (descubrimiento, evaluación y remediación de vulnerabilidades, EH, SAST, reportes, capacitación, integración con SIEM, etc.), según Cap. I, 6.5–6.13; Cap. III, 3.4.1–3.4.6,
44	GROWDATA	Se solicita aclarar si estas pruebas podrán ejecutarse de forma presencial o remota.	NO	Las pruebas se ejecutarán conforme a lo establecido en el documento. Si el numeral define la modalidad (presencial o remota), se procederá según lo indicado. Si no hay definición expresa, la programación se coordinará en el cronograma institucional, sin modificar requisitos ni plazos.
45	GROWDATA	Aunque se espcifican que son hasta 20K líneas de aplicaciones JAVA se tiene un estimado de cuantas lineas se tendrian que escanear	NO	El documento establece un tope de hasta 20.000 líneas de código Java. No se define un estimado adicional. La cantidad efectiva a escanear se confirmará en la fase de inventario/alistamiento, sin exceder el tope y sin modificar los requisitos ni los plazos.
46	GROWDATA	Se solicita a la entidad aclarar si los activos pueden repetirse y si las apps Web se encuentran dentro de los 10 activos.	NO	Repetición de activos: El conteo de “hasta 10 activos” aplica sobre activos únicos; no se contabilizan repeticiones, salvo que el numeral lo permita expresamente. Apps Web: Se incluyen dentro de los 10 activos solo si la definición de “activo” en el documento contempla aplicaciones Web; de lo contrario, aplican únicamente los tipos de activo allí definidos. (Esta respuesta se ciñe al documento y no modifica sus condiciones ni plazos.)

47	GROWDATA	Se solicita a la entidad indicar si este inventario es definitivo y si incluye infraestrcutura cloud/IoT	NO	inventario: Es definitivo únicamente si el numeral lo indica expresamente. Si no hay tal indicación, se toma como inventario base a validar en alistamiento, sin ampliar topes ni alcances. Cloud/IoT: Se incluyen solo si el documento los menciona de forma explícita en el alcance o en la definición de "activo". En ausencia de mención expresa, no hacen parte del inventario. (Esta respuesta se ciñe al documento y no modifica sus condiciones ni plazos.)
48	PricewaterhouseCoopers Asesores Gerenciales S.A.S.	Solicitamos amablemente tener en consideración que pueda contarse como una de las opciones de certificación la formación académica como especialización en seguridad de la información y/o maestría en ciberseguridad, con base en lo mencionado en el punto 3	NO	Dando respuesta a su observación, la entidad se permite indicar que NO SE ACEPTA. La Entidad mantiene los requisitos de certificación definidos en el punto 3 del pliego de condiciones, por cuanto estos fueron establecidos para garantizar perfiles con competencias técnicas específicas y verificables, acordes con las necesidades del proyecto. En consecuencia, la formación académica como especialización o maestría en seguridad de la información o ciberseguridad no será considerada como alternativa a las certificaciones exigidas, debiendo los oferentes cumplir estrictamente con los requisitos establecidos.
49	PricewaterhouseCoopers Asesores Gerenciales S.A.S.	La exigencia establecida en el pliego de condiciones, consistente en la presentación de únicamente tres certificaciones de experiencia y restringidas exclusivamente a los últimos cinco (5) años, resulta desproporcionada y limitante frente a los principios rectores de la contratación. Desde un punto de vista técnico, limitar la experiencia a solo tres certificaciones impide demostrar de manera integral las capacidades y trayectoria de los posibles oferentes, desconociendo que el conocimiento y experticia acumulada en el sector no se agotan en un número reducido de contratos, ni en un marco temporal tan estrecho. Este criterio reduce el espectro de participación, pues excluye a empresas que cuentan con una amplia experiencia debidamente acreditada pero que, por la naturaleza de sus proyectos, podrían no concentrarse en dicho lapso o en un número tan restringido de contratos, así mismo en cuantías. La restricción planteada vulnera los principios de selección objetiva y de transparencia, en la medida en que se convierte en una barrera de acceso que no guarda relación directa ni proporcional con el objeto contractual, pudiendo configurar un requisito habilitante de carácter discriminatorio o excluyente. La jurisprudencia del Consejo de Estado ha reiterado que los requisitos de experiencia deben ser razonables, proporcionales y adecuados al objeto del contrato, evitando condiciones que restrinjan de manera injustificada la participación de potenciales oferentes idóneos. En consecuencia, se solicita a la Entidad ajustar el requisito de experiencia, permitiendo un número mayor de certificaciones y una ventana temporal más amplia, de manera que se garantice la efectiva pluralidad de oferentes, la concurrencia real y la transparencia en el proceso de selección.	NO	El comité se rige por el documento de condiciones definitivas, el cual exige máximo tres (3) certificaciones de experiencia dentro de los últimos cinco (5) años. Este parámetro se mantiene por criterios de pertinencia (alineación al objeto), vigencia técnica, comparabilidad y trazabilidad en la verificación. No procede su ampliación ni equivalencias, pues el numeral no prevé ajustes. En consecuencia, el oferente debe seleccionar sus tres certificaciones más representativas dentro de la ventana temporal definida para la validación. (Esta respuesta se ciñe al documento y no lo modifica.)
50	PricewaterhouseCoopers Asesores Gerenciales S.A.S.	Solicitamos extender el plazo de presentación de ofertas con la intencion de evaluar cada uno de los requerimientos de la entidad punto por punto enfocado en lo técnico, jurídico y económico	NO	El cronograma se mantiene conforme al documento de condiciones definitivas. Cualquier ajuste de plazo solo puede realizarse mediante adenda publicada por la Entidad. A la fecha no se prevé modificación, por lo que se mantienen las fechas vigentes. (Esta respuesta se ciñe al documento y no lo modifica.)

51	PricewaterhouseCoopers Asesores Gerenciales S.A.S.	Respetuosamente solicitamos a la Entidad que se permita acreditar la experiencia con contratos cuya sumatoria sea igual o superior al 70% del presupuesto oficial del presente proceso de selección, o en su defecto se permita en calidad de MiPymes la presentación de máximo cinco (5) certificaciones de contratos ejecutados.	NO	La Entidad agradece la observación presentada y se permite aclarar el alcance del requisito de acreditación de experiencia, conforme a lo establecido en el pliego. Para efectos del presente proceso, la experiencia del proponente deberá acreditarse mediante un máximo de tres (3) certificaciones de contratos, las cuales, en su valor individual o en sumatoria, deberán ser iguales o superiores al cien por ciento (100%) del presupuesto destinado al proceso. En consecuencia, no resulta procedente aceptar la acreditación de experiencia por un porcentaje inferior ni ampliar el número máximo de certificaciones, incluyendo la solicitud planteada para MiPymes, toda vez que el criterio definido busca garantizar la idoneidad técnica y financiera del proponente frente a la magnitud del contrato, sin afectar la objetividad ni la eficiencia del proceso de evaluación.
52	SUMINISTROS OBRAS Y SISTEMAS S.A.S	ITEM 1 – Certificación para Gestión de Incidentes de Seguridad De manera comedida solicitamos a la Entidad evaluar la inclusión de un requisito orientado a robustecer la capacidad del proveedor para gestionar incidentes de seguridad de la información, asegurando la aplicación de marcos internacionales reconocidos. Proponemos exigir que: “El oferente cuente con procedimientos estructurados y operativos para la gestión integral de incidentes, respaldados por certificación vigente en una norma internacional de Gestión de Incidentes de Seguridad de la Información. La certificación debe evidenciar las prácticas de preparación, detección, análisis, respuesta y retroalimentación, en armonía con el MSPI del MinTIC. Se deberá adjuntar copia emitida por el organismo certificador al oferente.” Esta medida permitirá mitigar riesgos operacionales y mejorar la capacidad de respuesta ante escenarios críticos.	NO	Gracias por la propuesta. En esta etapa no procede incorporar nuevos requisitos. El comité se rige por el documento de condiciones definitivas; la certificación específica para gestión de incidentes no está prevista en el Ítem 1. por lo que se solicita aportar únicamente las evidencias expresamente solicitadas en el numeral correspondiente.
53	SUMINISTROS OBRAS Y SISTEMAS S.A.S	ITEM 2 – Aclaración del requisito de experiencia Solicitamos respetuosamente que se precise el alcance del numeral 3.1 respecto a las actividades que se consideran válidas para acreditar la experiencia habilitante. Proponemos confirmar una interpretación amplia que considere suficiente la ejecución de una o varias de las actividades relacionadas con la gestión de vulnerabilidades Esto permitirá garantizar la participación de oferentes idóneos, evitando interpretaciones restrictivas.	NO	La verificación del numeral 3.1 se realizará literalmente según el texto del documento. Se considerarán válidas solo las actividades expresamente previstas; no procede ampliar su alcance por interpretación. Si el numeral permite acreditar “una o varias” actividades, se validará así; de lo contrario, se exige la ejecución integral conforme al alcance definido. Por favor, aporte certificaciones que identifiquen actividades ejecutadas, periodo y resultados. Cualquier cambio solo procede vía adenda; a la fecha no hay modificación.
54	SUMINISTROS OBRAS Y SISTEMAS S.A.S	ITEM 3 – Certificación en Continuidad del Negocio Con el propósito de asegurar la continuidad operativa de los servicios contratados, sugerimos incorporar un requisito que exija: “Que el oferente cuente con un Sistema de Gestión de la Continuidad del Negocio certificado bajo norma internacional vigente aplicable a SGCN, para los procesos de seguridad y mesa de servicio. La oferta deberá incluir copia de la certificación emitida directamente al oferente.” Esta garantía resulta crucial para la estabilidad del servicio frente a eventos disruptivos.	NO	Gracias por la propuesta. En esta etapa no procede incorporar nuevos requisitos. El comité se rige por el documento de condiciones definitivas; el Ítem 3 no contempla exigir certificación de un Sistema de Gestión de Continuidad del Negocio (SGCN) para seguridad o mesa de servicio. Cualquier ajuste solo puede realizarse mediante adenda; a la fecha no hay modificación. La continuidad operativa se verificará conforme a los criterios vigentes del documento de condiciones definitivas, únicamente en lo que el numeral exija. Por favor, aportar las evidencias expresamente solicitadas en el documento.

55	SUMINISTROS OBRAS Y SISTEMAS S.A.S	ITEM 4 – Ajuste sobre certificación de canal autorizado Solicitamos modificar el numeral 3.2.b para que únicamente se requiera la certificación vigente que acredite al oferente como partner autorizado del fabricante o representante oficial, sin restringirlo a los más altos niveles de membresía. Con ello se evita limitar la concurrencia y se mantiene la validez técnica del respaldo del fabricante.	NO	El numeral 3.2.b se aplicará literalmente según lo redactado en el documento: se exige la certificación vigente que acredite al oferente como canal/partner autorizado con el nivel de membresía establecido en el pliego. No procede flexibilizar o reducir los niveles requeridos; cualquier cambio solo puede realizarse vía adenda y, a la fecha, no hay modificación. La exigencia asegura respaldo directo del fabricante, capacidad de escalamiento, calidad del soporte, y comparabilidad técnica entre propuestas. Por favor, adjuntar certificación oficial vigente emitida por el fabricante/mayorista/representante en Colombia, que identifique la marca y la solución objeto del proceso, y acredite el nivel exigido en el numeral.
56	SUMINISTROS OBRAS Y SISTEMAS S.A.S	ITEM 5 – Certificación en Seguridad para Servicios Cloud Con base en que los servicios a contratar se ejecutarán en entornos de nube, proponemos exigir que: "El oferente cuente con certificación vigente en una norma internacional de seguridad para servicios en la nube, que contemple controles de protección de datos, control de accesos, responsabilidad compartida, segregación lógica y monitoreo de recursos. La certificación deberá ser emitida directamente al oferente y adjuntarse a la oferta." Ello permite asegurar la adecuada gestión de riesgos inherentes a la operación cloud.	NO	l comité se rige por el documento de condiciones definitivas; el Ítem 5 no contempla exigir una certificación internacional específica de seguridad para servicios en la nube emitida al oferente. Cualquier cambio solo puede realizarse mediante adenda; a la fecha no hay modificación. La seguridad en nube se verificará conforme a los criterios vigentes del pliego (p. ej., controles exigidos, SLA, región, responsabilidad compartida, segregación y monitoreo), únicamente en los términos indicados por el numeral. Por favor aportar las evidencias expresamente solicitadas en el documento (políticas/procedimientos, fichas/compromisos del servicio y las certificaciones previstas en la invitación).
57	STAR SOLUTIONS. T.I.	1. Observación al requisito de membresías del fabricante – Art. 3.2 Certificaciones del Proponente Referencia: Exigencia de acreditar "los dos máximos niveles de membresía del fabricante". Observación Jurídica y Técnica Se solicita revisar este requisito por cuanto los niveles de membresía más altos de la mayoría de los fabricantes (Platinum / Tier 1 o equivalentes): a. Dependen de acuerdos comerciales y metas de facturación, no de superioridad técnica. b. Su exigencia puede constituir una barrera de acceso que desconoce el principio de pluralidad de oferentes (Ley 80/93). c. La capacidad técnica se acredita mediante certificaciones de personal, experiencia y cumplimiento normativo, no mediante volumen comercial. Star Solutions TI S.A.S Dirección Carrera 27 # 49 - 19 Teléfonos Móvil [+57] 300 701 0017 d. STAR SOLUTIONS TI cuenta con certificación ISO 27001:2022, estándar internacional que avala nuestro sistema de gestión de seguridad de la información, proporcionando garantías superiores a una membresía comercial. Solicitud Se solicita permitir: 1. Acreditar membresías equivalentes (Gold, Silver u otras), 2. O sustituir el requisito por certificaciones individuales del personal técnico y evidencia de cumplimiento de ISO 27001:2022.	NO	El Art. 3.2 se aplicará literalmente según el pliego: se exige acreditar los dos máximos niveles de membresía del fabricante. No procede admitir membresías equivalentes (Gold/Silver) ni sustituir el requisito por certificaciones de personal o por ISO/IEC 27001:2022, dado que: Las membresías de máximo nivel acreditan respaldo directo del fabricante, capacidad de escalamiento, prioridad de soporte y derechos/beneficios de canal necesarios para la ejecución y sostenibilidad del servicio. ISO/IEC 27001 valida el SGSI de la organización, y las certificaciones individuales acreditan competencias técnicas; no confieren estatus de canal ni facultades de representación ante el fabricante. Por lo tanto se deberá adjuntar certificación oficial vigente emitida por el fabricante/mayorista/representante en Colombia que acredite los niveles de membresía exigidos.

58	STAR SOLUTIONS. T.I.	2. Observación al requisito de estar clasificado como “Líder” en Gartner, Forrester u otros rankings Referencia: Numeral 3.2 – Certificaciones del Proponente. Observación Los rankings de consultoras privadas (Gartner, Forrester, GigaOm, SC Media): a. Evalúan principalmente capacidad de ejecución comercial global, no la idoneidad técnica para el contexto colombiano. b. Excluir fabricantes que no estén en la categoría “Líder” afecta la pluralidad y restringe injustificadamente la competencia. c. Muchos proveedores especializados en Ethical Hacking, análisis de código o ingeniería social no son evaluados por estos rankings, lo cual podría excluir tecnologías más robustas. d. La certificación ISO 27001:2022 constituye un medio de prueba objetivo, verificable y auditado, superior a la opinión de un consultor privado. Solicitud 1. Permitir participación de fabricantes ubicados en cualquier categoría del cuadrante. 2. Aceptar certificaciones técnicas de personal como evidencia suficiente de capacidad.	NO	El numeral 3.2 se aplicará literalmente: se exige que el fabricante esté clasificado como “Líder” en Gartner/Forrester u otros rankings definidos en el pliego. No procede permitir participación en categorías distintas del cuadrante (p. ej., Challengers/Niche/Strong Performers) ni sustituir este requisito por ISO/IEC 27001:2022 o certificaciones de personal, al no ser equivalentes al posicionamiento del fabricante exigido. Cualquier ajuste solo puede realizarse mediante adenda; a la fecha, no hay modificación. Evidencia a aportar (si el numeral la pide): soporte oficial del reporte vigente donde se verifique la clasificación “Líder” del fabricante (nombre del informe y fecha).
59	STAR SOLUTIONS. T.I.	3. Observación sobre la definición del alcance técnico del servicio – Página 13 del pliego Referencia: Alcance para Ethical Hacking (10 activos), análisis de código (20.000 líneas) e ingeniería social (200 usuarios). Star Solutions TI S.A.S Dirección Carrera 27 # 49 - 19 Teléfonos Móvil [+57] 300 701 0017 Observación El pliego no discrimina elementos esenciales que afectan los costos, las herramientas, el alcance y la viabilidad técnica: Tipología de los 10 activos (aplicaciones, APIs, infraestructura, nube, etc.). Lenguajes, frameworks o arquitecturas del código a analizar. Profundidad requerida del análisis: SAST, SCA, DAST, IAST o MAST. Canales incluidos para ingeniería social (correo, llamadas, mensajería). La falta de precisión puede generar interpretaciones distintas y afectar la comparabilidad de propuestas. Solicitud Definir explícitamente: 1. Tipo de activo incluido en Ethical Hacking. 2. Alcance del análisis de código (SAST/SCA/DAST). 3. Canales y criterios mínimos de la ingeniería social.	NO	Ethical Hacking (10 activos): Se verificarán únicamente los tipos de activo expresamente definidos en el pliego. Si la tipología no está discriminada, se precisará en alistamiento con base en el inventario institucional, sin exceder 10 activos ni incorporar tipos no previstos por el documento. Análisis de código (20.000 líneas): Se aplicará la(s) técnica(s) indicada(s) en el numeral. Si no se especifica (SAST/SCA/DAST/IAST/MAST), la modalidad se precisará en alistamiento con la Entidad, manteniendo el tope de hasta 20.000 líneas y sin ampliar el alcance. Ingeniería social (200 usuarios): Se ejecutará por los canales y bajo los criterios descritos en el pliego. En ausencia de definición expresa, los canales se acordarán en alistamiento con la Entidad, manteniendo el universo de 200 usuarios y los criterios de autorización, ética y trazabilidad previstos.
60	STAR SOLUTIONS. T.I.	4. Observación sobre tratamiento de información sensible durante las pruebas Observación El pliego no establece lineamientos acerca de: Entornos de prueba autorizados. Mecanismos de protección y transferencia del código fuente. Alcances del acceso a datos personales o productivos. Procedimientos de anonimización o minimización de datos. Custodia y destrucción de evidencias al finalizar el contrato. Dada la naturaleza de la información que gestiona PREVISORA, estos lineamientos son indispensables para garantizar cumplimiento normativo y seguridad operativa. Solicitud Incluir un anexo técnico que detalle: 1. Protocolos de manejo de información sensible. 2. Lineamientos de uso de ambientes aislados o sandbox. 3. Criterios de retención y destrucción de evidencia.	NO	La entidad ACLARA que no es posible detallar de forma puntual la tipología de los activos, lenguajes, arquitecturas, profundidad de los análisis o canales específicos, toda vez que dichos elementos dependen de las características y requerimientos de cada proyecto que se adelante durante la ejecución del contrato. Los oferentes deberán, por tanto, ajustarse a lo establecido en el pliego y considerar que el detalle operativo será definido en la etapa de ejecución, conforme a las necesidades que determine la Entidad

61	STAR SOLUTIONS. T.I.	5. Observación sobre criterios de aceptación y formato de entregables Star Solutions TI S.A.S Dirección Carrera 27 # 49 - 19 Teléfonos Móvil [+57] 300 701 0017 Observación El pliego no establece: Formato estándar de reportes, Nivel mínimo de detalle, Criterios para aceptación del entregable técnico. Esto puede generar diferencias entre propuestas y dificultades de evaluación. Solicitud Definir: 1. Formatos requeridos (PDF/XLS/API). 2. Mínimos de información: severidad, CVSS, evidencia, impacto, recomendación. 3. Si debe entregarse	NO	SE ACLARA que los criterios de aceptación, formatos y nivel de detalle de los entregables se regirán por lo establecido en el contrato y los lineamientos operativos que se definan durante la ejecución del mismo. En este sentido, los informes y entregables deberán contener la información técnica necesaria para su adecuada comprensión y gestión por parte de la Entidad, tales como la descripción del hallazgo, nivel de severidad, impacto y recomendaciones, sin que sea procedente fijar en esta etapa formatos o estructuras rígidas que generen mayor carga operativa. La validación y aceptación de los entregables se realizará por parte del supervisor del contrato, conforme a los criterios contractuales definidos.
62	STAR SOLUTIONS. T.I.	6. Observación sobre requisitos de integración e interoperabilidad de soluciones Observación No se especifica si las plataformas de Ethical Hacking, análisis de código, XDR, ingeniería social y cumplimiento deben: • Integrarse en consola unificada, • Exportar en formatos estandarizados (STIX/TAXII), • Operar de manera independiente. Esto impacta costos, diseño arquitectónico y selección de fabricantes. Solicitud Aclarar si la interoperabilidad es obligatoria o deseable.	NO	SE ACLARA que la información relacionada con los requisitos de integración e interoperabilidad entre las diferentes plataformas será definida y compartida durante la ejecución del contrato, de acuerdo con las necesidades técnicas y operativas de la Entidad. En consecuencia, los oferentes deberán ceñirse a los requisitos establecidos en el pliego de condiciones, entendiendo que los lineamientos específicos sobre integración, formatos de intercambio o esquemas de operación serán acordados en la etapa de ejecución, sin que ello implique compromisos adicionales distintos a los contractualmente previstos.
63	STAR SOLUTIONS. T.I.	7. Observación sobre modalidad de despliegue de las soluciones (on-premise / cloud / SaaS) Observación El pliego no determina si las soluciones deben operar: • En infraestructura propia de PREVISORA, • En modalidad SaaS. Star Solutions TI S.A.S Dirección Carrera 27 # 49 - 19 Teléfonos Móvil [+57] 300 701 0017 • En nube híbrida. Esto tiene impacto directo en costos, licenciamiento y cumplimiento regulatorio. Solicitud Definir el modelo de despliegue esperado para cada solución.	NO	SE ACLARA que el modelo de despliegue de las soluciones (on-premise, cloud, SaaS o esquemas híbridos) deberá ajustarse a lo establecido en el pliego de condiciones y a las necesidades que se definan durante la ejecución del contrato. Así mismo, se aclara que el oferente deberá asumir la totalidad de los costos asociados que se deriven del modelo de despliegue propuesto, incluyendo infraestructura, licenciamiento, operación, conectividad y cualquier otro componente necesario para el cumplimiento integral de los requisitos técnicos, funcionales y regulatorios exigidos por la Entidad.
64	STAR SOLUTIONS. T.I.	8. Observación sobre alcance de servicios de remediación	NO	SE ACLARA que las acciones de remediación de vulnerabilidades deberán ejecutarse en acompañamiento del contratista, quien será responsable de apoyar técnica y operativamente el proceso de mitigación conforme a la criticidad de los hallazgos, el estado de los controles existentes y el nivel de obsolescencia tecnológica. Así mismo, se mantiene la exigencia de que dichas acciones estén respaldadas por informes detallados en idioma español, los cuales deberán evidenciar el tratamiento aplicado a cada vulnerabilidad, su evolución y el estado actual de mitigación, garantizando la trazabilidad y el adecuado seguimiento por parte de la Entidad.

65	STAR SOLUTIONS. T.I.	9. Observación sobre el alcance real de la ingeniería social Observación El número de usuarios (200) no indica: • Si deben segmentarse por áreas o roles. • Si se realizarán campañas múltiples. • Si se incluye capacitación o solo simulación. • Si se debe entregar matriz de riesgo humano. Solicitud Definir el alcance funcional y pedagógico de la prueba. STAR SOLUTIONS TI S.A.S. agradece la oportunidad de participar en este proceso. Las observaciones aquí consignadas buscan fortalecer la transparencia, facilitar la participación plural y asegurar que la Entidad reciba una oferta técnicamente sólida, trazable, comparable y ajustada a sus necesidades reales de ciberseguridad.	NO	SE ACLARA que el alcance y la metodología de la ingeniería social, incluyendo la segmentación de usuarios, la realización de campañas, la inclusión de actividades de capacitación y la entrega de productos adicionales, serán definidos y acordados durante la ejecución del contrato con el supervisor designado por la Entidad, con el fin de establecer la metodología más adecuada según las necesidades institucionales.
66	TIC COLOMBIA SAS	6. Personal requerido Respetuosamente, solicitamos a la Entidad incorporar dentro de los requisitos del proceso el perfil de Profesional de Implementación, conforme a las siguientes características: • Título profesional: Ingeniero electrónico, de sistemas, telecomunicaciones o afines. • Especialización: Seguridad informática. • Experiencia: o Mínimo cuatro (4) años de experiencia general contados a partir de la tarjeta profesional. o Mínimo dos (2) años de experiencia específica en proyectos de seguridad informática, acreditada mediante certificaciones de experiencia laboral. • Certificaciones requeridas: o ITIL V4 Foundation o Certificación como auditor interno ISO 27001:2013 o superior	NO	No procede la modificación. El documento ya define el personal mínimo habilitante (Analista de Seguridad y Gerente de Proyecto) y permite que cada oferente incorpore perfiles adicionales según su modelo (Cap. III, 3.3). Por tanto, no se incluirá un nuevo perfil obligatorio de "Profesional de Implementación". Cualquier cambio solo puede realizarse mediante adenda (Cap. I, 20), y no se aceptan propuestas condicionadas a requisitos distintos a los establecidos (Cap. II, 1). Ustedes pueden incluir ese perfil en su equipo sin alterar las condiciones del proceso.
67	TIC COLOMBIA SAS	OBSERVACIÓN 1. Retiro del requisito de 'dos máximos niveles de membresía' por ser un filtro comercial restrictivo y no necesario: Causa legal/técnica: El requisito impone una jerarquía comercial propia de cada fabricante y ajena al mérito técnico exigible, lo cual afecta la pluralidad de oferentes y la selección objetiva al limitar la concurrencia a canales 'top tier'. El propio pliego ya exige ISO/IEC 2701:2022, perfiles habilitantes, ANS de disponibilidad (99,5%) y penalidades, controles que garantizan idoneidad y continuidad sin necesidad de un 'nivel máximo' de canal. Texto a reemplazar (extracto del pliego): 'Deberá adjuntar con su propuesta la certificación expedida por el fabricante, mayorista o representante oficial en Colombia, que lo acredite como canal autorizado en cualquiera de los dos máximos niveles de membresía, con una vigencia no mayor a dos (2) meses.' Propuesta de reemplazo: 'Carta de respaldo del fabricante o del distribuidor oficial que garantice suministro legítimo, acceso a parches/actualizaciones y soporte; acreditación vigente como partner autorizado sin limitar a niveles máximos; en consorcios/UT, la acreditación podrá aportarla el miembro responsable del componente técnico.' Argumento de la solicitud: Desde la perspectiva legal, el filtro comercial desproporcionado vulnera los principios de igualdad y pluralidad que informan el procedimiento de invitación abierta, pudiendo configurar direccionamiento. Desde la técnica, la entrega de parches y soporte se garantiza por contrato y por respaldo del fabricante, no por el 'tier'. Las obligaciones de seguridad y continuidad están consagradas en los ANS y en las penalidades de la minuta; establecer niveles máximos no añade garantías jurídicas ni técnicas adicionales, pero sí restringe el mercado.	NO	El Documento de Condiciones Definitivas exige la acreditación como canal autorizado en uno de los dos niveles superiores de membresía (Cap. III, 3.2.b), como garantía de respaldo directo del fabricante para suministro legítimo, acceso a parches/actualizaciones, escalamiento de soporte y continuidad, en armonía con las obligaciones del SGSI y la CBJ 006-2025. Esta condición no restringe la concurrencia ni configura direccionamiento, pues admite certificación de fabricante, mayorista o representante oficial y permite que en consorcios/UT la acreditación la aporte el miembro responsable.

68	TIC COLOMBIA SAS	OBSERVACIÓN 2. Modulación de la 'vigencia máxima de dos meses' de la acreditación (actualidad razonable sin afectar concurrencia) La exigencia de una vigencia de dos (2) meses resulta excesivamente rígida y puede excluir proveedores con acreditaciones válidas que por ciclos administrativos del fabricante tengan emisión superior a dos meses, sin que ello implique pérdida de validez. El control de actualidad puede satisfacerse con verificación directa al fabricante o mayorista y con el contrato de soporte adjunto, evitando sacrificar pluralidad. *Texto a reemplazar (extracto del pliego):* '…con una vigencia no mayor a dos (2) meses.' Propuesta de reemplazo: 'Acreditación vigente del fabricante o verificación documental emitida por el fabricante/mayorista dentro de los últimos seis (6) meses, o certificación de soporte activa; en su defecto, confirmación electrónica del fabricante durante la etapa de verificación.' Argumento de la solicitud: Legalmente, el estándar de 'actualidad razonable' debe armonizarse con la realidad del mercado para no transformar un control de vigencia en una barrera de entrada. Técnicamente, la continuidad del soporte y la legitimidad del licenciamiento se acreditan por contratos activos y cartas del fabricante, no por una ventana temporal rígida de dos meses.'	NO	El Documento de Condiciones Definitivas exige la acreditación como canal autorizado en uno de los dos niveles superiores de membresía (Cap. III, 3.2.b), como garantía de respaldo directo del fabricante para suministro legítimo, acceso a parches/actualizaciones, escalamiento de soporte y continuidad, en armonía con las obligaciones del SGSI y la CBJ 006-2025. Esta condición no restringe la concurrencia ni configura direccionamiento, pues admite certificación de fabricante, mayorista o representante oficial y permite que en consorcios/UT la acreditación la aporte el miembro responsable.
69	TIC COLOMBIA SAS	OBSERVACIÓN 3. Protección de la pluralidad y selección objetiva frente a jerarquías comerciales heterogéneas Los 'niveles máximos' de membresía son conceptos no estandarizados: cada fabricante los define con criterios propios, por lo que su comparación entre oferentes y su relación con la calidad es discutible. Impulsar un criterio heterogéneo como habilitante puede generar ventaja indebida y limitar la participación de integradores con respaldo oficial pero sin 'top tier'. Texto a reemplazar Exigencia de 'dos máximos niveles de membresía' como habilitante. *Propuesta de reemplazo:* 'Aceptar respaldo oficial del fabricante/distribuidor y evidencia de soporte/actualizaciones (SLA, plan de parches) como criterios habilitantes objetivos, sin jerarquías comerciales.' Argumento de la solicitud: Legalmente, la selección objetiva reclama criterios verificables y comparables; las jerarquías comerciales no aseguran mayor seguridad ni mejor prestación. Técnicamente, los riesgos operativos se mitigan por la arquitectura, cifrado, integración, SAST/EH y ANS, todos ya exigidos en el pliego; el 'nivel máximo' no es un control de seguridad, sino un emblema comercial.	NO	El Documento mantiene la acreditación como canal autorizado en uno de los dos niveles superiores (Cap. III, 3.2.b), certificable por fabricante/mayorista/representante oficial y válida en consorcios/UT cuando la aporte el miembro responsable. Este criterio es verificable (CUMPLE/NO CUMPLE) y asegura respaldo directo del fabricante, suministro legítimo, acceso a parches/actualizaciones y escalamiento de soporte, en armonía con el SGSI y la CBJ 006-2025.
70	TIC COLOMBIA SAS	OBSERVACIÓN 4. Claridad para proponentes plurales (consorcios/UT) y complementariedad técnica Causa: El pliego contempla la participación plural, pero no precisa expresamente que las certificaciones y respaldos puedan ser aportados por el integrante que ejecuta el componente técnico, lo cual desalienta la asociación y restringe el aprovechamiento de capacidades complementarias. Propuesta de reemplazo: Página 3 'En proponente plural (consorcio/UT), las certificaciones y respaldos requeridos podrán ser aportados por el miembro que ejecuta el alcance técnico relacionado; la verificación se realizará sobre el conjunto de la oferta y la matriz de responsabilidades.' Argumento de la solicitud (enfoque legal y técnico): Desde el plano legal, esta precisión protege la pluralidad y evita barreras indirectas; en lo técnico, favorece la suficiencia del equipo sin relajar controles de soporte ni seguridad establecidos en ANS/minuta.	NO	Se mantiene la exigencia de acreditación como canal autorizado en uno de los dos niveles superiores (Cap. III, 3.2.b). En proponente plural (consorcio/UT), las certificaciones y respaldos podrán ser aportados por el integrante que ejecuta el componente técnico correspondiente, siempre que ello esté identificado en el documento de constitución (Cap. III, 1.1.5) y en la matriz de responsabilidades; la verificación se realiza sobre el conjunto de la oferta (ver criterio de experiencia plural, Cap. III, 3.1.h). Notas: No se alteran condiciones del pliego; cualquier cambio solo vía adenda (Cap. I, 20). Las propuestas condicionadas a modificar requisitos no son admisibles (Cap. II, 1).

71	TIC COLOMBIA SAS	OBSERVACIÓN 5. Solicitud de Adenda: sustitución del criterio comercial por controles de licenciamiento y soporte verificables: Para blindar el proceso frente a riesgos operativos (licencias ilegítimas, falta de parches/soporte), se propone reemplazar el 'nivel máximo' por una combinación de controles objetivos: (i) carta de respaldo del fabricante; (ii) contrato de soporte activo; (iii) plan de gestión de parches y actualizaciones; (iv) verificación documental durante evaluación; (v) penalidades específicas por incumplimiento de soporte y seguridad ya previstas. Propuesta de reemplazo: 'Incluir en Adenda el paquete de controles (i–v) como habilitantes/obligatorios, eliminando la exigencia de jerarquía comercial.' Legalmente, se privilegian criterios objetivos y no discriminatorios alineados con selección objetiva; técnicamente, se fortalecen garantías directas de seguridad y continuidad sin restringir la participación. Conclusión y petición: Solicitamos la expedición de Adenda que elimine la exigencia de 'dos máximos niveles de membresía' y module la vigencia de la acreditación, sustituyéndolas por controles objetivos de licenciamiento y soporte que no restrinjan la concurrencia, y que se precise la aportación de certificaciones en consorcios/UT. Soporte	NO	El pliego exige la acreditación como canal autorizado en uno de los dos niveles superiores de membresía del fabricante/mayorista/representante oficial (Cap. III, 3.2.b), requisito objetivo y verificable (CUMPLE/NO CUMPLE) que asegura respaldo directo, suministro legítimo, acceso a parches/actualizaciones y escalamiento de soporte, en coherencia con las obligaciones de seguridad (ISO/IEC 27001:2022) y continuidad exigidas. En proponente plural (consorcio/UT), la acreditación puede ser aportada por el integrante responsable del componente técnico, conforme al documento de constitución y matriz de responsabilidades (Cap. III, 1.1.5 y 3.1.h). Cualquier modificación solo puede realizarse mediante adenda (Cap. I, 20). Las propuestas condicionadas a alterar requisitos no son admisibles (Cap. II, 1).
72	TI INFORMATICA	¿Qué expectativas tienen sobre cifrado (TLS, FIPS)? ¿Qué RTO/RPO y plan de contingencia esperan? ¿Habilitan los cuatro métodos: pasivo, activo no autenticado, activo autenticado y agente? ¿La plataforma debe orquestar parches y acciones de mitigación? ¿Qué límites de cambio y ventanas de mantenimiento aplican? ¿Qué herramienta ITSM usan para integrar tickets? ¿Cómo gestionan actas de aceptación de riesgo? ¿Confirman capacitación anual para 20 personas? ¿Qué SLA esperan para incidentes críticos (presencial vs. remoto)? ¿Soporte en español, 8x5 o 24x7? ¿Integración con EDR, WAF, NAC, MDM, SSO/MFA? ¿Cumplimiento normativo (ISO 27001, PCI DSS, SARLAFT, Ley 1581)? ¿Qué KPIs son clave (MTTR, % remediación, backlog)?	NO	1) ¿Expectativas sobre cifrado (TLS, FIPS)? Exigencia: Cifrado de extremo a extremo de la información en tránsito y en reposo entre la solución y los servicios internos. El pliego no prescribe un estándar específico (TLS/FIPS); el oferente debe asegurar buenas prácticas alineadas al SGSI. Referencia: Cap. I 6.3.b; Cap. III 3.2.a (ISO/IEC 27001:2022 por CBJ 006-2025). 2) ¿Qué RTO/RPO y plan de contingencia esperan? Plan de Continuidad y Recuperación de Desastres (PCN/DRP) con pruebas semestrales (periodicidad exigida). Los valores de RTO/RPO no están fijados en el pliego; deben proponerse por el oferente dentro del PCN/DRP y su BIA. Referencia: Cap. I 6.1.d; Minuta (Anexo 13) Cláusula 43 (PCN con BIA, incluyendo RTO/RPO). 3) ¿Habilitan los cuatro métodos: pasivo, activo no autenticado, activo autenticado y agente? Sí. Se exige descubrimiento/escaneo por: pasivo de red, activo no autenticado, activo autenticado y agente. Referencia: Cap. III 3.4.1 (8.e). 4) ¿La plataforma debe orquestar parches y acciones de mitigación? Sí. Se requiere que el servicio incluya acciones de remediación basadas en criticidad y que la plataforma cuente con funcionalidades adicionales como aplicación de parches y/o remediación temporal/definitiva. Referencia: Cap. III 3.4.3 (4). 5) ¿Qué límites de cambio y ventanas de mantenimiento aplican?

73	ACTIVOS TI	1 Solicitud de supresión total del requisito de certificación ISO/IEC 27001:2022 El pliego establece que el proponente debe contar con certificación ISO/IEC 27001:2022 "en cumplimiento de la Circular Básica Jurídica 006 de 2025 de la Superintendencia Financiera de Colombia". Sin embargo, tras revisar íntegramente dicha Circular, se evidencia que su contenido se limita a la depuración y reorganización formal de la CBJ, sin introducir nuevos requisitos en materia de seguridad de la información, y particularmente sin imponer la certificación ISO 27001 a proveedores o terceros. En consecuencia, la fundamentación normativa utilizada en el pliego no corresponde al contenido real de la regulación y configura una motivación inexacta del requisito. Si bien valoramos la importancia técnica del estándar ISO 27001, su exigencia no deriva de una obligación regulatoria y solo podría responder a una decisión interna de la Entidad. Mantenerlo como requisito habilitante basado en una norma que no lo contempla afecta los principios de selección objetiva, proporcionalidad y libre concurrencia, al introducir una barrera de acceso no prevista por el marco regulatorio aplicable. Por lo anterior, solicitamos la SUPRESIÓN TOTAL del requisito de certificación ISO/IEC 27001:2022, dado que no encuentra soporte jurídico en la Circular 006 ni en las disposiciones vigentes de la Superintendencia Financiera, y su imposición podría restringir injustificadamente la participación de oferentes idóneos. La verificación de los controles de seguridad puede efectuarse mediante los mecanismos previstos en la regulación (políticas, controles, procedimientos y evidencias), sin imponer una certificación no exigida por la norma.	NO	NO PROCEDE. Se mantienen las condiciones del Documento de Condiciones Definitivas. La circular 006/2025 de la SFC reexpide y depura la Circular Básica Jurídica; no introduce una obligación general de certificación ISO 27001 para todos los proveedores. La Entidad, bajo derecho privado, puede fijar requisitos mínimos de idoneidad y seguridad acordes con su SGSI
74	ACTIVOS TI	2 Solicitud de ampliación del límite de máximo tres (3) certificaciones de experiencia El numeral 3.1 del pliego establece que el proponente únicamente podrá aportar máximo tres (3) certificaciones de experiencia, evaluándose solo las tres primeras foliadas. Esta restricción resulta desproporcionada frente a la exigencia de acreditar experiencia equivalente al 100% del presupuesto oficial, cuyo valor asciende a $1.403 millones. Página 2 de 2 En servicios especializados como la gestión de vulnerabilidades y la seguridad de la información, la experiencia suele estar distribuida en múltiples contratos de diferentes cuantías. Limitarla a solo tres certificaciones impide reflejar adecuadamente la trayectoria real del proponente y afecta de manera directa la valoración objetiva de las capacidades técnicas del oferente. Adicionalmente, esta restricción afecta los principios de selección objetiva, proporcionalidad y libre concurrencia, dado que excluye injustificadamente a oferentes que podrían demostrar la idoneidad requerida mediante la sumatoria de varios contratos. Por ello, solicitamos modificar el requisito para permitir un número mayor de certificaciones —sugerimos un mínimo de seis (6). Esta modificación incrementa la pluralidad de oferentes, fortalece la competencia y garantiza una selección más objetiva y ajustada a la naturaleza técnica del objeto contractual.	NO	Se mantienen las condiciones del Documento de Condiciones Definitivas. El pliego establece que la experiencia se acredita con máximo tres (3) certificaciones, evaluándose solo las tres primeras foliadas (Cap. III, 3.1). Este criterio es objetivo y verificable (CUMPLE/NO CUMPLE) y garantiza orden, comparabilidad y eficiencia en la evaluación, sin impedir que el proponente alcance el 100% del presupuesto mediante contratos de mayor cuantía y con actualización/convertibilidad prevista (TRM/SMMLV) (Cap. III, 3.1.e–g).
75	INTERNEXA	En el numeral 6.1 – Disponibilidad y entrega del servicio, literal a), se indica que la solución puede ser entregada como servicio (SaaS) o soportarse en una nube alternativa previamente aprobada por LA PREVISORA S.A. Solicitamos amablemente a la Entidad aclarar cuáles son las nubes alternativas que actualmente se encuentran aprobadas, o en su defecto, cuáles son los criterios técnicos, de seguridad y de cumplimiento que utiliza LA PREVISORA S.A. para otorgar dicha aprobación. Esto con el fin de garantizar que la propuesta cumpla plenamente con los lineamientos establecidos por la Entidad.	NO	LA PREVISORA S.A. no tiene una lista de nubes preaprobadas. La aprobación de una nube alternativa se hace caso a caso si la propuesta evidencia: Disponibilidad 99,5% y soporte 24/7, PCN/DRP probado semestralmente, cifrado en tránsito y en reposo, integración con SIEM (Elastic) y plataformas internas, y cumplimiento de protección de datos. El oferente asume costos de aprovisionamiento en TRIARA–Claro y cualquier migración sin afectar a la Entidad. Acción esperada: Indique en su oferta proveedor/región, esquema de cifrado, RTO/RPO propuestos, plan de integración y contingencia, y responsabilidades/costos conforme al pliego.

76	INTERNEXA	Con relación al numeral 6.2, literales a) y b), solicitamos respetuosamente a la Entidad ampliar la información sobre los siguientes aspectos, con el fin de garantizar una correcta dimensionamiento de la propuesta y mitigar riesgos durante la ejecución: 1. Infraestructura requerida en el Datacenter de LA PREVISORA S.A. • Agradecemos indicar qué tipo de infraestructura se requiere aprovisionar (capacidades de cómputo, almacenamiento, networking, racks, energía, etc.). • De igual manera, solicitamos especificar el estado actual de dicha infraestructura, así como los mantenimientos vigentes y las adecuaciones técnicas que serían necesarias para asegurar la correcta instalación, operación y continuidad del servicio. 2. Migración en caso de cambio de proveedor de Datacenter, nube o infraestructura (literal b). • Solicitamos a LA PREVISORA S.A. informar cuál es el proveedor actual del Datacenter donde se aloja la solución o componentes relacionados. • Así mismo, agradeceríamos precisar qué infraestructura, componentes, servicios o cargas de trabajo se encuentran actualmente alojados allí, con el fin de evaluar adecuadamente el alcance, riesgos y costos asociados a un eventual proceso de migración, tal como se establece en el numeral 6.2 literal b).	NO	1.Infraestructura en Datacenter de LA PREVISORA S.A. (6.2.a): El pliego no prescribe capacidades específicas (cómputo, almacenamiento, networking, racks, energía). Cada oferente debe dimensionar y aprovisionar la infraestructura que su solución requiera, coordinando directamente con el proveedor del Datacenter y asumiendo los costos de espacio/colocación y servicios asociados. LA PREVISORA S.A. no realizará inversiones adicionales en infraestructura para la operatividad del servicio. Cualquier mantenimiento/adecuación técnica se gestiona con el Datacenter conforme a las necesidades del oferente y sin afectar la operación ni los ANS del contrato. 2. Migración ante cambio de proveedor de Datacenter/nube/infraestructura (6.2.b) Proveedor actual de Datacenter: TRIARA–Comcel (Claro); el contrato está vigente hasta octubre de 2026. La obligación de planear y ejecutar cualquier migración (inventario de componentes/cargas, riesgos, costos y continuidad) es del oferente, y debe hacerse sin afectar a LA PREVISORA S.A. ni generar costos adicionales para la Entidad.
77	INTERNEXA	Solicitamos aclaración, dado que el CVE no homologa soluciones; más bien existen herramientas compatibles con CVE que utilizan correctamente sus identificadores. Agradecemos a la Entidad indicar a qué tipo de validación hace referencia el requerimiento, si corresponde al uso de soluciones CVE-Compatible, y qué documento o lineamiento oficial se debe utilizar para soportar este cumplimiento en la propuesta.	NO	el documento establece que no se exige “homologación” por CVE; se exige uso compatible con CVE/NVD. La solución debe buscar por CVE-ID y mostrar CVE-ID en hallazgos (CVE Searchable / CVE Output) y mantener mapeo/actualización frente a CVE/NVD (feeds/API) y las evidencias (manual/datasheet/capturas) donde se vea el uso de CVE-ID y el mecanismo de actualización contra CVE/NVD
78	INTERNEXA	Agradecemos a la Entidad brindar mayor claridad sobre: 1. Si está previsto algún cambio de SIEM durante la vigencia del contrato, y en caso afirmativo, cuáles serían los lineamientos o condiciones técnicas para garantizar la continuidad de la integración. 2. El estado actual de soporte y mantenimiento de la plataforma Elastic (vigencia, modalidad y alcance). 3. Las características técnicas disponibles para la integración, incluyendo si la herramienta cuenta con APIs, conectores o mecanismos estándar para interoperar con soluciones de gestión de vulnerabilidades o análisis de seguridad.	NO	1. El pliego no informa un cambio de SIEM; deben integrarse con Elastic y ajustarse si la plataforma cambiara, sin afectar ANS. 2.No se detallan vigencias de soporte de Elastic; el oferente debe garantizar la interoperabilidad y mantener la integración durante la ejecución. 3.Proponga el mecanismo técnico (p. ej., API/connector, Syslog, webhooks), con cifrado en tránsito y reposo, indicando versiones/compatibilidad y un plan de continuidad, sin costo adicional para LA PREVISORA S.A.
79	INTERNEXA	Entendemos que el sistema de analisis de vulnerabilidades puede contemplar cualquiera de las combinaciones de los literales a al c, por favor confirmar este entendimiento	NO	Su entendimiento es correcto: el sistema de análisis de vulnerabilidades puede proponerse en cualquiera de las combinaciones previstas en los literales a)–c) del numeral aplicable, siempre que se mantengan los mínimos del pliego (métodos exigidos, integración con SIEM, cifrado en tránsito y reposo, ANS de disponibilidad y entregables).
80	INTERNEXA	Por favor especificar como se acredita este requerimiento si existe algun formato pre establecido o se hace mediante carta del Representante	NO	Para efectos del proceso los solicitado se acreditará mediante la carta de presentacion, y en caso de tener conocimiento de algun caso de corrupción reportarlo conforme se solicita en el numeral.

81	INTERNEXA	Solicitamos a la Entidad evaluar la eliminación del requisito que exige que el proponente sea partner del fabricante o que aporte certificación directa del mismo, en la medida en que dicho requerimiento podría limitar la pluralidad de oferentes y la libre concurrencia. Alternativamente, proponemos que se permita que la solución sea adquirida a través de un mayorista o canal autorizado del fabricante, garantizando la originalidad del licenciamiento, las actualizaciones y el soporte oficial, sin que sea obligatorio que el prestador del servicio ostente la calidad de partner directo. Lo anterior teniendo en cuenta que, al tratarse de un servicio especializado, este puede ser prestado por un integrador distinto al proveedor del licenciamiento, siempre que se acredite la experiencia, idoneidad técnica y el equipo necesario para la correcta implementación, operación y soporte de la solución. Esta alternativa permitiría ampliar la participación de oferentes, promover la competencia efectiva y asegurar el cumplimiento del objeto contractual, sin afectar la calidad ni la seguridad de la solución ofrecida.	NO	NO PROCEDE eliminar el requisito. Se mantienen las condiciones del Documento de Condiciones Definitivas. Fundamento: El documento de condiciones exige acreditación como canal autorizado en uno de los dos niveles superiores de membresía, certificable por el fabricante, mayorista o representante oficial en Colombia (Cap. III, 3.2.b). Este criterio es objetivo y verificable (CUMPLE/NO CUMPLE) y garantiza suministro legítimo, actualizaciones y escalamiento de soporte. En consorcios/UT, la acreditación puede aportarla el integrante responsable del componente técnico, sin exigir que el integrador sea el mismo proveedor del licenciamiento (Cap. III, 1.1.5). Cualquier modificación solo procede vía adenda (Cap. I, 20); propuestas condicionadas a cambiar requisitos no son admisibles (Cap. II, 1).
82	INTERNEXA	Solicitamos la ampliacion del plazo para la prestación de las propuestas a 29 de dcieimbre de 2025, con el fin de permitar una adecuada estructuracion tecnica y económica en beneficio de la entidad	NO	Se mantienen los términos y plazos establecidos en el Documento de Condiciones Definitivas y en el cronograma vigente; cualquier modificación se procede mediante adenda y será debidamente publicada. Sin embargo, hasta esta etapa no se amplía el plazo.
83	INTERNEXA	solicitamos a la Entidad para la acreditación de la experiencia, se permita y se tenga en cuenta que los documentos soporte de los contratos aportados incluyan sus respectivos anexos técnicos, los cuales hacen parte integral del contrato y en los que se detalla el alcance, actividades y servicios efectivamente ejecutados. Lo anterior permitirá evidenciar de manera clara y objetiva la correspondencia entre la experiencia acreditada y el objeto del presente proceso, garantizando una evaluación técnica adecuada y una interpretación homogénea por parte de los proponentes y de la Entidad.	NO	Se acepta que los anexos técnicos de los contratos se presenten como soporte complementario para acreditar la experiencia, siempre que estén vinculados y firmados al contrato correspondiente y detallen objeto, alcance, valor, fechas y resultados; no obstante, se mantienen las condiciones del pliego: máximo tres (3) certificaciones (se evalúan solo las tres primeras foliadas), y la certificación emitida por el contratante sigue siendo el documento base de evaluación; en proponente plural (UT/Consorcio), los soportes pueden ser del integrante responsable del componente técnico; los anexos no sustituyen la certificación ni amplían el número admitido, y la Entidad podrá solicitar aclaraciones y soportes adicionales por una única vez, sin mejorar la oferta.
84	ALINATECH	1. Observación al literal a): Respetuosamente se sugiere a la Entidad que el literal a) quede redactado así: “El objeto, alcance y/o obligaciones del servicio sea igual o similar al de la presente invitación, entendiéndose por similar a análisis y/o implementación y/o diagnóstico y/o planificación de soluciones para la gestión de vulnerabilidades, entendiéndose como: pruebas de Ethical Hacking y/o pruebas de penetración y/o evaluación de configuración segura (Security Hardening) y/o revisión de código seguro y/o análisis de amenazas y/o simulacros de respuesta a incidentes y/o parcheo de vulnerabilidades.”	NO	Se mantiene lo establecido en el documento de condiciones, toda vez que el alcance de “igual o similar” ya está definido con precisión en el Capítulo III, 3.1 literal a) y se alinea con el Objeto establecido en el Capítulo I, 4 (gestión de vulnerabilidades mediante pruebas de ethical hacking, pruebas de penetración, hardening, revisión de código seguro (SAST), análisis de amenazas, simulacros de respuesta a incidentes y parcheo de vulnerabilidades). Incluir términos adicionales como “diagnóstico” y “planificación”, así como ampliar el uso de “y/o”, podría introducir ambigüedades y diluir el criterio operativo de equivalencia ya previsto
85	ALINATECH	2. Observación al literal c): Respetuosamente se sugiere a la Entidad revisar el literal c), dado que limitar la experiencia únicamente a contratos con duración igual o superior a doce (12) meses restringe la participación de oferentes que cuentan con contratos completamente ejecutados y alineados con el objeto del proceso, pero cuya naturaleza técnica implica periodos de ejecución más cortos, como ocurre con servicios de Ethical Hacking, pruebas de penetración, análisis de vulnerabilidades y actividades asociadas. En este sentido, se solicita permitir la acreditación de contratos con una duración inferior a doce meses, siempre que se demuestre su ejecución total y que su objeto sea igual o similar al requerido.	NO	se mantienen las condiciones del proceso: los oferentes deberán acreditar contratos totalmente ejecutados (incluidas prórrogas) con duración ≥12 meses y antigüedad ≤5 años (literal d).

86	SKG	Frente a lo anterior, atentamente solicito aclarar, si el Rubro / Concepto “SEGURIDAD INFORMÁTICA Y ADMINISTRACIÓN DE INFRAESTRUCTURA TECNOLÓGICA/SEGURIDAD INFORMÁTICA” de Año de Vigencia 2025, cuyo valor tope corresponde a UN centavo ($0,01) ¿se debe redondear al peso más cercano? ¿O se debe ofertar por ese valor tope?	NO	El valor tope de UN CENTAVO (COP $0,01) para la vigencia 2025 corresponde a una definición de presupuesto interno de la Entidad, derivada de la asignación de recursos del CDP, y refleja que el primer mes es de implementación sin cobro. Esta cifra no se redondea y no requiere ajuste por parte de los oferentes. En consecuencia, los oferentes deben presentar su propuesta económica de conformidad con el formato del ANEXO No. 8 – Propuesta Económica, respetando estrictamente la distribución por vigencia y los topes establecidos en el Documento de Condiciones. Si el formulario no admite decimales, se registra 0 en 2025 y se incluye nota aclaratoria indicando que el valor corresponde a $0,01 según el tope definido, sin modificar las condiciones del proceso.
87	SKG	Atentamente solicito aclarar las siguientes dudas: • ¿Se deben diligenciar las tres hojas de cálculo? • ¿Existen valores topes de referencia para los ítems indicados en las hojas de cálculo de Nombres “Formato Propuesta Económica” y “Hoja1” • En la Nombre de la Hoja: “Hoja2”, ¿en que celdas se debe hacer nuestro ofrecimiento económico?	NO	Por favor diligencien únicamente lo requerido en el Anexo No. 8 – Propuesta Económica, respetando los topes por vigencia establecidos en el documento
88	SKG	Atentamente solicitamos eliminar el texto subrayado, toda vez que el mismo actualmente ha sido retirado de los Decretos y Leyes que reglamentan la acreditación de la experiencia de los socios, en empresas que tienen menos de tres años de constitución, porque la misma, limitaba la creación y crecimiento de las nuevas empresas.	NO	Agradecemos su observación, sin embargo el requisito se mantiene para efectos de empresas menores a 3 años se procedera conforme lo indican los terminos.
89	SKG	Atentamente solicito confirmar que el SARLAFT en LA PREVISORA S.A., no se debe presentar conla propuesta, y este documento corresponde a documentación que debe presentar el adjudicatario dentro de los documentos de legalización del contrato.	NO	Se confirma que el requisito deberá ser acreditado por el Oferente Seleccionado, durante el periodo de formalización de contrato y su cumplimiento será obligatorio para realizar la respectiva suscripción.
90	SKG	Atentamente solicitamos indicar en el numeral indicado, que el caso de proponentes plurales, estos documentos pueden ser presentados por uno o varios de sus integrantes.	NO	La presentación de documentos por proponentes plurales (consorcios/uniones temporales) se rige estrictamente por el Documento de Condiciones Definitivas – Invitación Abierta No. 023-2025, conforme al alcance previsto en cada numeral. En ese sentido, deberán diligenciar y aportar lo requerido según el documento.
91	SKG	En relación con el requisito de acciones de remediación descrito en el Anexo 7 (condición técnica obligatoria en la sección de Seguridad, gestión y reportes, punto 4), y considerando el objeto general del contrato que incluye el tratamiento de vulnerabilidades mediante remediación,contención o mitigación, solicitamos respetuosamente aclarar el alcance, profundidad y extensión esperados para dichas acciones. En particular, ¿se espera que el proveedor asuma responsabilidades que involucren intervenciones complejas y extensas, tales como la reinstalación de sistemas operativos, modificaciones en infraestructuras críticas (por ejemplo, redes, directorio activo o componentes de seguridad), adquisición de controles o salvaguardas adicionales, o incluso la reescritura de código fuente para subsanar vulnerabilidades identificadas? Esta clarificación es relevante para equilibrar las mejores prácticas de segregación de funciones (evitando que el proveedor sea 'arte y parte' en la detección y remediación simultánea), garantizar la viabilidad económica de la propuesta y evitar interpretaciones que pudieran generar costos adicionales no contempladosen el presupuesto oficial	NO	Las acciones de remediación del Anexo 7 se entienden como recomendación, guía y acompañamiento, incluida la aplicación de parches y acciones temporales/definitivas soportadas por la plataforma, con informe y re-test (Cap. III, §§3.4.3.4 y 3.4.6.7–9). No se espera que el proveedor ejecute intervenciones complejas fuera del alcance (p. ej., reinstalaciones de SO, cambios en infraestructura crítica como redes/AD/seguridad, adquisiciones o reescritura de código); esos casos se escalan a las áreas internas o terceros. Se mantiene la segregación de funciones y los topes del presupuesto; la verificación será CUMPLE/NO CUMPLE conforme al documento

92	SKG	Solicitamos respetuosamente aclarar si serán consideradas válidas y puntuables las simulaciones controladas de ataques que se ejecuten mediante plataformas de emulación de adversarios open source y de libre uso, ampliamente adoptadas por la comunidad internacional de ciberseguridad, siempre que dichas plataformas estén plenamente alineadas con el marco MITRE ATT&CK (incluyendo el mapeo completo de técnicas, tácticas y procedimientos), permitan la generación de reportes detallados de las cadenas de ataque simuladas, evidencien el impacto potencial sobre los activos de LA PREVISORA S.A. y se realicen en entornos controlados o de laboratorio que garanticen cero riesgo para los sistemas productivos. Esta aclaración resulta relevante para dimensionar adecuadamente el compromiso técnico y económico que se incluirá en la propuesta.	NO	Sí. Las simulaciones controladas de ataques realizadas con plataformas de emulación de adversarios open source serán válidas y puntuables siempre que cumplan lo exigido en el Factor Técnico 1.2.2: estar respaldadas por carta de compromiso, corresponder a las categorías allí previstas y ejecutarse durante la vigencia, con informe de resultados y planes de mejora. Se deberán realizar en entornos controlados, sin afectar la operación; la taxonomía de incidentes de la Superfinanciera es la referencia obligatoria indicada en el documento (Notas 1–3 del 1.2.2). Para claridad: el condicionamiento de "no open source" aplica solo al requisito de escaneos a demanda (Cap. I 6.8.d / Cap. III 3.4.6.5); no restringe el uso de herramientas open source en estas simulaciones controladas. Se mantienen las condiciones del documento.
93	SKG	Solicitamos respetuosamente aclarar el alcance detallado y extensión de las capacidades requeridas en los literales a), b) y c), considerando que una solución comercial que cumpla estrictamente con dichas funcionalidades (por ejemplo, plataformas de alto nivel con IA/ML integrada) podría desbordar el presupuesto, haciendo económicamente inviable la propuesta para muchos oferentes y potencialmente limitando la competencia en el proceso. En este contexto, ¿se aceptarán soluciones de tipo open source, abiertas o de bajo costo (con soporte enterprise opcional), siempre que demuestren cumplimiento equivalente y carta firmada por el representante legal, y que estén alineadas con las mejores prácticas de ciberseguridad. Esta aclaración es esencial para dimensionar adecuadamente la propuesta técnica y económica, garantizando la viabilidad del proyecto y el cumplimiento de los objetivos de la invitación.	NO	Por favor remítanse al Documento de Condiciones Definitivas – Invitación Abierta No. 023-2025. Para los literales a), b) y c) del Factor Técnico, la evaluación será CUMPLE/NO CUMPLE con los soportes allí exigidos (brochure/datasheet y carta firmada). El tipo de solución (comercial, abierta o open source) se rige por lo indicado en el documento y sus excepciones.
94	SKG	Solicitamos respetuosamente aclarar el alcance exacto del servicio esperado, específicamente si se limita a las actividades iniciales de respuesta a incidentes (preservación, adquisición e inicio de cadena de custodia de evidencia digital con entrega de informe preliminar) o si se exige la realización de la investigación forense completa (análisis de memoria, disco, red, reconstrucción de línea de tiempo, identificación de actores de amenaza y elaboración de informe pericial apto para procesos judiciales o regulatorios). Adicionalmente, solicitamos confirmar si será aceptado el uso de herramientas forenses open source ampliamente reconocidas. Esta aclaración resulta indispensable para dimensionar adecuadamente el perfil, cantidad y costo del recurso humano especializado, así como para garantizar la viabilidad económica de la propuesta sin incurrir en sobrecostos que afecten la competitividad del proceso	NO	Por favor remítanse al Documento de Condiciones Definitivas – Invitación Abierta No. 023-2025. En el Factor Técnico 1.2.1 (Análisis Forense) se exige la disponibilidad y activación del servicio forense, liderazgo del proceso ante incidentes y la documentación/capacitación asociada, sin que el documento obligue a realizar una investigación forense integral de tipo pericial/judicial. La verificación será CUMPLE/NO CUMPLE conforme a los entregables allí listados. Respecto al uso de herramientas forenses open source, el documento no establece restricción específica para esta actividad; la única restricción "no open source" aplica a escaneos a demanda (Cap. I 86.8.d y Cap. III 3.4.6.5). En todos los casos deben cumplirse las buenas prácticas (entornos controlados, cadena de custodia, informes). Cualquier cambio solo procede mediante Adenda.
95	Octapus	1. Por favor aclarar si el entendimiento es el correcto y este requerimiento hace referencia a la solución a usar para escaneo de vulnerabilidades de los 500 IP/host y 50 servicios Web?.	NO	Sí, el entendimiento es correcto. El requerimiento se refiere a la solución/plataforma de gestión de vulnerabilidades que debe realizar el escaneo (continuo y a demanda) sobre al menos 500 IP/HOST y 50 servicios web (ver Cap. I 6.4 y Cap. III 3.4.1). Adicionalmente, para escaneos a demanda se exige herramienta licenciada (no open source) (Cap. I 6.8.d / Cap. III 3.4.6.5). Se mantienen las condiciones del documento.

96	Octapus	2. Por favor aclarar si este soporte técnico hace referencia hacia problemas y/o incidentes en la herramienta o a que tipo de incidentes se refieren, y si se puede realizar la atención a los mismos de forma virtual/remota.	NO	El soporte técnico cubre tanto problemas de la plataforma/servicio de gestión de vulnerabilidades como incidentes de seguridad vinculados a la solución (eventos que afecten o puedan afectar la disponibilidad, integridad o confidencialidad). La atención puede realizarse de forma remota o presencial, conforme al plan de gestión de incidentes previsto en la propuesta; para incidentes críticos se exige soporte 24/7 y prioridad de respuesta dentro de 2 horas hábiles desde la detección. En consecuencia, la verificación se hará bajo CUMPLE/NO CUMPLE de conformidad con el Documento de Condiciones Definitivas – Invitación Abierta No. 023-2025.
97	Octapus	3. Dentro del documento “Documento_Condiciones Definitivas_INVAB_0xx-2025V4”, en el ítem 6.11 Análisis de Código, por favor informar cuantas aplicaciones propias tienen?.	NO	El Documento de Condiciones Definitivas no especifica la cantidad de aplicaciones propias. En 6.11 (Análisis de código) y Cap. III 3.4.6.9 solo se indica que el SAST debe cubrir aplicaciones propias (hasta 20.000 líneas en Java) y realizar máximo dos análisis a demanda por año, por lo tanto, las propuestas deben contemplar lo señalado en el documento de condiciones.
98	Octapus	4. Dentro del documento “Documento_Condiciones Definitivas_INVAB_0xx-2025V4”, en el ítem 6.11 Análisis de Código, por favor si las 20 mil líneas de código en Java, es por cada aplicación o por el total de la aplicaciones propias?.	NO	El límite de “hasta 20.000 líneas de código en Java” del ítem 6.11 – Análisis de Código aplica por aplicación en los ejercicios SAST de aplicaciones propias. El documento no establece una suma global de líneas para todas las aplicaciones; se mantiene lo previsto en 6.11 y Cap. III 3.4.6.9. En consecuencia, la verificación se hará bajo CUMPLE/NO CUMPLE conforme al Documento de Condiciones Definitivas.
99	Octapus	5. Dentro del documento “Documento_Condiciones Definitivas_INVAB_0xx-2025V4”, en el ítem 6.13 Capacitación, mencionan “a) Brindar una capacitación virtual de máximo 2 horas en los años 2026 y 2027, sobre el uso de la solución a un máximo de 20 personas, entregando: grabación, material didáctico y evaluación (si aplica). Estará enfocada a mostrar bondades y formas de revisión y validación de la plataforma, para lo cual se acordará entre las partes el plan de capacitación”. Podrían por favor aclarar esta capacitación en la solución hace referencia a la solución de escaneo de vulnerabilidades o a que solución?.	NO	La capacitación del ítem 6.13 se refiere al uso de la solución objeto del contrato: la plataforma integral de gestión de vulnerabilidades (SaaS) ofrecida por el proveedor. No se limita únicamente al módulo de escaneo; abarca las funcionalidades de descubrimiento, análisis, tableros y reportes, validación de hallazgos y seguimiento de remediaciones, conforme a lo indicado (“mostrar bondades y formas de revisión y validación de la plataforma”). El plan de capacitación se acordará entre las partes, manteniendo lo previsto en el Documento de Condiciones Definitivas.
100	Octapus	6. Dentro del documento “Documento_Condiciones Definitivas_INVAB_0xx-2025V4”, en el ítem 6.15 Pruebas de ingeniería Social, mencionan “…e incluirán como mínimo los siguientes vectores de ataque: phishing, spear phishing y ataques de insiders entre otros.” Pudieran por favor aclarar cuantos vectores de ataque mínimo se deben considerar por prueba.	NO	Por cada prueba anual de ingeniería social se deberán incluir mínimo tres (3) vectores de ataque: phishing, spear phishing y ataques de insiders. Se mantiene lo indicado: alcance acordado con la entidad y muestra mínima de 200 usuarios. Esta precisión no modifica las condiciones del documento.
101	Octapus	7. Solicitamos amablemente a la entidad modificar lo indicado dentro del documento en el ítem 3.2 Certificaciones del Proponente las opciones del requerimiento solicitado de la siguiente forma: c) EL PROPONENTE debe entregar confirmación de que la solución a entregar para la gestión de vulnerabilidades esta como Líder en al menos uno de los siguientes rankings internacionales: Gartner, Forrester Wave, GigaOm Radar o SC MEDIA Awards en las categorías de Vulnerability Assessment, Vulnerability Managemet Software, Risk Management Consulting, Security Consulting Services, Exposure Assessment Platforms o Unified Vulnerability Management. Este reconocimiento debe corresponder a la versión más reciente publicada por cada entidad.	NO	La solicitud no procede. Se mantiene el texto del literal c) tal como fue publicado: el proponente debe acreditar que la solución está como Líder en al menos uno de los siguientes rankings internacionales (Gartner, Forrester Wave, GigaOm Radar o SC MEDIA Awards) en las categorías Vulnerability Assessment, Vulnerability Management Software, Risk Management Consulting o Security Consulting Services, y que el reconocimiento corresponda al reporte más reciente.

102	Octapus	8. Para el equipo mínimo de trabajo dentro del ítem 3.3 Recurso Humano Mínimo Habilitante, para el perfil “Gerente del Proyecto”, en el requerimiento de Educación pudieran por favor considerar el siguiente ajuste: 1. Ingeniero de sistemas electrónico o afines. 2. Estudios de Postgrado en Gerencia, Gestion o Dirección de Proyectos y/o con certificación PMP (Project Management Professional), PMI-ACP (Agile Certified Practitioner) y/o Scrum Máster Certified (SMC) 3. Debe contar con al menos una de las siguientes Certificaciones: • CISSP – Certified Information Systems Security Professional • CISM – Certified Information Security Manager • ISO/IEC 27001/2022 Lead Implementer o Lead Auditor o Internal Auditor • CRISC – Certified in Risk and Information Systems Control • ISO 27032 – Auditor en Ciberseguridad • CSFPC (Cybersecurity Framework Professional Certificate)	NO	La solicitud no procede. Se mantienen las condiciones publicadas en el numeral 3.3 – Recurso Humano Mínimo Habilitante para el perfil Gerente del Proyecto, incluyendo: Formación: Ingeniero de sistemas, electrónico o afines, con posgrado en Gerencia/Gestión/Dirección de Proyectos y/o certificación PMP, PMI-ACP y/o SMC. Certificación (al menos una): CISSP, CISM, ISO/IEC 27001/2022 Lead Implementer o Lead Auditor, CRISC, ISO 27032 – Auditor en Ciberseguridad, CSFPC. El agregado de ISO/IEC 27001/2022 Internal Auditor no sustituye las certificaciones mínimas exigidas (Lead Implementer o Lead Auditor). El oferente puede aportar certificaciones adicionales como valor agregado; no obstante, la verificación se realizará bajo el esquema CUMPLE/NO CUMPLE respecto de los requisitos mínimos establecidos en el documento.
103	Octapus	9. Para el equipo mínimo de trabajo dentro del ítem 3.3 Recurso Humano Mínimo Habilitante, para el perfil “Gerente del Proyecto”, en el requerimiento de Experiencia pudieran por favor considerar el siguiente ajuste: Experiencia mínima de cinco (5) años como Gerente o director de Proyectos, acreditando al menos dos proyectos en ciberseguridad y/o pruebas de análisis de vulnerabilidades y/o Hacking ético y/o Red Team y/o relacionado con la implementación o mantenimiento de SGSI demostrable con certificación Laboral.	NO	La solicitud no procede. Se mantiene lo dispuesto en el numeral 3.3 para el perfil Gerente del Proyecto:Experiencia mínima de cinco (5) años como Gerente o Director de Proyectos, acreditando al menos dos (2) proyectos en ciberseguridad y/o relacionados con la implementación o mantenimiento del SGSI, demostrables mediante certificación laboral.
104	Octapus	10. Dentro del objeto de la presente Invitación Abierta mencionaban “ “EL PROVEEDOR se obliga con LA PREVISORA S.A., a prestar un servicio especializado que proporcione una solución tecnológica de gestión de vulnerabilidades, orientada a la identificación, detección, prevención, análisis, monitoreo continuo y seguimiento en tiempo real de vulnerabilidades presentes en los activos tecnológicos de LA PREVISORA S.A., que incluya servicios de análisis de código seguro, ejecución de pruebas de penetración y ethical hacking, análisis técnico y priorización de las vulnerabilidades detectadas, el tratamiento inmediato mediante acciones de remediación, contención o mitigación en tiempo real y la implementación de postura de seguridad (Hardening) sobre los activos tecnológicos de La Previsora.” Podrían por favor aclarar si dentro del proyecto se debe realizar alguna actividad de hardening, y si sí, sobre que tecnologías y/o dispositivos se deberá realizar y su periodicidad.	NO	Sí. Conforme al Objeto del proceso, la prestación del servicio incluye la implementación de postura de seguridad (Hardening) sobre los activos tecnológicos de la entidad (Cap. I, 4). El hardening se aplica sobre los activos gestionados por la solución y dentro del alcance técnico descrito, entre los que se encuentran: servidores Windows/Linux virtualizados, dispositivos de seguridad Fortinet, periféricos (p. ej., impresoras HP y teléfonos NEC), dispositivos de red (switches HP y inalámbrico Aruba), servicios web (p. ej., IIS, Apache Tomcat) y bases de datos (SQL Server, MySQL, Oracle, Sybase), de acuerdo con los hallazgos y buenas prácticas (Cap. I, 6.3; Cap. III, 3.4.1.8 y 3.4.4). En cuanto a la periodicidad, el documento no fija un cronograma específico por activo. El hardening se ejecutará de forma continua y/o a demanda, derivado de la criticidad y del análisis de vulnerabilidades, con evidencias en los informes mensuales (Cap. III, 3.5.3), seguimientos semanales (Cap. III, 3.5.8) y los re-tests asociados a las pruebas de ethical hacking semestrales (Cap. III, 3.5.6), manteniendo las condiciones publicadas.
105	Octapus	11. La presencialidad del ingeniero “Analista de seguridad” se requiere ante eventos programados o se requiere cumplir con algunos días de presencialidad. Adicional podrían informar cual sería el horario de cubrimiento de labores de este perfil.	NO	Conforme al numeral 3.3 – Recurso Humano Mínimo Habilitante, el Analista de seguridad debe estar dedicado 100% en modalidad híbrida (presencial y virtual), en el horario laboral de LA PREVISORA S.A. de lunes a viernes de 8:00 a.m. a 5:00 p.m., y cuando sea requerido por LA PREVISORA S.A. para un incidente de seguridad, en horario no hábil. los demas recursos no se establecen días fijos de presencialidad. La asistencia presencial se requerirá para eventos programados (p. ej., reuniones, pruebas, capacitaciones, despliegues) o cuando lo solicite el supervisor, y se definirá en el plan de trabajo y cronograma del kickoff (Cap. III, 3.5.1). Cobertura de incidentes

106	Octapus	12. La solución de Monitoreo y escaneo de vulnerabilidades puede ser 100% SaaS en nube sin necesidad de requerir infraestructura local o se requiere solución local de hardware físico.	NO	Conforme al numeral 6.1.a del Documento_Condiciones Definitivas, la solución puede entregarse 100% como servicio (SaaS) en nube, sin requerir infraestructura local. Adicionalmente, el documento prevé que el proveedor también puede soportar instalación en nube alternativa o, si llegara a ser necesario, realizar aprovisionamiento en el Datacenter de LA PREVISORA S.A. (ver 6.2 y 3.4.1). En este último caso, los costos asociados al aprovisionamiento (principal o alterno) son a cargo del proponente y, de optar por despliegue en sitio, la arquitectura deberá cumplir con lo indicado en 6.14 (separación/independencia del sistema).
107	Octapus	13. La administración principal de la herramienta de Monitoreo y escaneo de vulnerabilidades estará a cargo de la entidad o será una tarea delega al equipo de ingeniería del contratista?.	NO	De acuerdo con las Obligaciones específicas de EL OFERENTE/PROVEEDOR (numeral 6.3), la administración, actualización y mantenimiento de la solución están a cargo del contratista. Asimismo, dentro del Recurso Humano Mínimo Habilitante (numeral 3.4.6.1) el Analista de seguridad del proveedor debe garantizar la administración y gestión de la solución, los informes y el control de vulnerabilidades.
108	Octapus	14. Podrían por favor compartir los formatos de anexos en formato editable Word.	NO	En atención a su solicitud, se informa que los formatos y anexos del proceso se ponen a disposición de todos los oferentes únicamente en formato PDF, mediante publicación en la página web de La Previsora. En consecuencia, no se entregan formatos en Word ni de manera particular a ningún proponente. Cualquier actualización o cambio a los documentos se realizará exclusivamente mediante adenda y será publicada para conocimiento general en formato PDF.
109	Octapus	15. Podrían por favor compartir todas las preguntas y respuestas de los otros oferentes para retroalimentarnos con las consultas y respuestas generadas.	NO	Conforme al Documento de Condiciones Definitivas (Cap. I, numerales 19 y 28, y Cronograma – numeral 17), una vez cerradas las etapas correspondientes, LA PREVISORA S.A. publica en la página web institucional el consolidado de preguntas y sus respuestas del proceso. Esta información no se remite de manera particular; se divulga únicamente por los canales oficiales y en las fechas previstas.
110	OLIMPIAIT	En el marco del proceso licitatorio mencionado, respetuosamente solicito que se considere la siguiente adecuación en los requisitos de certificación del profesional propuesto para el perfil de gerente de proyecto: 1. Certificaciones principales (requeridas) Se solicita que se acepten como habilitantes las siguientes certificaciones de gestión de proyectos, ampliamente reconocidas a nivel internacional:PMP – Project Management Professional y SCRUM Master / SCRUM Product Owner (según la necesidad del rol) Ambas acreditaciones garantizan competencias sólidas en gestión de proyectos bajo enfoques predictivos y ágiles, asegurando una adecuada dirección, planificación, seguimiento y control del proyecto. 2. Certificaciones complementarias (opcionales / valorables): Asimismo, solicitamos que se consideren como certificaciones opcionales o puntuables, que suman valor agregado al profesional, las siguientes acreditaciones internacionales en ciberseguridad, gestión de riesgos y sistemas de gestión asÍ: CISSP – Certified Information Systems Security Professional y/o CISM – Certified Information Security Manager y/o ISO/IEC 27001:2022 Lead Implementer o Lead Auditor y/o CRISC – Certified in Risk and Information Systems Control y/o ISO 27032 – Auditor en Ciberseguridad y/o CSFPC – Cybersecurity Framework Professional Certificate Estas certificaciones, aun siendo especializadas, no afectan la capacidad del profesional de geretem de proyecto.	NO	La solicitud no procede. Se mantienen los requisitos del documento: Formación: Ingeniero de sistemas/electrónico o afines con posgrado en proyectos y/o certificación PMP, PMI-ACP y/o SMC. Obligatorio acreditar al menos una certificación de seguridad: CISSP, CISM, ISO/IEC 27001:2022 Lead Implementer/Lead Auditor, CRISC, ISO 27032 – Auditor o CSFPC. Las certificaciones PMP/Scrum pueden presentarse como valor agregado, pero no sustituyen la certificación mínima en seguridad exigida para habilitar el perfil. Esta aclaración no modifica las condiciones del documento.

111	OLIMPIAIT	Con respecto a esta indicación en el pliego, se entiende que este personal requerido, debe ser contratado directamente por el proponente durante la ejecución del contato, sin terceros e intermediarios. Es correcta nuestra apreciación? De lo contrario, requerir que el personal deba estar contratado antes de surtir una adjudicación.	NO	1.Sí, su apreciación es correcta: el personal mínimo debe estar contratado directamente por el proponente durante la ejecución, sin terceros ni intermediarios. 2.No se exige que esté contratado antes de la adjudicación; de resultar seleccionado, el proponente debe entregar HV y soportes en máximo 10 días hábiles. 3.Cualquier cambio requiere aprobación del supervisor y reemplazo con perfil igual o superior; los roles mínimos no se tercerizan. Aplican penalidades por no asignación/afectación del servicio (Cap. III, 3.6 y Minuta – cesión/subcontratación).
112	OLIMPIAIT	Respetuosamente solicitamos que, para la acreditación de los 30 puntos del factor ambiental, se contemple como válido que la compañía haya implementado su Plan de Gestión Ambiental en el año 2025, toda vez que se requiere de un tiempo razonable para evidenciar aspectos de su ejecución. La implementación de un plan de esta naturaleza implica fases progresivas para obtener resultados y registros que solo pueden generarse con el transcurso del tiempo. En este sentido, proponemos que se acepte como alternativa la presentación del plan adoptado y vigente a la fecha de la oferta, en tanto se avanza en la generación de evidencias propias de su implementación.	NO	El criterio definido para la asignación del puntaje ambiental exige que el oferente cuente con un Plan de Gestión Ambiental iplementado, no menciona la fecha del mismo, lo cual implica no solo su adopción formal, sino también la existencia de acciones, registros y evidencias que demuestren su ejecución efectiva. Entendemos que la implementación de un plan ambiental puede requerir fases progresivas, pero para efectos de calificación en el presente proceso, es necesario contar con elementos verificables que respalden su aplicación. Esto garantiza el compromiso ambiental del oferente. Por lo anterior, el criterio se mantiene dada la importancia de demostrar no solo su adopción, sino también su implementación y ejecución.
113	OLIMPIAIT	Se entiende que para las empresas que no manejan residuos peligrosos, el puntaje total asignado de gestion de residuos, aplican los 15 puntos. Es claro nuestro entendimiento?. Por favor aclarar	NO	Todos los oferentes, independientemente del tipo de residuos que generen, deben certificar mediante el representante legal los tipos de residuos generados en el desarrollo de su objeto social y presentar Certificados de disposición final de dichos residuos, con fecha de expedición no mayor a un (1) año antes de la entrega y/o presentación de la propuesta. En el caso de empresas que no generan residuos peligrosos, deberán demostrar la adecuada gestión de los residuos ordinarios o reciclables que sí se generen, conforme a la normatividad vigente. Por lo tanto, el cumplimiento de estos requisitos es necesario para la asignación del puntaje correspondiente, sin que se otorgue automáticamente por NO generar residuos peligrosos.
114	OLIMPIAIT	Respetuosamente se solicita a la PREVISORA, aplazar la entrega de ofertas en por lo menos cinco (5) días hábiles, por todos los temas de dimensionamiento y costeo de la solución requerida y de esta forma poder presentar una propuesta aterrizada que se ajueste a los requerimientos de la enidad.	NO	Se mantiene el cronograma publicado en el Documento de Condiciones Definitivas. Cualquier ajuste solo procede mediante adenda y será publicado por los canales oficiales. En ausencia de adenda, las fechas y horas de cierre del proceso se conservan

115	OLIMPIAIT	El Numeral 3.1.a. establece que la experiencia se acreditará mediante un objeto contractual que sea "igual o similar al de la presente invitación". Para definir la similitud, se proporciona una lista amplia de siete (7) categorías de servicios, incluyendo, entre otros: Análisis y/o implementación de soluciones para la gestión de vulnerabilidades, Pruebas de Ethical Hacking, Revisión de código seguro, y Análisis de amenazas y Simulacros de respuesta a incidentes . Considerando que la Entidad permite presentar hasta un máximo de tres (3) certificaciones para acreditar la experiencia, la redacción actual genera una ambigüedad sobre la condición mínima que debe cumplir cada una de dichas certificaciones: 1. Si se debe entender que el objeto contractual de cada certificación debe incluir la totalidad de los siete (7) tipos de servicios listados para ser considerado "similar". 2. Si basta con que el objeto contractual de cada certificación incluya al menos una de las categorías de servicios indicadas en la lista, para ser considerada como experiencia "similar" y relevante al proceso. Una interpretación restrictiva (opción 1) limitaría la concurrencia, pues las actividades listadas combinan servicios de índole continua (monitoreo, gestión de vulnerabilidades) con servicios de índole puntual o proyectual (Ethical Hacking, Revisión de código seguro) . Con base en lo expuesto, y con el propósito de garantizar la claridad y objetividad en la verificación del cumplimiento del requisito habilitante, solicitamos a LA PREVISORA S.A. que aclare y confirme, que: Para efectos del cumplimiento del Numeral 3.1.a., bastará con que el objeto contractual de cada certificación presentada contenga y acredite la ejecución de, al menos, una de las categorías de servicios listadas por la Entidad como experiencia "similar", permitiendo así que la sumatoria de las certificaciones (máximo tres) demuestre el expertise relevante en el campo de ciberseguridad.	NO	Por favor acójase estrictamente a lo señalado en el Documento de Condiciones Definitivas. La verificación de la experiencia “igual o similar” y el cumplimiento del requisito se realizará únicamente conforme al texto vigente del numeral 3.1.
116	OLIMPIAIT	El objeto definido en el presente proceso incorpora un alcance amplio que incluye múltiples actividades de ciberseguridad (identificación, detección, análisis, monitoreo continuo, seguimiento en tiempo real, priorización y remediación de vulnerabilidades, entrega de reportes y colaboración directa con el equipo interno). Sin embargo, exigir que la certificación de experiencia cumpla con la totalidad de estas actividades en un único contrato puede resultar restrictivo para la pluralidad de oferentes, dado que no todas las entidades contratan todos estos servicios de manera conjunta en un solo proyecto. En la práctica, la prestación de servicios de seguridad informática se realiza a través de contratos que abarcan distintos componentes (p. ej., gestión de vulnerabilidades, monitoreo continuo, análisis y priorización, gestión de incidentes, etc.), los cuales pueden estar distribuidos en diferentes contratos sin que ello desvirtúe la idoneidad ni la pertinencia de la experiencia. Se sugiere que el pliego aclare que la experiencia presentada podrá corresponder a uno o varios contratos que incluyan actividades relacionadas con el objeto, siempre que, en conjunto, evidencien la prestación de servicios especializados de ciberseguridad de características similares a las requeridas.	NO	El numeral 3.1 permite acreditar la experiencia con máximo tres (3) certificaciones de contratos. No se exige que un solo contrato contenga la totalidad de actividades del objeto; la verificación de “igual o similar” se realiza respecto de las categorías de servicio relacionadas con el objeto. La sumatoria de las certificaciones debe alcanzar como mínimo el 100% del presupuesto oficial, y cada contrato debe cumplir plazo ≥ 12 meses y antigüedad ≤ 5 años, además de las condiciones de validez (objeto, fechas, valor, firma y datos del firmante). Cuando una certificación incluya varios contratos, el oferente debe identificar si son adiciones al principal o contratos diferentes y precisar cuáles pretende usar para acreditar la experiencia, conforme al texto del pliego. La evaluación se realizará únicamente bajo el esquema CUMPLE/NO CUMPLE previsto en el documento, sin precisiones adicionales.

117	OLIMPIAIT	Con el fin de evitar interpretaciones restrictivas que limiten la pluralidad de oferentes y evitar rechazos de propuestas por motivos semánticos en lugar de sustanciales, se solicita a LA PREVISORA S.A. que aclare y confirme que se aceptarán como equivalentes y válidos los objetos contractuales que, aun cuando empleen una redacción distinta, acrediten de manera funcional actividades equivalentes a las categorías listadas en el Numeral 3.1.a: Ejemplos: 1. "Evaluación de vulnerabilidades" y "Servicios de análisis de vulnerabilidades" corresponden directamente a "análisis y/o implementación de soluciones para la gestión de vulnerabilidades". 2. "Pruebas de intrusión" y "Ethical Hacking" corresponden directamente a "pruebas de Ethical Hacking" y "pruebas de penetración (Pentesting)". 3. "Evaluación de código fuente" corresponde directamente a "revisión de código seguro". De esta manera se asegura que la acreditación de experiencia se fundamente en la naturaleza del servicio efectivamente prestado y no en una literalidad semántica del objeto contractual.	NO	Se mantiene lo señalado en el Documento de Condiciones Definitivas. Para la verificación de la experiencia “igual o similar”, LA PREVISORA S.A. evaluará el contenido funcional de las certificaciones y su relación directa con las categorías previstas en el numeral 3.1.a, no la literalidad del texto.
118	OLIMPIAIT	La acreditación de la Experiencia Técnica Habilitante se entenderá cumplida si el objeto contractual de la certificación, o la sumatoria de las certificaciones presentadas (máximo tres), acredita la ejecución de, al menos, una de las categorías de servicios listadas como "similar". Esta aclaración es crucial para garantizar el principio de selección objetiva al validar el expertise demostrable de los oferentes en el ámbito de la ciberseguridad avanzada.	NO	se ratifica lo previsto en el Capítulo III, numeral 3.1 (Experiencia del Proponente): la experiencia habilitante se acredita con máximo tres (3) certificaciones cuyo objeto sea igual o similar al listado de servicios definido (p. ej., gestión de vulnerabilidades, pruebas de Ethical Hacking/Pentesting, hardening, análisis de código seguro, simulacros de respuesta a incidentes, parcheo), siempre que se cumplan todas las condiciones exigidas: (i) la cuantía de la sumatoria de las certificaciones sea ≥ 100% del presupuesto oficial; (ii) el plazo de ejecución de cada contrato sea ≥ 12 meses; y (iii) la antigüedad no supere 5 años a la fecha de la propuesta (además de los requisitos formales indicados en el mismo numeral). En ese sentido, la “similitud” se verifica por correspondencia directa con las categorías de servicios listadas, pudiendo acreditarse una o varias de ellas según el alcance real de cada certificación, pero sin que ello releve al oferente de cumplir la sumatoria de cuantía, plazos y antigüedad exigidos; la validación se realiza bajo criterio CUMPLE/NO CUMPLE, manteniendo el principio de selección objetiva y las reglas del documento sin modificación.
119	OLIMPIAIT	Se observa que la exigencia de experiencia en “análisis y/o implementación de soluciones para la gestión de vulnerabilidades” resulta incongruente con el objeto del presente proceso, el cual corresponde a la contratación de un servicio especializado de seguridad informática. La inclusión del término “implementación de soluciones” remite a actividades de suministro o despliegue tecnológico, distintas a la naturaleza del servicio requerido, lo que podría restringir injustificadamente la participación. Se sugiere ajustar el requisito, limitándolo a la prestación de servicios relacionados con el análisis, gestión o monitoreo de vulnerabilidades, en coherencia con el objeto contractual.	NO	Se aclara que el requisito de experiencia en “análisis y/o implementación de soluciones para la gestión de vulnerabilidades” se mantiene conforme al Capítulo III, 3.1 (Experiencia del Proponente), en tanto resulta coherente con el objeto del proceso definido en el Capítulo I, 4 (Objeto) y con las obligaciones técnicas del servicio (v.gr. 6.1, 6.3 y Capítulo III, 3.4.1)

120	OLIMPIAIT	El Objeto Principal está centrado en la provisión de un "servicio especializado de seguridad informática" basado en el "monitoreo continuo". Si bien el primer mes está destinado a la implementación de la solución, este periodo se considera parte del proceso de alistamiento e instalación y no genera costo alguno para LA PREVISORA S.A., lo que refuerza el carácter de servicio continuo y no de proyecto de integración o adquisición y posterior implementación de una solución. No obstante, el Numeral 3.1.a. exige experiencia en "implementación de soluciones para la gestión de vulnerabilidades". La inclusión explícita del término "implementación de soluciones" puede interpretarse como la exigencia de experiencia en proyectos de adquisición, integración o desarrollo de infraestructura, lo cual podría ser desproporcionado y no estrictamente coherente con la naturaleza de servicio continuo (SaaS) y monitoreo en tiempo real que constituye el corazón del Objeto Principal. En aras de la coherencia del proceso y para asegurar que la experiencia solicitada sea adecuada y proporcionada al Objeto Principal del contrato, se solicita a LA PREVISORA S.A. aclarar que la experiencia en la categoría mencionada se limita al componente de "Análisis y Gestión de Vulnerabilidades" o que, en su defecto, se elimine el término "y/o implementación de soluciones" de dicho literal.	NO	En atención a la observación, se ratifica lo dispuesto en el Cap. I, 4 (Objeto)—servicio especializado de seguridad informática con monitoreo continuo—y en el Cap. I, 9 (Plazo)—primer mes de alistamiento/implementación sin costo—aclarando que, en el Cap. III, 3.1.a (Experiencia del Proponente), la referencia a “análisis y/o implementación de soluciones para la gestión de vulnerabilidades” no alude a proyectos de adquisición o despliegue de infraestructura, sino a la puesta en marcha operativa de la plataforma SaaS o nube aprobada, su parametrización, integración y administración requeridas por los numerales 6.1.a, 6.3 y Cap. III, 3.4.1 del documento
121	OLIMPIAIT	El Objeto Principal está centrado en la provisión de un "servicio especializado de seguridad informática" basado en el "monitoreo continuo". Si bien el primer mes está destinado a la implementación de la solución, este periodo se considera parte del proceso de alistamiento e instalación y no genera costo alguno para LA PREVISORA S.A., lo que refuerza el carácter de servicio continuo y no de proyecto de integración o adquisición y posterior implementación de una solución. No obstante, el Numeral 3.1.a. exige experiencia en "implementación de soluciones para la gestión de vulnerabilidades". La inclusión explícita del término "implementación de soluciones" puede interpretarse como la exigencia de experiencia en proyectos de adquisición, integración o desarrollo de infraestructura, lo cual podría ser desproporcionado y no estrictamente coherente con la naturaleza de servicio continuo (SaaS) y monitoreo en tiempo real que constituye el corazón del Objeto Principal. Alternativamente, se solicita confirmar que la experiencia en "Análisis de amenazas y Simulacros de respuesta a incidentes" o la experiencia en "evaluación de vulnerabilidades" será considerada suficiente para cumplir con esta subcategoría de experiencia similar.	NO	En atención a la observación, se ratifica lo dispuesto en el Cap. I, 4 (Objeto)—servicio especializado de seguridad informática con monitoreo continuo—y en el Cap. I, 9 (Plazo)—primer mes de alistamiento/implementación sin costo—aclarando que, en el Cap. III, 3.1.a (Experiencia del Proponente), la referencia a “análisis y/o implementación de soluciones para la gestión de vulnerabilidades” no alude a proyectos de adquisición o despliegue de infraestructura, sino a la puesta en marcha operativa de la plataforma SaaS o nube aprobada, su parametrización, integración y administración requeridas por los numerales 6.1.a, 6.3 y Cap. III, 3.4.1 del documento
122	OLIMPIAIT	Las condiciones técnicas y obligatorias mínimas indican una fuerte orientación y requisito de que el proyecto se cumpla mediante una única solución o plataforma tecnológica integrada. Si bien el documento utiliza a menudo el singular ("la solución", "la herramienta"), la condición radica en la exigencia de integración y centralización de todas las capacidades requeridas dentro de una misma oferta licenciada, es decir, la entidad no solo pide una herramienta, sino que exige que las distintas funcionalidades coexistan o se entreguen desde una única estructura central. A continuación, se detallan los puntos que sustentan esta interpretación de "Plataforma Única e Integrada": • Entrega como Servicio (SaaS): La herramienta debe entregarse como servicio (SaaS), preferiblemente en la nube del fabricante. La documentación se refiere consistentemente a "La herramienta ofrecida" y al sistema de análisis de vulnerabilidades (singular). • Licenciamiento Consolidado: Se exige incluir licencias para activos de red (IP/HOST) y para servicios web, y se especifica que estos últimos "deberán estar incluidos dentro de la misma plataforma a entregar". Esto refuerza que las licencias para el escaneo de aplicaciones y de infraestructura deben ser gestionadas a través de una única plataforma central. • Gestión Centralizada y Módulos: Se requiere que la herramienta incluya la administración, mantenimiento y gestión por parte del oferente, y que garantice la integración con múltiples plataformas tecnológicas internas. Más adelante, para los aspectos calificables, se otorgan puntos a la herramienta que integre un "módulo de gestión de postura de seguridad", lo que implica que las capacidades de monitoreo deben ser parte de la solución central. • Funcionalidades del Recurso Humano: El Analista de Seguridad debe garantizar la administración y gestión de "la herramienta" para el control de las vulnerabilidades y mantener actualizado el inventario de activos gestionados en "la herramienta de gestión de vulnerabilidad a contratar".	NO	Se precisa que el Documento de Condiciones mantiene la exigencia de gestión centralizada del servicio sobre “la solución” entregada como SaaS (Cap. I, 6.1.a), con administración, mantenimiento e integración a múltiples plataformas internas (Cap. I, 6.3.c; Cap. III, 3.4.1, 7) y visualización y reportes unificados (Cap. I, 6.6), sin que ello implique la obligación de un software monolítico: se admite el uso de componentes licenciados especializados siempre que formen parte de la oferta, queden orquestados bajo un único punto de control (dashboards, alertas, reporting, inventario y trazabilidad) y se cumpla que el escaneo de aplicaciones web esté incluido dentro de la misma plataforma a entregar (Cap. III, 3.4.1, 8.b), que los escaneos a demanda se realicen con herramientas licenciadas e integradas (p. ej., Cap. III, 3.4.6, 5) y que el SAST requerido (Cap. I, 6.11; Cap. III, 3.4.6, 9) pueda ejecutarse con motores dedicados cuyos resultados se incorporen al control central y al SIEM (Cap. I, 6.7). En consecuencia, lo habilitante y relevante es la integración funcional y la gestión unificada del servicio conforme a las reglas publicadas, asegurando pluralidad de oferentes sin modificar las condiciones del documento

123	OLIMPIAIT	Las condiciones técnicas y obligatorias mínimas indican una fuerte orientación y requisito de que el proyecto se cumpla mediante una única solución o plataforma tecnológica integrada. Si bien el documento utiliza a menudo el singular ("la solución", "la herramienta"), la condición radica en la exigencia de integración y centralización de todas las capacidades requeridas dentro de una misma oferta licenciada, es decir, la entidad no solo pide una herramienta, sino que exige que las distintas funcionalidades coexistan o se entreguen desde una única estructura central. Recordamos que el objeto contractual definido corresponde a la prestación de un servicio especializado de seguridad informática, y no a la adquisición de una herramienta tecnológica en particular. En ese sentido, conforme al principio de planeación y al principio de pluralidad de oferentes establecidos en la Ley 80 de 1993 y la Ley 1150 de 2007, la entidad no puede condicionar la forma en que el contratista ejecutará dicho servicio, salvo en lo estrictamente necesario para garantizar la finalidad perseguida por el contrato. La exigencia de que todas las funcionalidades se concentren en una sola herramienta tecnológica resulta restrictiva, pues desconoce que en el mercado es usual que la prestación de servicios de ciberseguridad se realice a través de un conjunto de herramientas integradas, que en su conjunto permiten alcanzar la misma finalidad con igual o mayor eficacia. Lo relevante para la entidad debe ser que el servicio contratado garantice gestión centralizada, integración funcional y calidad técnica, independientemente de si se logra mediante una única plataforma o mediante varias herramientas interoperables. Por lo anterior, se solicita a LA PREVISORA S.A. ajustar el requisito, de manera que se exija únicamente que el oferente asegure la entrega del servicio con una gestión unificada por parte del oferente y resultados verificables, sin limitar la arquitectura tecnológica interna, lo cual amplía la concurrencia de oferentes y evita direccionamientos implícitos hacia fabricantes específicos.	NO	precisa que el Documento de Condiciones no exige que todas las capacidades provengan de un único software monolítico; lo que se mantiene es la gestión centralizada del servicio sobre “la solución” entregada como SaaS (Cap. I, 6.1.a), con administración, mantenimiento e integración a múltiples plataformas internas (Cap. I, 6.3.c; Cap. III, 3.4.1, 7) y visualización/reportes unificados (Cap. I, 6.6). En ese sentido, se admite el uso de componentes licenciados especializados siempre que formen parte de la oferta y queden orquestados bajo un único punto de control (dashboards, alertas, inventario, reporting y trazabilidad), cumpliendo que el escaneo de aplicaciones web esté incluido dentro de la misma plataforma a entregar (Cap. III, 3.4.1, 8.b), que los escaneos a demanda se realicen con herramientas licenciadas e integradas (p. ej., Cap. III, 3.4.6, 5) y que el SAST requerido (Cap. I, 6.11; Cap. III, 3.4.6, 9) pueda ejecutarse con motores dedicados cuyos resultados se incorporen al control central y al SIEM (Cap. I, 6.7). De esta forma, lo habilitante y relevante es la integración funcional y la gestión unificada con resultados verificables, asegurando la pluralidad de oferentes en coherencia con el régimen jurídico aplicable (Cap. I, 14), sin ajustar ni modificar las condiciones del documento; la verificación se realizará bajo el criterio CUMPLE/NO CUMPLE previsto.
124	OLIMPIAIT	Revisando el Objeto Principal de la invitación, el cual busca contratar un "servicio especializado de seguridad informática" basado en el "monitoreo continuo y seguimiento en tiempo real de las vulnerabilidades". La naturaleza del contrato es la prestación de un servicio, donde la tecnología subyacente es el medio para lograr un fin. Sin embargo, el Numeral 3.4.1. y otros apartados técnicos imponen la condición de que la prestación de todas las funcionalidades requeridas (monitoreo de IP/HOST, escaneo de servicios web, etc.) deben realizarse mediante una "única plataforma a entregar" o "la herramienta ofrecida" (en singular). La condición de exigir que la totalidad de las prestaciones del servicio (incluyendo escaneo de infraestructura, escaneo web y capacidades de análisis de código SAST) provengan de una única solución monolítica o integrada en la "misma plataforma" restringe la competencia y puede interpretarse como una exigencia que atenta contra el principio de selección objetiva. En un contrato de servicios, la Entidad debe enfocarse en la finalidad del objeto y la calidad del resultado, y no en condicionar al oferente al uso de una arquitectura tecnológica rígida. Los oferentes podríamos cumplir el objeto contractual con la más alta calidad mediante la articulación e integración de soluciones especializadas (por ejemplo, una herramienta de gestión de vulnerabilidades complementada con un motor de análisis de código estático), siempre y cuando la gestión, el monitoreo y los reportes se centralicen y cumplan con los ANS. Se solicita a LA PREVISORA S.A. aclarar que: La prestación del "servicio especializado de seguridad informática" puede llevarse a cabo mediante la integración funcional de diversas soluciones, plataformas o herramientas tecnológicas del oferente, siempre que este garantice la unicidad de la gestión por parte del	NO	se precisa que el Documento de Condiciones no exige que todas las capacidades provengan de un único software monolítico; lo que se mantiene es la gestión centralizada de la prestación del servicio especializado de seguridad informática (Cap. I, 4; Cap. I, 6.1.a), con administración, mantenimiento e integración a múltiples plataformas internas (Cap. I, 6.3.c; Cap. III, 3.4.1, 7) y visualización/reportes unificados (Cap. I, 6.6). En ese marco, se admite la integración funcional de diversas soluciones licenciadas siempre que formen parte de la oferta y queden orquestadas bajo un único punto de control (dashboards, alertas, inventario, reporting y trazabilidad), cumpliendo que el escaneo de aplicaciones web esté incluido dentro de la misma plataforma a entregar (Cap. III, 3.4.1, 8.b), que los escaneos a demanda se efectúen con herramientas licenciadas e integradas (p. ej., Cap. III, 3.4.6, 5) y que el SAST requerido (Cap. I, 6.11; Cap. III, 3.4.6, 9) incorpore sus resultados al control central y al SIEM (Cap. I, 6.7). En consecuencia, lo habilitante y relevante es la integración funcional, la gestión unificada por parte del oferente, la continuidad del servicio y el cumplimiento íntegro de los requisitos técnicos mínimos del Numeral 3.4, bajo verificación CUMPLE/NO CUMPLE, asegurando la pluralidad de oferentes sin modificar las condiciones del documento.

125	OLIMPIAIT	En caso de que la entidad considere necesario definir ciertas características técnicas de las herramientas que espera se utilicen en la prestación del servicio, debe precisarse que ello no puede implicar la exigencia de que una sola herramienta concentre todas las funcionalidades requeridas. Tal exigencia sería contraria al principio de libre concurrencia y podría configurar un direccionamiento hacia soluciones de un fabricante específico, lo cual está expresamente proscrito en el marco normativo de la contratación estatal (artículos 24 y 25 de la Ley 80 de 1993, así como el artículo 5 de la Ley 1150 de 2007). En el mercado de ciberseguridad es común que distintos componentes especializados —por ejemplo, un motor de análisis de vulnerabilidades, una herramienta de escaneo de aplicaciones y un módulo de análisis de código— operen de manera integrada para prestar un servicio robusto, sin que necesariamente provengan de un mismo software monolítico. La finalidad del contrato se logra en la medida en que dichas herramientas se gestionen de forma centralizada e integrada dentro del servicio, independientemente de su origen o fabricante. Por lo anterior, se solicita que el pliego de condiciones precise que lo relevante es la integración funcional del servicio ofrecido y la entrega de resultados consolidados, sin imponer que las capacidades provengan de una sola herramienta. Esta precisión garantiza pluralidad de oferentes y evita un direccionamiento técnico que limite injustificadamente la competencia.	NO	Se precisa que el Documento de Condiciones no exige concentrar todas las capacidades en una sola herramienta; lo habilitante es la integración funcional y la gestión centralizada del servicio SaaS (Cap. I, 4; 6.1.a; 6.3.c; 6.6; Cap. III, 3.4.1.7), admitiéndose diversas soluciones licenciadas del oferente siempre que queden orquestadas bajo un único punto de control y se cumpla: escaneo web incluido en la plataforma (Cap. III, 3.4.1.8.b), escaneos a demanda con herramientas licenciadas e integradas (Cap. III, 3.4.6.5) y SAST con resultados incorporados al control central/SIEM (Cap. I, 6.11; 6.7; Cap. III, 3.4.6.9), conforme a los ANS (Cap. III, 3.6). En consecuencia, lo relevante es la entrega de resultados consolidados, garantizando pluralidad de oferentes y selección objetiva, sin modificar las condiciones del documento.
126	OLIMPIAIT	Revisando el requisito obligatorio mínimo contenido en el Numeral 3.4.1., el cual exige que el licenciamiento de los servicios de escaneo web para 50 aplicaciones esté incluido "dentro de la misma plataforma a entregar" al igual que los análisis de código con el resto de las funcionalidades de gestión de vulnerabilidades. Reconociendo que el Objeto Principal de la invitación es la contratación de un servicio especializado de seguridad informática basado en el monitoreo continuo y la gestión efectiva de amenazas. La Entidad requiere un amplio espectro de servicios, incluyendo: monitoreo continuo de infraestructura, escaneo de vulnerabilidades web (DAST), y análisis de código estático (SAST). La exigencia de que estas funcionalidades altamente especializadas provengan de una única y misma plataforma resulta desproporcionada y restrictiva al principio de selección objetiva y la libre concurrencia, por las siguientes razones: 1. Naturaleza Especializada del Mercado: Las soluciones líderes en el mercado de ciberseguridad avanzada, tales como plataformas especializadas en Vulnerability Management and Remediation y herramientas líderes en Application Security Testing (SAST) y escaneo web dinámico (DAST), a menudo no son desarrolladas por un único fabricante. Los proponentes con el expertise más calificado frecuentemente utilizamos la integración de las mejores herramientas especializadas para cumplir con el alcance total de los requerimientos de la Entidad. 2. Direccionamiento Innecesario: Al imponer la unicidad tecnológica ("misma plataforma a entregar"), la Entidad está indebidamente especificando el medio interno de prestación del servicio, en lugar de centrarse en la finalidad y la calidad del resultado del servicio. Esto limita artificialmente la participación a aquellos fabricantes o integradores que ofrecen una suite monolítica que cumpla con todos los requisitos, a pesar de que la prestación mediante	NO	Se ratifica el requisito del Numeral 3.4.1, literal 8) b) (“escaneo de aplicaciones web incluido dentro de la misma plataforma a entregar”), por lo cual no procede eliminar o modificar dicha frase; sin embargo, se precisa que el Documento no exige un software monolítico: se admite la integración de componentes licenciados especializados siempre que formen parte de la oferta y queden orquestados bajo un único punto de control con gestión centralizada, visualización/reportes unificados y coherencia de la información (Cap. I, 4, 6.1.a, 6.6; Cap. I, 6.7; Cap. III, 3.4.1.7, 3.4.6.5 y 3.4.6.9), cumpliendo los ANS vigentes (Cap. III, 3.6). En consecuencia, lo relevante es la integración funcional y la entrega de resultados consolidados; se garantiza la pluralidad de oferentes y la selección objetiva sin modificar las condiciones del documento.

127	OLIMPIAIT	Agradecemos nos indiquen cuáles son las políticas aplicables al objeto del contrato en relación con el Sistema de Seguridad de la Información implementado por la Entidad.	NO	Se informa que, conforme al Documento de Condiciones Definitivas, el servicio deberá ajustarse a las políticas internas del Sistema de Gestión de Seguridad de la Información (SGSI) de LA PREVISORA S.A., entre ellas: Política del SGSI, Confidencialidad de la Información (Cap. I, 12), Tratamiento y Protección de Datos Personales (Anexo 12), Plan de Continuidad y Recuperación de Desastres (Cap. I, 6.1.d), Reglamento de Conectividad (Minuta, Cláusula 45), Gestión de Incidentes y Reporte al SIEM (Cap. I, 6.7; Cap. III, 3.4.6), así como lineamientos corporativos complementarios (Manual de Contratación; Código de Ética y Línea Ética; SARLAFT). La Entidad también exige observar las directrices de la Superintendencia Financiera (p. ej., Circular 052 de 2007 y CBJ 006-2025) y se reserva la facultad de verificar el cumplimiento de requisitos de seguridad durante la ejecución (Cap. I, 5.5; Minuta, Cláusulas 15–19 y 17 Seguridad de la Información). Estas políticas serán suministradas y/o validadas en el inicio y durante la vigencia del contrato, sin modificación de las condiciones del documento.
128	OLIMPIAIT	La presente obligación resulta demasiado amplia y abierta. Sugerimos que se limite de manera expresa a las actividades relacionadas con la prestación del servicio ofertado y a los entregables definidos en el anexo de especificaciones técnicas, a fin de otorgar mayor claridadsobre los informes y entregables del servicio.	NO	Se precisa que la obligación se circunscribe al objeto contractual (Cap. I, 4), a las obligaciones generales y específicas del servicio (Cap. I, 5 y 6) y a los entregables definidos (Cap. III, 3.5), así como a los informes requeridos para la forma de pago (Cap. II, 5) y al plan de trabajo que aprueba el Supervisor (Cap. I, 10); en consecuencia, su ejecución se limita expresamente a las actividades relacionadas con la prestación del servicio ofertado y a los entregables contenidos en el documento y anexos, manteniendo las condiciones publicadas y la verificación CUMPLE/NO CUMPLE sin modificación del pliego.
129	OLIMPIAIT	Observamos que la redacción actual podría dar lugar a interpretaciones que excedan las especificaciones técnicas contratadas. Solicitamos que se precise que las instrucciones del supervisor deberán limitarse al objeto del contrato y a las condiciones definidas en los pliegos y la propuesta, evitando la generación de obligaciones adicionales no previstas.	NO	Se mantienen las condiciones del documento: las instrucciones del supervisor se circunscriben al objeto del contrato y a las condiciones definidas en los pliegos y en la propuesta y a la ejecución del contrato, el propósito de asegurar el cumplimiento, sin generar obligaciones adicionales ni costos no previstos. Cualquier ajuste de alcance o requisitos solo procederá mediante los trámites formales (adenda y/o modificación contractual), y los entregables e informes siguen siendo los previstos en el documento, bajo verificación CUMPLE/NO CUMPLE.
130	OLIMPIAIT	La presente obligación no guarda relación con el objeto del contrato ni con las actividades propias de su ejecución. En tal sentido, solicitamos se elimine esta obligación, toda vez que resulta ajena al alcance contractual y no corresponde a los entregables ni responsabilidades asociados al servicio contratado.	NO	Agradecemos su observación sin embargo se mantine la misma por tratarse de obligaciones generales para las contrataciones que realiza la previsora, su alcance se definira en la minuta de contrato definitiva que se suscriba con el oferente seleccionado.
131	OLIMPIAIT	Agradecemos aclarar el alcance de la presente obligación.	NO	Agradecemos su observación sin embargo se mantine la misma por tratarse de obligaciones generales para las contrataciones que realiza la previsora, su alcance se definira en la minuta de contrato definitiva que se suscriba con el oferente seleccionado.

132	OLIMPIAIT	Agradecemos nos indiquen cuáles disposiciones de la Circular 052 de 2007 resultan aplicables al objeto del presente contrato.	NO	Para el objeto del contrato, resultan aplicables las disposiciones del Capítulo Décimo Segundo de la Circular Externa 052 de 2007 de la SFC, en particular: (i) los criterios de seguridad y calidad de la información (confidencialidad, integridad, disponibilidad; efectividad, eficiencia, confiabilidad) y sus definiciones (núms. 2.1 y 2.2); (ii) las obligaciones generales de seguridad y calidad (núm. 3.1), incluida la exigencia de cifrado fuerte, autenticación y controles de acceso; (iii) la gestión de tercerización/outsourcing (núm. 3.2) y la documentación/divulgación de medidas y procedimientos (núms. 3.3 y 3.4); (iv) los requerimientos para canales tecnológicos relevantes al servicio, como acceso remoto e Internet (núms. 4.8 y 4.9); (v) las reglas de actualización de software (núm. 5); y (vi) el apartado de análisis de vulnerabilidades (núm. 7), obligatorio para establecimientos de crédito y administradores de sistemas de pago de bajo valor y adoptable por otras entidades vigiladas atendiendo su naturaleza y actividad. La circular también contextualiza etapas y plazos de implementación del capítulo (2008–2010), que enmarcan la obligatoriedad de estos requerimientos. Fuentes: texto del capítulo y alcance en la Circular Básica Jurídica anexa a la CE 052/2007 SFC/CBJ, PDF y guía de aplicación (incluida la delimitación del núm. 7) en compendio institucional Banco de Bogotá, PDF; cronograma y contexto de implementación en el sitio oficial SFC (CE 052/2007).
133	OLIMPIAIT	Agradecemos eliminar o aclarar la presente obligación, toda vez que no se encuentra relacionada al objeto y alcance del servicio.	NO	Agradecemos su observación sin embargo se mantine la misma por tratarse de obligaciones generales para las contrataciones que realiza la previsora, su alcance se definira en la minuta de contrato definitiva que se suscriba con el oferente seleccionado.
134	OLIMPIAIT	Agradecemos aclarar y especificar el procedimiento que tiene la PREVISORA para dicho impuesto.	NO	LA PREVISORA S.A., aplicara lo definido en el numeral 6. Impuestos, Tasas y Contribuciones, para efectos del impuesto del timbre se le llega a ser aplicable se incluira la clausula respectiva en la minuta que se formalizaré con el oferente seleccionado
135	OLIMPIAIT	El plazo dispuesto puede resultar insuficiente en situaciones de fuerza mayor como renuncia, incapacidad prolongada o incluso fallecimiento, entre otras. Solicitamos ampliar este término a treinta (30) días hábiles en dichos casos excepcionales, de manera que se garantice una adecuada gestión del recurso humano sin afectar la continuidad del servicio.	NO	Se mantienen las condiciones del documento: el plazo vigente para sustitución del recurso no se amplía; los eventos de fuerza mayor se gestionan dentro del término mediante plan de contingencia y reemplazo oportuno, sin afectar ANS ni la continuidad del servicio. Cualquier cambio de plazo solo procede vía adenda/modificación contractual.
136	OLIMPIAIT	la redacción actual otorga a la Entidad una facultad amplia para solicitar cambios de personal sin precisar criterios objetivos ni un alcance definido. Solicitamos que se aclare que esta facultad solo podrá ejercerse de manera motivada frente a situaciones debidamente justificadas, relacionadas con el incumplimiento de funciones, falta de idoneidad o situaciones que afecten la adecuada prestación del servicio.	NO	la facultad de la Entidad para solicitar cambios de personal se circunscribe a la adecuada ejecución del servicio y se ejercerá de forma motivada y documentada por el Supervisor, cuando exista evidencia de incumplimiento de funciones, falta de idoneidad/perfil, afectación de ANS o situaciones que impacten la calidad y continuidad del servicio (incluidas las políticas de seguridad y confidencialidad). El reemplazo deberá ser con perfil equivalente o superior, sin suspender el servicio ni generar costos no previstos

137	OLIMPIAIT	Observamos que los porcentajes de penalización establecidos resultan desproporcionados en relación con la naturaleza de los descuentos, cuya finalidad debe ser incentivar el cumplimiento y garantizar la continuidad del servicio. En aplicación de los principios de proporcionalidad y razonabilidad, solicitamos que los porcentajes se ajusten a un rango entre el 1% y el 5%. Respetuosamente solicitamos precisar que el cómputo de los niveles de disponibilidad no deberá incluir eventos atribuibles a terceros o ajenos al control del contratista. En estos casos, la indisponibilidad no puede ser imputada al contratista ni dar lugar a la aplicación de penalidades.	NO	Se mantienen las condiciones del documento: los porcentajes de penalización previstos en el Cap. III (ANS) se aplican sin ajuste; por tanto, no procede limitar el rango al 1%–5%. En cuanto al cómputo de disponibilidad, se realizará conforme a la fórmula y criterios definidos en el documento, excluyendo únicamente los eventos expresamente previstos como fuerza mayor, paradas programadas autorizadas o afectaciones atribuibles a terceros fuera del control del contratista, siempre que estén debidamente soportadas y validadas por el Supervisor. Cualquier modificación de porcentajes o criterios de cómputo solo procede vía adenda/modificación contractual; la verificación se hará bajo CUMPLE/NO CUMPLE.
138	OLIMPIAIT	El plazo dispuesto puede resultar insuficiente en situaciones de fuerza mayor como renuncia, incapacidad prolongada o incluso fallecimiento, entre otras. Solicitamos ampliar este término a treinta (30) días hábiles en dichos casos excepcionales, de manera que se garantice una adecuada gestión del recurso humano sin afectar la continuidad del servicio.	NO	e mantienen las condiciones del documento: no procede ampliar el término a treinta (30) días hábiles. Los eventos de fuerza mayor se gestionan dentro del plazo vigente mediante plan de contingencia, reemplazo oportuno con perfil equivalente o superior y continuidad del servicio sin afectar ANS ni generar costos no previstos. Cualquier ajuste de plazo solo procede vía adenda/modificación contractual.
139	OLIMPIAIT	Respetuosamente solicitamos que las penalidades previstas se ajusten en dos aspectos: (i) que no sean aplicables en (i) que no sean aplicables en circunstancias de fuerza mayor; y (ii) que los porcentajes de descuento se limiten a un máximo del 5%, en consideración a los principios de proporcionalidad y razonabilidad y a la naturaleza de estas medidas, cuya finalidad principal es apremiar el cumplimiento del contrato.	NO	Se mantienen las condiciones del documento: las penalidades/ descuentos por ANS se aplican conforme al Cap. III (ANS), por lo que no procede limitar los porcentajes a un máximo del 5% ni modificar su esquema. En todo caso, el cómputo y la aplicación de penalidades excluyen los eventos expresamente previstos como fuerza mayor, ventanas de mantenimiento autorizadas y afectaciones atribuibles a terceros fuera del control del contratista, siempre que estén debidamente soportadas y validadas por el Supervisor. Cualquier ajuste de rangos o condiciones solo procede mediante adenda/modificación contractual; la verificación se realizará bajo criterio CUMPLE/NO CUMPLE.
140	OLIMPIAIT	Respecto a la posible aplicación acumulativa de descuentos por incumplimientos de los ANS podría generar sanciones excesivas que desborden la finalidad propia de estas medidas, la cual debe orientarse a incentivar el cumplimiento del servicio. En atención a los principios de proporcionalidad y razonabilidad, y a la naturaleza de estas sanciones como mecanismos de apremio, solicitamos que la imposición de descuentos acumulativos se limite hasta un máximo del cinco por ciento (5%) del valor de la factura mensual.	NO	No procede. Se mantienen los ANS y correctivos del documento: disponibilidad con descuentos de 2%, 5% o 10% según el rango, y gestión de personal 1%/3% por día con tope 15% mensual. Fijar un límite adicional del 5% implicaría modificar las condiciones. Fundamento: Cap. I, 6.1 b (disponibilidad 99.5%) y Cap. III, 3.6 ANS (descuentos y tope 15%
141	OLIMPIAIT	Solicitamos amablemente que las causales de terminación sean bilaterales, de manera que tanto la Entidad como el Proveedor puedan invocarlas en caso de presentarse circunstancias que afecten la ejecución del contrato para cualquiera de las partes.	NO	Agradecemos su observación sin embargo se mantine la misma por tratarse de condiciones generales en los contratos suscritos por LA PREVISORA S.A.
142	OLIMPIAIT	Respetuosamente manifestamos que la Cláusula Décima Novena – Protección de Datos Personales no resulta aplicable al objeto del presente contrato. El servicio a contratar corresponde a un servicio especializado de seguridad informática, orientado a la identificación, detección, análisis, monitoreo y seguimiento de vulnerabilidades en activos tecnológicos, aplicaciones, redes y sistemas de información de LA PREVISORA S.A. En el marco de estas actividades, el proveedor no realizará operaciones de tratamiento de datos personales suministrados o transmitidos por LA PREVISORA S.A., como recolección, almacenamiento, circulación o supresión de información de titulares. Por lo anterior, solicitamos que dicha cláusula sea retirada, toda vez que el servicio únicamente se refiere a la gestión de vulnerabilidades.	NO	Agradecemos su observación sin embargo se mantine la misma por tratarse de obligaciones generales para las contrataciones que realiza la previsora, su alcance se definira en la minuta de contrato definitiva que se suscriba con el oferente seleccionado.
143	OLIMPIAIT	Solicitamos amablemente aclarar que obligaciones ambientales considera aplicables al presente servicio.	NO	Gestión de residuos tecnológicos (RAEE), Eficiencia energética, Uso racional de recursos, Compromiso con la economía circular y demás acciones que garanticen la implementación de su Plan de Gestión Ambiental

144	OLIMPIAIT	De manera respetuosa solicitamos que la aplicación de la Cláusula Penal prevista en el contrato, se limite a los casos de incumplimiento grave y total que imposibiliten la ejecución del contrato. Lo anterior en atención a que la finalidad de la cláusula penal debería constituirse en una medida de protección frente a incumplimientos de entidad significativa, y no en una sanción automática frente a cualquier incumplimiento parcial o menor que no afecte la continuidad ni el cumplimiento sustancial del objeto contractual.	NO	Agradecemos su observación sin embargo se mantine la misma por tratarse de condiciones generales en los contratos suscritos por LA PREVISORA S.A.
145	OLIMPIAIT	Solicitamos respetuosamente que se aclare el alcance de la cláusula de propiedad intelectual y cesión de derechos de autor. Lo anterior, teniendo en cuenta que el servicio a contratar se soporta en licenciamiento de terceros, cuya titularidad permanece en cabeza de sus fabricantes, y en herramientas propias del proveedor que no son objeto de cesión. En ese orden, es necesario establecer expresamente que cualquier software, metodología, conocimiento o activo preexistente, ya sea del proveedor o de un tercero, mantiene su titularidad y no puede entenderse como parte de los derechos a transferir.	NO	Agradecemos su observación sin embargo se mantine la misma por tratarse de obligaciones generales para las contrataciones que realiza la previsora, el anexo respectivo es un modelo de contratación, su alcance se definira en la minuta de contrato definitiva que se suscriba con el oferente seleccionado.
146	OLIMPIAIT	Las obligaciones del proveedor incluyen frases como “todas las inherentes”, “todas las necesarias”, “todas las solicitadas por el supervisor”, las cuales son cláusulas con obligaciones indeterminadas y desproporcionadas, pues no limita de manera clara el objeto y alcance del mismo. En tal virtud, se solicita limitar las obligaciones a las definidas en el contrato y anexos técnicos, agregando que cualquier obligación adicional debe estar documentada, ser técnicamente viable y no alterar el equilibrio económico.	NO	Agradecemos su observación sin embargo se mantine la misma por tratarse de obligaciones generales para las contrataciones que realiza la previsora, el anexo respectivo es un modelo de contratación, su alcance se definira en la minuta de contrato definitiva que se suscriba con el oferente seleccionado.
147	OLIMPIAIT	El documento exige que el proveedor responda por todos los daños y perjuicios, sin límite, incluidos daños a terceros y asegurados, responsabilidad ilimitada, ya que los riesgos de ciberseguridad nunca pueden ser 100% mitigados. Se solicitar un límite de responsabilidad, excluyendo: pérdida de reputación, lucro cesante, daños indirectos, fuerza mayor y ataques corporativos externos no atribuibles al proveedor.	NO	Se mantiene la responsabilidad integral del proveedor, sin límites contractuales ni exclusiones, conforme al documento.
148	OLIMPIAIT	Los TDR incluyen: 500 IP/HOST; 50 servicios web; crecimiento del 10% sin incremento de tarifa, esto implica un crecimiento acumulado que puede generar costos no contemplados para el proveedor. Se solicita definitr contractualmente un limite del crecimiento máximo total o que permita renegociar tarifa si aumenta más del 10% anual.	NO	Se mantienen las condiciones: cobertura mínima 500 IP/HOST y 50 servicios web, con crecimiento anual del 10% sin incremento proporcional de tarifa. No se pacta límite adicional ni renegociación de tarifa; una propuesta condicionada en ese sentido sería causal de rechazo. Fundamento: Cap. I, 6.4 (a); Cap. II, 1 “Propuestas parciales y condicionadas”; Cap. IV, 31 (causales 14 – ofertas condicionadas).
149	OLIMPIAIT	El riesgo derivado de cambios normativos, jurisprudenciales o de lineamientos emitidos por entes rectores del Estado no debe ser trasladado al contratista en ningún porcentaje, dado que: Se trata de un riesgo exógeno, cuya causa, materialización y alcance dependen exclusivamente de decisiones del Estado y del ordenamiento jurídico, sin posibilidad real de gestión o control por parte del contratista. La asignación de riesgos debe realizarse bajo criterios de gestión, capacidad de control e influencia, conforme a los principios de selección objetiva y equilibrio económico del contrato. Trasladar al contratista este tipo de riesgo implica una carga excesiva, contraria a la distribución razonable prevista en la normatividad de contratación estatal. Este riesgo, por su naturaleza, debe ser asumido íntegramente por la Entidad, quien es la que tiene capacidad de interpretar, ajustar y adaptar sus procesos al marco regulatorio vigente.Por lo anterior, se recomienda eliminar la participación del contratista en este riesgo y clasificarlo como un riesgo exclusivo de la Entidad.	NO	Se mantiene la asignación de riesgos definida en la Matriz de Riesgos del proceso y en el Documento de Condiciones; excluir o trasladar totalmente el riesgo por cambios normativos implicaría modificar las condiciones y la distribución de riesgos prevista. Una oferta condicionada en ese sentido sería causal de rechazo.

150	OLIMPIAIT	Este riesgo no debe ser trasladado al contratista, en ningún porcentaje, por las siguientes razones: La supervisión y el control de ejecución del contrato son responsabilidades propias, exclusivas e indelegables de la Entidad Estatal, conforme a la normativa de contratación pública. El contratista no tiene competencia, facultad ni capacidad para determinar, sustituir o garantizar la forma en que la Entidad ejerce su supervisión; por tanto, se trata de un riesgo completamente ajeno a su gestión. La adecuada supervisión es un mecanismo de control interno de la Entidad, cuyo incumplimiento puede generar efectos directos sobre la ejecución contractual, pero no es un riesgo atribuible al contratista, quien depende de las instrucciones y validaciones de la supervisión. Trasladar este riesgo al contratista contravendría los principios de equilibrio económico, transparencia y responsabilidad, dado que implicaría exigirle asumir consecuencias derivadas de actuaciones exclusivamente internas de la Entidad. Por lo anterior, se recomienda clasificar este riesgo como un riesgo exclusivo de la Entidad y eliminar cualquier asignación al contratista.	NO	Se mantiene la asignación de riesgos del proceso y el régimen de supervisión previsto en el documento: el proveedor debe acatar y coordinar con el supervisor conforme al objeto contratado. Reclasificarlo como riesgo exclusivo de la Entidad implicaría modificar las condiciones; una oferta condicionada en ese sentido sería causal de rechazo.
151	OLIMPIAIT	Se solicita aclarar a que se refiere con "auditorias de cuentas"	NO	El término “auditorías de cuentas” no está definido ni exigido en el Documento de Condiciones. El alcance contempla actividades técnicas de seguridad (Ethical Hacking, SAST, forense, alertas e integración), no auditorías financieras/contables. Se mantiene el alcance establecido, sin adiciones. Fundamento: Cap. I 6.9, 6.11, 6.15; Cap. III 3.4.5; Cap. IV 1.2.1–1.2.3.
152	OLIMPIAIT	Este riesgo no debe trasladarse al contratista, en ningún porcentaje, por las siguientes razones: La entrega oportuna, completa y veraz de la información necesaria para la ejecución del proyecto es una obligación exclusiva de la Entidad Estatal, como parte de sus deberes de supervisión, coordinación y suministro de insumos esenciales. El contratista no tiene control sobre la disponibilidad, tiempos de gestión interna, validaciones o autorizaciones que la Entidad requiere para entregar dicha información. Por lo tanto, se trata de un riesgo totalmente externo y no gestionable por el contratista. La falta de información oportuna por parte de la Entidad puede afectar directamente el cronograma, la calidad y el cumplimiento contractual, lo cual constituye un evento que activa el principio de equilibrio económico y no puede imputarse al contratista. Atribuir este riesgo al contratista implicaría trasladar consecuencias derivadas de actuaciones internas de la Entidad, contradiciendo los principios de responsabilidad, buena fe, colaboración y distribución objetiva de riesgos. En conclusión, se recomienda mantener este riesgo como responsabilidad exclusiva de la Entidad Estatal y eliminar cualquier porcentaje de asignación al contratista.	NO	Se mantiene la asignación de riesgos del proceso (Cap. I, 15 y Anexo 9 – Matriz de Riesgos). La obligación de LA PREVISORA S.A. de suministrar información oportuna ya está prevista (Cap. I, 7), sin reclasificar el riesgo como exclusivo de la Entidad. Una oferta condicionada en ese sentido sería causal de rechazo (Cap. II, 1; Cap. IV, 31 – causal 14).

153	OLIMPIAIT	Se solicita a la entidad confirmar si el análisis de vulnerabilidades debe cubrir todas las soluciones descritas (servidores, dispositivos Fortinet, periféricos, dispositivos de red y servicios web) o únicamente los sistemas operativos. Adicionalmente, se requiere aclarar si el crecimiento proyectado del 5% anual está incluido dentro de las cantidades mencionados o si debe considerarse como adicional en la propuesta.	NO	Cobertura: El análisis de vulnerabilidades debe cubrir todos los tipos de activos descritos (servidores Windows/Linux, dispositivos Fortinet, periféricos, dispositivos de red y servicios web), además de puertos, servicios/aplicaciones y bases de datos, no solo sistemas operativos. Fundamento: Cap. III, 3.4.1 (listado de activos y licenciamiento mínimo) y 3.4.4 (alcances de escaneo: SO, servicios web, puertos, apps y BD). Crecimiento: Se mantienen ambos parámetros: Licenciamiento: crecimiento 10% anual sin incremento proporcional de tarifa. Inventario estimado de activos: crecimiento 5% anual para dimensionamiento/cobertura técnica. Fundamento: Cap. I, 6.4(a) (10% sin incremento) y Cap. III, 3.4.1 (5% sobre IP/HOST y servicios web).
154	OLIMPIAIT	Se solicita a la entidad confirmar cuáles son los objetivos específicos que se deben cubrir en las pruebas de Ethical Hacking, con el fin de dimensionar adecuadamente el alcance del pentesting, indicando si se requiere evaluar aplicaciones web, infraestructura, redes internas y externas, servicios críticos, así como la profundidad esperada en cada uno de estos componentes. Adicionalmente, precisar en el re-test qué vulnerabilidades deben ser verificadas, por ejemplo, si aplica únicamente para las de criticidad alta y crítica, o también para las de nivel medio o todas las detectadas.	NO	Cobertura integral: aplicaciones web, infraestructura, redes internas/externas y servicios críticos, en caja gris, hasta 10 activos por semestre con OSSTMM/ISSAF/OWASP; pruebas en SO, puertos, servicios/aplicaciones y BD (IPv4/IPv6). Re-test: obligatorio hasta confirmar remediación; se prioriza en vulnerabilidades alta/crítica y puede ampliarse según la priorización de LA PREVISORA. Fundamento: Cap. I 6.9; Cap. III 3.4.1, 3.4.4, 3.4.6
155	OLIMPIAIT	Se solicita a la entidad confirmar si el análisis de código orientado a la detección de vulnerabilidades mediante técnicas SAST, debe realizarse dentro de la misma solución de gestión de vulnerabilidades o si se permite incorporar una herramienta adicional especializada para este fin; igualmente, precisar si las licencias correspondientes a dicha herramienta deben quedar registradas a nombre de la entidad, si se pueden utilizar soluciones open source o deben ser exclusivamente comerciales y licenciadas, y en caso de requerir licenciamiento, indicar el tiempo mínimo de vigencia que debe contemplarse.	NO	Cobertura integral: aplicaciones web, infraestructura, redes internas/externas y servicios críticos, en caja gris, hasta 10 activos por semestre con OSSTMM/ISSAF/OWASP; pruebas en SO, puertos, servicios/aplicaciones y BD (IPv4/IPv6). Re-test: obligatorio hasta confirmar remediación; se prioriza en vulnerabilidades alta/crítica y puede ampliarse según la priorización de LA PREVISORA. Fundamento: Cap. I 6.9; Cap. III 3.4.1, 3.4.4, 3.4.6
156	OLIMPIAIT	De acuerdo al entendieminto se solicita a la entidad confirmar si, dado que el alcance descrito establece que se trata de un servicio especializado para la gestión de vulnerabilidades, incluyendo análisis de código seguro, pruebas de penetración, ethical hacking y acciones de remediación, no es necesario que las licencias queden registradas a nombre de la entidad, considerando que la responsabilidad de la administración y operación recae en el proveedor durante la vigencia del contrato.	NO	Se confirma: no se exige que las licencias queden registradas a nombre de LA PREVISORA S.A.. La solución se entrega como SaaS y el proveedor incluye y administra el licenciamiento durante la vigencia; si se requieren licencias de software base para componentes de despliegue, son costeadas por el proveedor y sujetas a aprobación, sin cambio de titularidad.
157	OLIMPIAIT	Se recomienda a la entidad reconsiderar el requisito que solicita adjuntar certificación expedida por el fabricante, mayorista o representante oficial en Colombia que acredite al oferente como canal autorizado en niveles de membresía, dado que este criterio aplica principalmente para partners que revenden soluciones, pero no garantiza la calidad ni la experiencia en la prestación de servicios especializados de ciberseguridad. En su lugar, se sugiere exigir evidencia de experiencia comprobada en proyectos similares como servicios gestionados, contar con un SOC propio y ser miembro de FIRST u organizaciones equivalentes, lo cual aporta mayor valor y confiabilidad en la ejecución del servicio.	NO	Se mantiene la exigencia de acreditación como canal autorizado por fabricante/mayorista/representante en Colombia, conforme al documento. Este requisito asegura soporte oficial y continuidad del licenciamiento y servicio. La experiencia comprobada ya se exige en Cap. III, 3.1 (máx. tres certificaciones, objeto similar y cuantía), y los aspectos técnicos se evalúan en Cap. IV, 1.2.1–1.2.3. Criterios como SOC propio o membresía FIRST no están previstos; incluirlos implicaría modificar las condiciones.
158	OLIMPIAIT	Se recomienda a la entidadreconsiderar el requisito que exige que la solución esté posicionada como líder en rankings internacionales (Gartner, Forrester Wave, GigaOm Radar o SC MEDIA Awards), ya que esta condición solo favorece a un número muy reducido de soluciones presentes en dichos cuadrantes, restringiendo la participación y reduciendo la competencia. En su lugar, se sugiere establecer criterios basados en cumplimiento técnico, experiencia comprobada en proyectos similares y certificaciones de calidad, lo cual garantiza la idoneidad del servicio sin limitar la oferta a fabricantes específicos.	NO	Se mantiene el requisito de liderazgo en rankings internacionales (Gartner, Forrester Wave, GigaOm Radar o SC MEDIA Awards) como evidencia objetiva e independiente del desempeño de la solución; el documento exige al menos uno de dichos listados, sin restringir a un único fabricante. La experiencia y el cumplimiento técnico ya están previstos y se evalúan en los numerales correspondientes. Modificar este criterio implicaría cambiar las condiciones del proceso.

159	OLIMPIAIT	Observación 1 Documento: "Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf" Tema: “Limitación de Responsabilidad en Infraestructura”. Texto: 6.2. Responsabilidad sobre infraestructura a) Asumir todos los costos de aprovisionamiento […] de la infraestructura requerida en el Datacenter de LA PREVISORA S.A. b) Garantizar y asumir costos de la migración en caso de cambio de proveedor… Esta cláusula es muy favorable para la Entidad, pero jurídicamente puede ser considerada de difícil cumplimiento si no se acota. Exigir al proveedor asumir costos de migración "en caso de cambio de proveedor de Datacenter" (decisión	NO	Se mantienen las obligaciones del numeral 6.2 a–b: el proveedor asume todos los costos de aprovisionamiento y los costos de migración en caso de cambio de proveedor de Datacenter/nube, garantizando la continuidad sin costos para LA PREVISORA. Este lineamiento ya está reiterado en 3.4.1 (Datacenter TRIARA–Claro; costos de espacios/colocation y eventuales migraciones a cargo del proponente). Propuestas que pretendan acotar o condicionar estos costos implican modificar las condiciones y son causal de rechazo.
160	OLIMPIAIT	Observación 2 Documento: ANEXO No. 9 Matriz de riesgos precontractuales contractuales (003).xlsx. Tema: “Insuficiencia en la Tipificación del Riesgo de Fuga de Información (Confidencialidad). Texto: "Riesgos Operacionales: "Demoras en la entrega de la información necesaria…", "Incumplimiento del tiempo y alcance del proyecto…". (Snippet de Matriz)." La matriz de riesgos actual se enfoca excesivamente en el cumplimiento de cronogramas (riesgos típicos de obra o suministro). En un contrato de Gestión de Vulnerabilidades, el riesgo operativo/jurídico más grave no es el retraso, sino la fuga de información (Data Leakage) o el uso indebido de los hallazgos por parte del personal del contratista. El proveedor tendrá acceso a las "llaves del reino" (vulnerabilidades críticas). La matriz actual no parece ponderar este riesgo con la severidad adecuada. Agregar un Riesgo Específico en la etapa Contractual clasificado como: Riesgo: Divulgación no autorizada, copia o uso indebido de la información sobre vulnerabilidades de la Entidad. Consecuencia: Materialización de ciberataques por terceros, daño reputacional severo y sanciones de la SIC/Superfinanciera. Tratamiento: Exigencia de firma de Acuerdos de Confidencialidad (NDA) individuales por cada ingeniero del proveedor, implementación de controles DLP (Data Loss Prevention) en los equipos del proveedor y constitución de pólizas con amparo específico para responsabilidad civil por violación de datos.	NO	Se mantiene la Matriz de Riesgos y el marco contractual vigente, que ya mitiga la fuga de información mediante: confidencialidad (causal de terminación inmediata), seguridad de la información (controles de cifrado, accesos y reporte de incidentes), protección de datos personales y propiedad/entrega/destrucción de la información. La exigencia de ISO/IEC 27001:2022 refuerza estos controles. Incorporar NDA individuales, DLP obligatorios o nuevas pólizas implicaría modificar las condiciones.
161	OLIMPIAIT	Observación 3 Documento: “Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf” Tema: “Criterios de Calificación vs. Requisitos Habilitantes (Servicio Forense).”. Texto: "Ítem 10: "Entrega de información técnica errada al contratista por parte de la Entidad" | Consecuencia: "se retrasa el proyecto" Aunque el riesgo está correctamente asignado a la ADRES, el tratamiento propuesto ("Control de calidad") es preventivo pero no correctivo. Legalmente, si la ADRES entrega información errada que causa retraso, esto no solo implica ajustar el cronograma, sino que podría generar reclamaciones por mayores permanencias (costos administrativos de personal ocioso) por parte del contratista. Agregar en la columna de "Tratamiento" o "Consecuencia" que, ante la materialización de este riesgo, se procederá a la suspensión del plazo o prórroga automática del cronograma por el tiempo equivalente al retraso, para blindar a la entidad de demandas por incumplimiento de plazos que no son culpa del contratista.	NO	Se mantiene la Matriz de Riesgos y el régimen contractual vigente. La gestión de demoras por información errada se atiende mediante los mecanismos contractuales de suspensión/ajuste de cronograma previstos en la Minuta, no por “prórroga automática” en la Matriz. Introducir esa condición modificaría las reglas del proceso.

162	OLIMPIAIT	Observación No. 4 Documento: Proyecto de Pliego de Condiciones Tema: Indeterminación en la remuneración (Pago por horas vs. Pago por producto). Texto: "1.2.1. Se otorgarán 80 puntos al proponente que incluya en su propuesta un servicio especializado de Análisis Forense, el cual deberá garantizar la disponibilidad de personal especializado..." (Página 57).". Desde la óptica de la gestión del riesgo jurídico, existe una inconsistencia. Si el Análisis Forense es necesario para responder a incidentes de seguridad (cuyo impacto legal y reputacional es altísimo), no debería ser un factor opcional que otorga puntos ("calificable"), sino un requisito técnico mínimo ("habilitante"). Al dejarlo como puntaje, la Entidad asume el riesgo de adjudicar el contrato a un proveedor que no tenga capacidad forense, quedando desprotegida ante un incidente real. Reevaluar la matriz de contratación. Si la Entidad considera crítico tener capacidad de respuesta forense ante un incidente, este ítem debe moverse a los Requisitos Técnicos Habilitantes (Obligatorios). Si se mantiene como puntaje, se sugiere incluir una obligación contractual para que, en caso de que el adjudicatario no tenga este servicio in-house, deba demostrar un convenio de respaldo con un tercero para emergencias forenses, sin costo adicional para la entidad.	NO	Se mantiene el servicio forense como factor técnico calificable (80 puntos); la capacidad mínima de respuesta a incidentes ya está cubierta en requisitos obligatorios (plan de gestión de incidentes, EH semestral, SAST, alertas e integración).
163	OLIMPIAIT	Observación No. 5. Documento:Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf Tema: Requisito de que la solución sea “Líder” en rankings (Gartner, Forrester, GigaOm, SC Media) Página: Cap. III (Certificaciones del Proponente): Texto del documento: “confirmación de que la solución… está como Líder en al menos uno de los siguientes rankings: Gartner, Forrester Wave, GigaOm Radar o SC MEDIA Awards.” Observación y Sustento Técnico: Solicitud 1: Agradecemos a la Entidad nos confirme si se acepta que la solución sea Líder o Strong Performer en cualquiera de los listados mencionados o bien que el oferente presente evidencia de evaluación analítica (brief de analista, datasheet y referencias de clientes) en lugar de exclusivamente la posición 'Líder' Solicitud 2: Solicitamos aclarar si se aceptan combinaciones (p. ej. plataforma base no líder + módulo de gestión de vulnerabilidades líder) y documentación que acredite integración y cobertura funcional.	NO	Solicitud 1 (aceptar “Strong Performer” u otras evidencias): No procede. Se mantiene la exigencia de que la solución esté como “Líder” en al menos uno de los rankings indicados, según la versión más reciente y con brochure/datasheet y carta firmada que confirmen el cumplimiento. Alternativas como “Strong Performer” o briefs/ referencias no sustituyen la posición Líder. Fundamento: Cap. III, 3.2 c (liderazgo en rankings y soportes requeridos). Solicitud 2 (combinaciones: plataforma base no líder + módulo líder): No procede. El requisito aplica a la solución propuesta en su conjunto para la gestión de vulnerabilidades; no se aceptan combinaciones que fragmenten liderazgo por módulos si la solución integral no ostenta la posición Líder. Cualquier condicionamiento o re-planteamiento modificaría las condiciones. Fundamento: Cap. III, 3.2 c; Cap. II, 1 (propuestas condicionadas); Cap. IV, 31 (causal 14).
164	OLIMPIAIT	Observación No. 6. Documento: Tema: Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf. Página:Cap. 6.1 / 3.6 ANS Texto del documento: “Garantizar una disponibilidad mínima del 99.5%… penalizaciones: 99.5–99% = 2%; 98.99–98% = 5%; <98% = 10% (descuento sobre factura).” Observación y Sustento Técnico: Solicitud 1: Agradecemos a la Entidad nos confirme el método de cálculo de disponibilidad (fórmula), periodo de medición (mensual o calendario) y si existen ventanas programadas de mantenimiento excluidas (frecuencia, duración máxima por mes y aviso previo requerido). Solicitud 2: Solicitamos aclarar procedimiento de disputa de mediciones (evidencias a aportar) y si existen métricas de disponibilidad por componente (UI, API, escaneos) o sólo disponibilidad global	NO	Solicitud 1 (método, periodo, ventanas): No procede modificar. Se mantiene el esquema de penalización por disponibilidad mínima 99.5%; el periodo de medición es mensual (descuento sobre la factura del mes siguiente). La fórmula de cálculo y las ventanas de mantenimiento (si aplica) se precisarán en el acta de inicio sin cambiar porcentajes ni rangos. Fundamento: Cap. I, 6.1 b; Cap. III, 3.6 ANS. Solicitud 2 (disputa y métricas por componente): No procede modificar. El procedimiento de disputa se atiende con el supervisor, aportando evidencias (logs de monitoreo, reportes de uptime, tickets/mesa de servicio), conforme se defina en el acta de inicio. La disponibilidad exigida aplica a la solución en su conjunto; cualquier detalle por componente (UI, API, escaneos) se usará para seguimiento operativo, sin alterar el esquema de descuentos. Fundamento: Cap. III, 3.6 ANS; Cap. I, 10 (Supervisión).

165	OLIMPIAIT	Observación No. 7. Documento: Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf Tema: Plan de Continuidad y Recuperación de Desastres Página: Cláusula 6.1.d / cláusulas de continuidad Texto del documento: “deberá incluir e implementar PLAN DE CONTINUIDAD Y RECUPERACIÓN DE DESASTRES … PROBADO SEMESTRALEMNTE.” Observación y Sustento Técnico: Solicitud 1: Agradecemos a la Entidad nos confirme el tipo de pruebas exigidas (tabletop, simulacros, failover parcial o completo), el alcance mínimo (componentes incluidos) y si la Entidad coordina ventanas de pruebas o las define el proveedor. Solicitud 2: Solicitamos aclarar los RTO/RPO objetivo exigidos para los ejercicios y si las pruebas semestrales implican penalidades en caso de fallo en la ejecución del plan de PCN o si se requiere solo evidencias y mejoras documentadas.	NO	Tipo y alcance de pruebas: El oferente debe proponer en su PCN/DRP la matriz semestral (tabletop, simulacro, failover parcial/total) que demuestre continuidad de componentes críticos de la solución (plataforma, agentes/escáner, reportes, integración SIEM, cifrado). Las ventanas se coordinan y aprueban con la supervisión del contrato. (Cap. I 6.1.d; Cap. III 3.5.1; Cap. I 10). RTO/RPO: No están fijados en el Documento; el oferente los define y sustenta en su PCN/DRP, alineados con la disponibilidad ≥99,5% exigida. (Cap. III 3.6.2). Penalidades: No hay penalidad independiente por “fallo” de la prueba; aplican las penalidades de disponibilidad si la prueba causa indisponibilidad del servicio. Siempre se deben entregar evidencias y mejoras documentadas. (Cap. III 3.6.2; Cap. III 3.5).
166	OLIMPIAIT	Observación No. 8. Documento: Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf Tema: Cobertura de licenciamiento: 500 IP/HOST y 50 servicios web; crecimiento anual y “Sin incremento proporcional de tarifa Página: Cap. 6.4 / 3.4.2 Texto del documento: “Incluir licencias para al menos 500 IP/HOST y 50 servicios web, con crecimiento anual del 10%/5%. Sin incremento proporcional de tarifa.” Observación y Sustento Técnico: Solicitud 1: Agradecemos a la Entidad nos confirme la definición operativa de 'IP/HOST' (servidor virtualizado, contenedor, IP pública/privada) y cuál fórmula se utilizará para el cómputo mensual/reportado. Solicitud 2: Solicitamos aclarar la discrepancia de crecimiento anual indicada en distintas secciones (10% vs. 5%) y si la Entidad acepta un mecanismo de ajuste en caso de crecimiento excepcional o cambios tecnológicos que incrementen el conteo de activos >15% anual	NO	Definición operativa de IP/HOST y cómputo: Para efectos de licenciamiento, IP/HOST corresponde a cada activo direccionable gestionado por la solución (p. ej., servidores Windows/Linux virtualizados, dispositivos de seguridad Fortinet, periféricos con IP —impresoras, teléfonos—, dispositivos de red —switches HP, WLAN Aruba—), así como servicios web internos/externos del dominio institucional (Cap. III 3.4.1). El cómputo se hará sobre el inventario efectivo gestionado y escaneado en el mes, reportado por el proveedor en los informes (Cap. III 3.5, p. 53–54), y validado por la supervisión (Cap. I 10, p. 14–15). Crecimiento anual (10% vs 5%): Para evaluación y ejecución prevalece lo dispuesto en 6.4.a: crecimiento anual del 10% “sin incremento proporcional de tarifa” en el licenciamiento mínimo (p. 12). La referencia del 5% en 3.4.1 se entiende como parámetro operativo de proyección de activos y no altera el licenciamiento mínimo exigido. Crecimientos excepcionales (>15%): El Documento no prevé un mecanismo automático de ajuste tarifario; rige la condición de “sin incremento proporcional de tarifa” (Cap. I 6.4.a). Si se presenta un crecimiento excepcional o cambio tecnológico que incremente el conteo por encima del 10%, se coordinará con la supervisión dentro del plan de trabajo (Cap. III 3.5.1, p. 53), sin perjuicio de los topes presupuestales y de que cualquier modificación sustancial requiera Adenda (Cap. I 20, p. 17).

167	OLIMPIAIT	Observación No. 9. Documento: Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf. Tema: Pruebas de Ethical Hacking — alcance y número de activos (2 pruebas anuales, hasta 10 activos por prueba). Página: Cap. 6.9 / 3.4.2 Texto del documento: “Realizar dos pruebas de Ethical Hacking (una por semestre), tipo caja gris, sobre hasta 10 activos.” Observación y Sustento Técnico: Solicitud 1: Agradecemos nos confirme la definición de 'activo' para las pruebas (IP, dominio, aplicación, subdominio, endpoint) y el criterio para selección (la compañía selecciona o se acuerda lista conjunta) Solicitud 2: Solicitamos aclarar la política de re-test (plazos, ejemplos de evidencia) y si los retests se consideran dentro de las dos pruebas anuales o se realizan a demanda sin costo adicional	NO	Solicitud 1 (definición de “activo” y selección): Para estas pruebas, “activo” corresponde a cualquier elemento TI direccionable o servicio en alcance (p.ej., servidores Windows/Linux virtualizados, dispositivos de seguridad Fortinet, periféricos con IP —impresoras, teléfonos—, dispositivos de red HP/Aruba, y servicios/aplicaciones web como IIS/Apache Tomcat) según lo descrito en el Documento (Cap. III 3.4.1, p. 50–51; definición de Host, p. 8). La lista de hasta 10 activos por prueba es seleccionada por LA PREVISORA S.A. y se acuerda operativamente en el plan de trabajo con la supervisión (Cap. III 3.4.6.6.a, p. 52–53; Cap. III 3.5.1 Kickoff, p. 53; Cap. I 10, p. 14–15). Solicitud 2 (política de re-test y evidencias): El Documento exige re-test sobre los activos evaluados hasta confirmar remediación (Cap. I 6.9.b, p. 13; Cap. III 3.4.6.6.c, p. 52–53). No fija plazos específicos: los tiempos se acuerdan con la supervisión según el plan de acción. Los re-test no sustituyen las dos pruebas semestrales; se realizan a demanda, con evidencias en los informes técnicos/ejecutivos y el informe de re-test previstos en los Entregables 4–6 (p. 54)
168	OLIMPIAIT	Observación No. 11. Documento: Documento_Condiciones Definitivas_INVAB_0xx-2025V4.pdf Tema: Propiedad intelectual y cesión de código fuente. Riesgo por cláusula amplia. Página: Cláusula cuadragésima séptima/tercera Texto del documento: “La propiedad intelectual de todo material creado… será de propiedad de LA PREVISORA S.A… suscripción del contrato de cesión de derechos será requisito para pago del último sprint.” Observación y Sustento Técnico: Solicitud 1: Agradecemos confirmar si la cláusula de propiedad intelectual distingue entre software desarrollado ex-novo y software preexistente del proveedor, y si se aceptan licencias de uso para componentes preexistentes Solicitud 2: Solicitamos aclarar el mecanismo para la entrega de código fuente (formatos, repositorios, documentación) y si el pago final podrá condicionarse a entrega de documentación técnica en lugar de cesión total de IP de componentes preexistentes	NO	Agradecemos su observación sin embargo se mantine la misma por tratarse de obligaciones generales para las contrataciones que realiza la previsora, el anexo respectivo es un modelo de contratación, su alcance se definira en la minuta de contrato definitiva que se suscriba con el oferente seleccionado.

169	LICITACIONES TIC	OBSERVACIÓN 1. Retiro del requisito de 'dos máximos niveles de membresía' por ser un filtro comercial restrictivo y no necesario: Causa legal/técnica: El requisito impone una jerarquía comercial propia de cada fabricante y ajena al mérito técnico exigible, lo cual afecta la pluralidad de oferentes y la selección objetiva al limitar la concurrencia a canales 'top tier'. El propio pliego ya exige ISO/IEC 2701:2022, perfiles habilitantes, ANS de disponibilidad (99,5%) y penalidades, controles que garantizan idoneidad y continuidad sin necesidad de un 'nivel máximo' de canal. Texto a reemplazar (extracto del pliego): 'Deberá adjuntar con su propuesta la certificación expedida por el fabricante, mayorista o representante oficial en Colombia, que lo acredite como canal autorizado en cualquiera de los dos máximos niveles de membresía, con una vigencia no mayor a dos (2) meses.' Propuesta de reemplazo: 'Carta de respaldo del fabricante o del distribuidor oficial que garantice suministro legítimo, acceso a parches/actualizaciones y soporte; acreditación vigente como partner autorizado sin limitar a niveles máximos; en consorcios/UT, la acreditación podrá aportarla el miembro responsable del componente técnico.' Argumento de la solicitud: Desde la perspectiva legal, el filtro comercial desproporcionado vulnera los principios de igualdad y pluralidad que informan el procedimiento de invitación abierta, pudiendo configurar direccionamiento. Desde la técnica, la entrega de parches y soporte se garantiza por contrato y por respaldo del fabricante, no por el 'tier'. Las obligaciones de seguridad y continuidad están consagradas en los ANS y en las penalidades de la minuta; establecer niveles máximos no añade garantías jurídicas ni técnicas adicionales, pero sí restringe el mercado.	NO	El requisito se mantiene en los términos previstos: "Certificación expedida por el fabricante, mayorista o representante oficial en Colombia que acredite al oferente como canal autorizado en cualquiera de los dos máximos niveles de membresía, con vigencia no mayor a dos (2) meses" (Cap. III 3.2.b). Justificación técnica y jurídica (proporcionalidad al objeto): El objeto contractual es de alta criticidad (gestión integral de vulnerabilidades, parches, hardening, pruebas EH, integración con SIEM); por ello se exige capacidad de escalamiento directo con el fabricante (soporte L3/L4, acceso prioritario a parches/actualizaciones y tratamiento de vulnerabilidades día cero) que no se garantiza únicamente con ISO/IEC 27001, ANS y penalidades. (Cap. I 6.3.b, 6.7, 6.9; Cap. III 3.4.1–3.4.6). La exigencia de "dos máximos niveles" es una condición habilitante técnica, general y objetiva, no direcciona a un fabricante específico y no restringe la participación de quienes acrediten dichos niveles en Colombia; es idónea y necesaria para mitigar riesgos operativos de suministro y continuidad (coherente con la referencia a CBJ 006-2025 en Cap. I 6.3.d, p. 12). El proceso se rige por derecho privado y selección objetiva conforme al Documento; cualquier modificación del requisito solo procede por Adenda (Cap. I 14 y 20). Sobre la propuesta de reemplazo planteada por el observante: No es procedente sustituir el requisito por una "carta de respaldo general" sin nivel de membresía. Se mantiene el literal de Cap. III 3.2.b. En caso de oferentes plurales (consorcio/UT), la acreditación deberá recaer en el integrante responsable del componente técnico, conforme al documento de constitución, sin alterar el requisito habilitante.
170	LICITACIONES TIC	OBSERVACIÓN 2. Modulación de la 'vigencia máxima de dos meses' de la acreditación (actualidad razonable sin afectar concurrencia) La exigencia de una vigencia de dos (2) meses resulta excesivamente rígida y puede excluir proveedores con acreditaciones válidas que por ciclos administrativos del fabricante tengan emisión superior a dos meses, sin que ello implique pérdida de validez. El control de actualidad puede satisfacerse con verificación directa al fabricante o mayorista y con el contrato de soporte adjunto, evitando sacrificar pluralidad. *Texto a reemplazar (extracto del pliego):* '…con una vigencia no mayor a dos (2) meses.' Propuesta de reemplazo: 'Acreditación vigente del fabricante o verificación documental emitida por el fabricante/mayorista dentro de los últimos seis (6) meses, o certificación de soporte activa; en su defecto, confirmación electrónica del fabricante durante la etapa de verificación.' Argumento de la solicitud: Legalmente, el estándar de 'actualidad razonable' debe armonizarse con la realidad del mercado para no transformar un control de vigencia en una barrera de entrada. Técnicamente, la continuidad del soporte y la legitimidad del licenciamiento se acreditan por contratos activos y cartas del fabricante, no por una ventana temporal rígida de dos meses.'	NO	se ratifica la vigencia máxima de 2 meses para la certificación de canal autorizado en dos niveles máximos.

171	LICITACIONES TIC	OBSERVACIÓN 3. Protección de la pluralidad y selección objetiva frente a jerarquías comerciales heterogéneas Los 'niveles máximos' de membresía son conceptos no estandarizados: cada fabricante los define con criterios propios, por lo que su comparación entre oferentes y su relación con la calidad es discutible. Impulsar un criterio heterogéneo como habilitante puede generar ventaja indebida y limitar la participación de integradores con respaldo oficial pero sin 'top tier'. Texto a reemplazar Exigencia de 'dos máximos niveles de membresía' como habilitante. *Propuesta de reemplazo:* 'Aceptar respaldo oficial del fabricante/distribuidor y evidencia de soporte/actualizaciones (SLA, plan de parches) como criterios habilitantes objetivos, sin jerarquías comerciales.' Argumento de la solicitud: Legalmente, la selección objetiva reclama criterios verificables y comparables; las jerarquías comerciales no aseguran mayor seguridad ni mejor prestación. Técnicamente, los riesgos operativos se mitigan por la arquitectura, cifrado, integración, SAST/EH y ANS, todos ya exigidos en el pliego; el 'nivel máximo' no es un control de seguridad, sino un emblema comercial.	NO	El objeto contratado exige escalamiento directo con fabricante (L3/L4) y acceso prioritario a parches/actualizaciones y atención a vulnerabilidades día cero, condiciones que no se garantizan con una carta genérica sin nivel. (Cap. I 6.3, 6.7, 6.9; Cap. III 3.4.1–3.4.6) El criterio es general y objetivo (no señala fabricante específico) y busca mitigar riesgos de continuidad y suministro propios del servicio de alta criticidad. El proceso se rige por derecho privado y la selección objetiva conforme al Documento.
172	LICITACIONES TIC	OBSERVACIÓN 4. Claridad para proponentes plurales (consorcios/UT) y complementariedad técnica Causa: El pliego contempla la participación plural, pero no precisa expresamente que las certificaciones y respaldos puedan ser aportados por el integrante que ejecuta el componente técnico, lo cual desalienta la asociación y restringe el aprovechamiento de capacidades complementarias. Propuesta de reemplazo: Página 3 'En proponente plural (consorcio/UT), las certificaciones y respaldos requeridos podrán ser aportados por el miembro que ejecuta el alcance técnico relacionado; la verificación se realizará sobre el conjunto de la oferta y la matriz de responsabilidades.' Argumento de la solicitud (enfoque legal y técnico): Desde el plano legal, esta precisión protege la pluralidad y evita barreras indirectas; en lo técnico, favorece la suficiencia del equipo sin relajar controles de soporte ni seguridad establecidos en ANS/minuta.	NO	se acepta la complementariedad técnica en consorcios/UT para aportar las certificaciones/respaldos desde el miembro técnico, manteniendo íntegras las condiciones del requisito (nivel de membresía y vigencia) y la verificación sobre el conjunto de la oferta.
173	LICITACIONES TIC	OBSERVACIÓN 5. Solicitud de Adenda: sustitución del criterio comercial por controles de licenciamiento y soporte verificables: Para blindar el proceso frente a riesgos operativos (licencias ilegítimas, falta de parches/soporte), se propone reemplazar el 'nivel máximo' por una combinación de controles objetivos: (i) carta de respaldo del fabricante; (ii) contrato de soporte activo; (iii) plan de gestión de parches y actualizaciones; (iv) verificación documental durante evaluación; (v) penalidades específicas por incumplimiento de soporte y seguridad ya previstas. Propuesta de reemplazo: 'Incluir en Adenda el paquete de controles (i–v) como habilitantes/obligatorios, eliminando la exigencia de jerarquía comercial.' Legalmente, se privilegian criterios objetivos y no discriminatorios alineados con selección objetiva; técnicamente, se fortalecen garantías directas de seguridad y continuidad sin restringir la participación. Conclusión y petición: Solicitamos la expedición de Adenda que elimine la exigencia de 'dos máximos niveles de membresía' y module la vigencia de la acreditación, sustituyéndolas por controles objetivos de licenciamiento y soporte que no restrinjan la concurrencia, y que se precise la aportación de certificaciones en consorcios/UT. Soporte	NO	No se procede con la solicitud de Adenda para eliminar la exigencia de "dos máximos niveles de membresía" ni para ampliar la vigencia de la certificación. El requisito permanece conforme al Cap. III, 3.2.b y se verifica de acuerdo con el Cap. I, 27. En consorcios/UT, las certificaciones y respaldos pueden ser aportados por el miembro técnico responsable, manteniendo la verificación sobre el conjunto de la oferta (Cap. I 1.1.5; Cap. III 3.2.b

174	ACTIVOS TI	1 Solicitud de supresión total del requisito de certificación ISO/IEC 27001:2022 El pliego establece que el proponente debe contar con certificación ISO/IEC 27001:2022 “en cumplimiento de la Circular Básica Jurídica 006 de 2025 de la Superintendencia Financiera de Colombia”. Sin embargo, tras revisar íntegramente dicha Circular, se evidencia que su contenido se limita a la depuración y reorganización formal de la CBJ, sin introducir nuevos requisitos en materia de seguridad de la información, y particularmente sin imponer la certificación ISO 27001 a proveedores o terceros. En consecuencia, la fundamentación normativa utilizada en el pliego no corresponde al contenido real de la regulación y configura una motivación inexacta del requisito. Si bien valoramos la importancia técnica del estándar ISO 27001, su exigencia no deriva de una obligación regulatoria y solo podría responder a una decisión interna de la Entidad. Mantenerlo como requisito habilitante basado en una norma que no lo contempla afecta los principios de selección objetiva, proporcionalidad y libre concurrencia, al introducir una barrera de acceso no prevista por el marco regulatorio aplicable. Por lo anterior, solicitamos la SUPRESIÓN TOTAL del requisito de certificación ISO/IEC 27001:2022, dado que no encuentra soporte jurídico en la Circular 006 ni en las disposiciones vigentes de la Superintendencia Financiera, y su imposición podría restringir injustificadamente la participación de oferentes idóneos. La verificación de los controles de seguridad puede efectuarse mediante los mecanismos previstos en la regulación (políticas, controles, procedimientos y evidencias), sin imponer una certificación no exigida por la norma.	NO	La Circular Básica Jurídica 006/2025 no impone por sí sola la certificación, pero el marco específico de CE 005/2019 (nube) y los lineamientos de seguridad Taxonomía Única de Incidentes Cibernéticos/Finanzas Abiertas justifican y exigen contar con ISO/IEC 27001 para proveedores en este tipo de servicios. Por lo anterior, se niega la supresión solicitada y se ratifica el requisito habilitante.
175	ACTIVOS TI	2 Solicitud de ampliación del límite de máximo tres (3) certificaciones de experiencia El numeral 3.1 del pliego establece que el proponente únicamente podrá aportar máximo tres (3) certificaciones de experiencia, evaluándose solo las tres primeras foliadas. Esta restricción resulta desproporcionada frente a la exigencia de acreditar experiencia equivalente al 100% del presupuesto oficial, cuyo valor asciende a $1.403 millones. En servicios especializados como la gestión de vulnerabilidades y la seguridad de la información, la experiencia suele estar distribuida en múltiples contratos de diferentes cuantías. Limitarla a solo tres certificaciones impide reflejar adecuadamente la trayectoria real del proponente y afecta de manera directa la valoración objetiva de las capacidades técnicas del oferente. Adicionalmente, esta restricción afecta los principios de selección objetiva, proporcionalidad y libre concurrencia, dado que excluye injustificadamente a oferentes que podrían demostrar la idoneidad requerida mediante la sumatoria de varios contratos. Por ello, solicitamos modificar el requisito para permitir un número mayor de certificaciones —sugerimos un mínimo de seis (6). Esta modificación incrementa la pluralidad de oferentes, fortalece la competencia y garantiza una selección más objetiva y ajustada a la naturaleza técnica del objeto contractual.	NO	No se procede a ampliar el número máximo de certificaciones de experiencia. Se mantiene el límite de tres (3), conforme al Cap. III 3.1. El pliego dispone mecanismos de actualización por SMMLV, consolidación de contratos con adiciones y sumatoria ponderada en consorcios/UT, que permiten acreditar el 100% del presupuesto exigido.
176	TI INFORMATICA	Qué expectativas tienen sobre cifrado (TLS, FIPS)?	NO	que el cifrado propuesto cumpla lo exigido por el Documento (cifrado en tránsito y en reposo, sin afectación de ANS) y que cualquier mención a TLS o FIPS esté soportada por evidencias técnicas del oferente, manteniendo íntegras las condiciones del pliego.

177	TI INFORMATICA	¿Qué RTO/RPO y plan de contingencia esperan?	NO	RTO/RPO: El oferente debe definir y sustentar valores por componente de la solución (consola, motor de escaneo, agentes, repositorios e integraciones), alineados al ANS de disponibilidad ≥ 99,5%. (Cap. I 6.1.d; Cap. III 3.6.2) Pruebas del PCN/DRP: Semestrales (tabletop/simulacro/failover parcial o total), con evidencias de resultados, hallazgos y mejoras. (Cap. I 6.1.d; Cap. III 3.5 / Entregables) Penalidades: No hay penalidad separada por "fallo" de prueba; aplican las de disponibilidad si la prueba afecta el ANS mensual. (Cap. III 3.6.2) Ventanas: El proveedor propone y LA PREVISORA S.A. aprueba/coordina las ventanas en Kickoff para no afectar operación. (Cap. III 3.5.1; Cap. I 10) Contenido mínimo del plan: Roles y escalamiento, criterios de activación, arquitectura de continuidad/recuperación (sitio alterno, backups, verificación), runbooks de failover/fallback, cronograma y re-tests hasta remediación. (Cap. I 6.1.d; Cap. III 3.5)
178	TI INFORMATICA	¿Habilitan los cuatro métodos: pasivo, activo no autenticado, activo autenticado y agente?	NO	Sí. El Documento habilita la cobertura mediante los cuatro enfoques, conforme a las capacidades exigidas de descubrimiento y escaneo de la solución: Pasivo: a través de la integración con el SIEM institucional para correlación/alertamiento. (Cap. I 6.7.b; Cap. III 3.4.5.3) Activo no autenticado: escaneos de red y servicios sin credenciales para descubrimiento y evaluación inicial. (Cap. III 3.4.1) Activo autenticado: escaneos con credenciales/APIs para profundidad en configuración y parches. (Cap. III 3.4.1) Agente: uso de agentes/sondas en host cuando aplique, según el alcance y la arquitectura ofertada. (Cap. III 3.4.1)
179	TI INFORMATICA	¿La plataforma debe orquestar parches y acciones de mitigación?	NO	Sí. La plataforma debe gestionar y orquestar la remediación de vulnerabilidades mediante parches, hardening y acciones de mitigación, directamente o integrándose con herramientas de parcheo/ITSM, con trazabilidad y evidencias en los entregables y re-test hasta confirmar cierre, sin afectar los ANS de disponibilidad.
180	TI INFORMATICA	¿Qué límites de cambio y ventanas de mantenimiento aplican?	NO	los mantenimientos y pruebas se ejecutan en ventanas aprobadas, con reversión y evidencias, sin afectar el ANS ni los entregables.
181	TI INFORMATICA	¿Qué herramienta ITSM usan para integrar tickets?	NO	La plataforma ITSM es Aranda
182	TI INFORMATICA	¿Cómo gestionan actas de aceptación de riesgo?	NO	Cuándo aplica: cuando la vulnerabilidad no puede corregirse de inmediato; se definen controles compensatorios y se documenta la aceptación formal. (Cap. I 10; Cap. III 3.5) Flujo: identificación (CVE/activo/severidad) → plan de mitigación y runbook → acta firmada (responsable + supervisión) → ticket en Aranda y seguimiento en informes; re-test hasta confirmar eficacia. (Cap. III 3.5) Condiciones: la aceptación no exime del ANS ≥ 99,5%; si los controles o pruebas causan indisponibilidad, aplican penalidades por disponibilidad. (Cap. III 3.6.2) Contenido mínimo del acta: CVE/activo, riesgo inherente/residual, controles, plazo y criterios de éxito, vigencia y eventos de revisión, firmas y ID de ticket Aranda.

183	TI INFORMATICA	¿Confirman capacitación anual para 20 personas?	NO	Sí, se confirma. De conformidad con el Documento, el proveedor debe impartir capacitación anual para 20 personas (roles técnico y operativo), programada y aprobada en el plan de trabajo (Kickoff), con materiales, registro de asistencia y evidencia en los entregables. Cualquier ajuste que modifique esta condición solo procede por Adenda.
184	TI INFORMATICA	¿Qué SLA esperan para incidentes críticos (presencial vs. remoto)?	NO	Se mantienen los SLA establecidos en el documento; si un oferente propone tiempos de llegada presencial más estrictos, lo podrá realizar pero no modifica las condiciones mínimas del servicio.
185	TI INFORMATICA	¿Soporte en español, 8x5 o 24x7?	NO	Español + 24×7 para críticos; 8×5 para la operación diaria y acompañamiento.
186	TI INFORMATICA	¿Integración con EDR, WAF, NAC, MDM, SSO/MFA?	NO	Se mantienen las condiciones: integración obligatoria con SIEM y capacidad de integración con otras plataformas de seguridad sin especificar marcas ni protocolos en el pliego. Si un oferente aporta integraciones concretas (EDR/WAF/NAC/MDM/SSO-MFA), se valorará dentro del factor técnico sin alterar requisitos habilitantes.
187	TI INFORMATICA	¿Cumplimiento normativo (ISO 27001, PCI DSS, SARLAFT, Ley 1581)?	NO	Se mantienen las condiciones: ISO 27001, SARLAFT y Ley 1581 como exigencias; PCI DSS no es requisito del pliego (opcional como valor agregado).
188	TI INFORMATICA	¿Qué KPIs son clave (MTTR, % remediación, backlog)?	NO	KPIs se reportan mensualmente conforme a los entregables y dashboards definidos en el pliego; el documento no fija metas numéricas (límites) — se mantienen las condiciones. Si un oferente propone metas más estrictas (p. ej., MTTR por críticos ≤ N días), puede considerarse valor agregado sin modificar el documento.
189	TI INFORMATICA	¿Cadencia de informes (semanal, mensual, trimestral)?	NO	Se mantiene la cadencia definida: semanal / mensual / trimestral / semestral / a demanda, conforme a los Entregables del capítulo III. Semanal: Seguimientos (actas, correos o reportes breves del estado de vulnerabilidades y su gestión). Referencia: Cap. III, 3.5(8). Mensual: Informe mensual con gráficas por criticidad, backlog, planes de acción y nivel de riesgo (ISO 27005). Referencia: Cap. III, 3.5(3 a–f). Trimestral: Informe trimestral de seguimiento de vulnerabilidades internas. Referencia: Cap. III, 3.5(7). Semestral: Informes de Ethical Hacking (técnico y ejecutivo). Referencia: Cap. III, 3.5(4–5). A demanda: Informes de re-test para confirmar remediación de hallazgos. Referencia: Cap. III, 3.5(6). Cierre del contrato: Plan de empalme e informe final 60 días antes de terminar. Referencia: Cap. III, 3.5(10).

190	TI INFORMATICA	¿Audiencias (CISO, auditoría, tecnología)?	NO	1) CISO / Comité de Seguridad: Dashboard ejecutivo global y informe mensual con KPIs (criticidad, backlog, planes de acción y nivel de riesgo ISO 27005). Informe ejecutivo semestral de Ethical Hacking. Actas de aceptación de riesgo cuando aplique. 2) Auditoría (interna/externa) Informe trimestral de seguimiento de vulnerabilidades internas. Evidencias: informes técnicos de EH y re-tests; base de conocimiento y trazabilidad de tratamiento. Soportes de confidencialidad y protección de datos cuando corresponda. 3) Tecnología (Infraestructura / SOC / Desarrollo / Arquitectura) Seguimiento semanal (actas/correos/estado de gestión). Informe técnico mensual con detalle por activo, referencias CVE, planes de remediación y tiempos; inventario actualizado. Resultados SAST, integración con SIEM (Elastic) y alertas; evidencia de descubrimiento y cobertura de escaneo. Distribución y canales La supervisión (Subgerente y Especialista de Infraestructura y Servicios TI) define la distribución y puede solicitar ajustes y entregas a cada audiencia. Referencia: Cap. I 10 (supervisión). Correspondencia formal por los canales establecidos. Referencia: Cap. I 13 (correspondencia). Idioma: español para gestión y reportes. Referencia: Cap. III 3.4.3
191	TI INFORMATICA	¿Retención de datos y residencia (país/región)?	NO	Se mantienen las condiciones del documento: retención/entrega/destrucción según contrato (con plazo 15 días tras la terminación) y sin imposición de residencia geográfica para SaaS, siempre bajo cifrado, confidencialidad y cumplimiento de Ley 1581; en componentes locales, el datacenter es TRIARA y los costos/migraciones los asume el proveedor
192	TI INFORMATICA	¿Requieren hardening documentado por tecnología?	NO	Se mantiene: el hardening debe estar documentado en los informes y la base de conocimiento; el formato específico lo presenta cada oferente en español (con referencias a hallazgo/activo/acción/responsable/fecha), sin modificar las condiciones del pliego.
193	TI INFORMATICA	¿Control de acceso y cadena de custodia en pruebas?	NO	Se mantienen las condiciones del documento: control de acceso conforme a roles, autenticación única y reglamento de conectividad; cadena de custodia aplicada en el servicio forense y en la trazabilidad de entrega/devolución de información. Si un oferente propone formatos/protocolos adicionales de cadena de custodia, se considerará valor agregado sin modificar el pliego.
194	SOSNET	ITEM 1 – Certificación para Gestión de Incidentes de Seguridad De manera comedida solicitamos a la Entidad evaluar la inclusión de un requisito orientado a robustecer la capacidad del proveedor para gestionar incidentes de seguridad de la información, asegurando la aplicación de marcos internacionales reconocidos. Proponemos exigir que: “El oferente cuente con procedimientos estructurados y operativos para la gestión integral de incidentes, respaldados por certificación vigente en una norma internacional de Gestión de Incidentes de Seguridad de la Información. La certificación debe evidenciar las prácticas de preparación, detección, análisis, respuesta y retroalimentación, en armonía con el MSPI del MinTIC. Se deberá adjuntar copia emitida por el organismo certificador al oferente.” Esta medida permitirá mitigar riesgos operacionales y mejorar la capacidad de respuesta ante escenarios críticos.	NO	Se mantienen las condiciones del documento sin incluir una certificación adicional en gestión de incidentes (p. ej., normas específicas como ISO/IEC 27035). El oferente puede presentar sus procedimientos estructurados y cualquier certificación complementaria como valor agregado dentro de su propuesta técnica, sin cambiar los requisitos habilitantes ni los factores de evaluación

195	SOSNET	ITEM 2 – Aclaración del requisito de experiencia Solicitamos respetuosamente que se precise el alcance del numeral 3.1 respecto a las actividades que se consideran válidas para acreditar la experiencia habilitante. Proponemos confirmar una interpretación amplia que considere suficiente la ejecución de una o varias de las actividades relacionadas con la gestión de vulnerabilidades Esto permitirá garantizar la participación de oferentes idóneos, evitando interpretaciones restrictivas.	NO	1) Alcance y modelo de prestación El objeto exige una solución de gestión integral de vulnerabilidades que incluya hardening, pruebas de EH/pentesting, SAST y acompañamiento para tratamiento de hallazgos. Cap. I, 4; 6.9; 6.11; 6.10(b). La solución se entrega en modelo SaaS, integrándose con las plataformas internas; el cifrado extremo a extremo es obligatorio (en tránsito y reposo). Cap. III, 3.4.1(1–7); Cap. I, 6.3(b–c). 2) Integraciones y seguridad Integración obligatoria con el SIEM (Elastic) y capacidad de integrarse con otras plataformas tecnológicas de la entidad. Cap. I, 6.7(b); Cap. III, 3.4.1(7); 3.4.5. Políticas de acceso y roles (lectura/escritura) en español; autenticación única y personalizada; prohibición de claves compartidas. Cap. III, 3.4.3; Minuta, Cl. 17. 3) Soporte y ANS Críticos: soporte 24×7 y atención prioritaria ≤ 2 horas hábiles según el plan de gestión de incidentes. Cap. I, 6.1(e); 6.10(c); Cap. III, 3.6(1). Penalizaciones por disponibilidad (<99.5%) según ANS definidos. Cap. III, 3.6(2). 4) Cadencia de informes y evidencias Semanal: seguimientos del estado de vulnerabilidades. Cap. III, 3.5(8). Mensual: informe con gráficas, backlog, planes de acción y nivel de riesgo (ISO 27005). Cap. III, 3.5(3 a–f). Trimestral: seguimiento interno de vulnerabilidades. Cap. III, 3.5(7). Semestral: informes técnico y ejecutivo de Ethical Hacking y re-tests
196	SOSNET	ITEM 3 – Certificación en Continuidad del Negocio Con el propósito de asegurar la continuidad operativa de los servicios contratados, sugerimos incorporar un requisito que exija: “Que el oferente cuente con un Sistema de Gestión de la Continuidad del Negocio certificado bajo norma internacional vigente aplicable a SGCN, para los procesos de seguridad y mesa de servicio. La oferta deberá incluir copia de la certificación emitida directamente al oferente.” Esta garantía resulta crucial para la estabilidad del servicio frente a eventos disruptivos.	NO	Se mantienen las condiciones actuales (PCN/DRP obligatorio y verificado). Cualquier certificación en SGCN (p. ej., ISO 22301) podrá presentarse como valor agregado dentro de la propuesta, sin convertirse en requisito habilitante ni modificarse el pliego.
197	SOSNET	ITEM 4 – Ajuste sobre certificación de canal autorizado Solicitamos modificar el numeral 3.2.b para que únicamente se requiera la certificación vigente que acredite al oferente como partner autorizado del fabricante o representante oficial, sin restringirlo a los más altos niveles de membresía. Con ello se evita limitar la concurrencia y se mantiene la validez técnica del respaldo del fabricante.	NO	Se mantienen las condiciones del numeral 3.2(b): dos máximos niveles de canal autorizado, certificación vigente y emitida por el fabricante/mayorista/representante oficial. La propuesta de restringir el requisito a “partner autorizado sin nivel” no procede.
198	SOSNET	ITEM 5 – Certificación en Seguridad para Servicios Cloud Con base en que los servicios a contratar se ejecutarán en entornos de nube, proponemos exigir que: “El oferente cuente con certificación vigente en una norma internacional de seguridad para servicios en la nube, que contemple controles de protección de datos, control de accesos, responsabilidad compartida, segregación lógica y monitoreo de recursos. La certificación deberá ser emitida directamente al oferente y adjuntarse a la oferta.” Ello permite asegurar la adecuada gestión de riesgos inherentes a la operación cloud.	NO	1.Se mantienen las condiciones del documento: seguridad SaaS con cifrado, gobierno de datos, integración con SIEM, ANS y continuidad, respaldadas por ISO 27001. 2.Certificaciones cloud adicionales (p. ej., ISO/IEC 27017, ISO/IEC 27018, CSA-STAR) pueden presentarse como valor agregado dentro de la oferta, sin convertirse en requisito habilitante ni modificar el pliego

199	IO SERVICES	ITEM 1 – Experiencia del Proponente Respetuosamente solicitamos a la Entidad precisar el alcance del requisito habilitante de experiencia establecido en el numeral 3.1, particularmente frente a la interpretación del objeto, alcance y obligaciones de los contratos que pueden ser presentados para acreditarla. El pliego define la experiencia similar como actividades relacionadas con análisis y/o implementación de soluciones de gestión de vulnerabilidades, dentro de las cuales se incluyen Ethical Hacking, pruebas de penetración, Security Hardening, revisión de código seguro, análisis de amenazas, simulacros de respuesta a incidentes y parcheo de vulnerabilidades. Para garantizar la adecuada aplicación de los principios de proporcionalidad, concurrencia y selección objetiva, solicitamos confirmar que dicha experiencia podrá validarse bajo una lectura amplia y no restrictiva, aceptando contratos cuyo objeto contemple una o varias de estas actividades, así: "Que el objeto, alcance y/o obligaciones del servicio sean iguales o similares al de la presente invitación. Se entenderá como similar toda actividad relativa al análisis y/o implementación de soluciones para la gestión de vulnerabilidades, tales como: pruebas de Ethical Hacking y/o pruebas de penetración y/o Security Hardening y/o revisión de código seguro y/o análisis de amenazas y/o simulacros de respuesta a incidentes y/o parcheo de vulnerabilidades." Esta precisión garantiza la participación plural de oferentes con experiencia pertinente sin exigir la ejecución simultánea de todas las actividades descritas.	NO	Conforme al numeral 3.1 del documento, la experiencia similar se entiende en sentido amplio, como análisis y/o implementación de soluciones para la gestión de vulnerabilidades, incluyendo —sin limitarse a—: Ethical Hacking, pruebas de penetración, Security Hardening, revisión de código seguro (SAST), análisis de amenazas, simulacros de respuesta a incidentes y parcheo de vulnerabilidades. En ese marco, sí procede confirmar que la experiencia podrá acreditarse con contratos cuyo objeto contemple una o varias de dichas actividades; no se exige su ejecución simultánea. Se mantienen las condiciones del pliego.
200	IO SERVICES	ITEM 2 – Certificación del Oferente como canal autorizado Solicitamos respetuosamente modificar lo previsto en el numeral 3.2, literal b, de manera que únicamente se exija aportar una certificación vigente que acredite al oferente como partner autorizado de la solución propuesta, emitida directamente por el fabricante o su representante en Colombia. La restricción a los máximos niveles de membresía podría limitar la libre concurrencia y la pluralidad de oferentes, razón por la cual la acreditación general como canal autorizado garantiza el respaldo del fabricante sin restringir injustificadamente la participación.	NO	El requisito habilitante previsto en el numeral 3.2(b) establece que el oferente debe acreditarse como canal autorizado en cualquiera de los dos máximos niveles de membresía, mediante certificación vigente emitida por el fabricante, mayorista o representante oficial en Colombia. En ese sentido, no procede la modificación solicitada y se mantienen las condiciones del pliego.
201	IO SERVICES	ITEM 3 – Sistema de Gestión de Continuidad del Negocio Solicitamos considerar la incorporación de un requerimiento adicional que garantice la resiliencia operativa y la continuidad del servicio ante incidentes o fallas de carácter disruptivo. Proponemos incluir: "El oferente deberá contar con un sistema formal de gestión de continuidad del negocio certificado en una norma internacional vigente aplicable a los SGCN, para los procesos asociados a seguridad y mesa de servicios. Con la propuesta deberá adjuntarse copia de la certificación emitida por el organismo certificador directamente al oferente." Esta incorporación asegurará que los servicios críticos permanezcan operativos bajo eventos de riesgo, conforme a las mejores prácticas internacionales.	NO	El documento ya exige continuidad operativa y contingencias sin requerir una certificación adicional de SGCN (p. ej., ISO 22301). En consecuencia, no procede modificar las condiciones del pliego.
202	IO SERVICES	ITEM 4 – Gestión de Incidentes de Seguridad de la Información Con el fin de fortalecer las capacidades del proveedor en la atención y tratamiento de incidentes de seguridad, solicitamos incluir el siguiente requisito técnico: "El oferente deberá contar con procedimientos formales, documentados y operativos para la gestión de incidentes de seguridad de la información, soportados en una certificación vigente en una norma internacional de Gestión de Incidentes de Seguridad de la Información. La certificación deberá demostrar el cumplimiento de estándares aplicables a las fases de preparación, detección, evaluación, respuesta y aprendizaje, en coherencia con el MSPI del MinTIC. Se deberá anexar copia de dicha certificación emitida por el ente certificador al oferente." Esto garantiza que la respuesta a incidentes se realice bajo un marco estructurado y alineado con los lineamientos del sector público.	NO	El documento ya exige capacidades y evidencias suficientes para la gestión integral de incidentes sin requerir una certificación adicional específica (p. ej., ISO/IEC 27035). En consecuencia, no procede modificar las condiciones del pliego

203	IO SERVICES	ITEM 5 – Seguridad en servicios Cloud Solicitamos incluir un requerimiento técnico adicional para asegurar que los servicios en la nube ofrecidos cumplan estándares internacionales de protección de información en entornos cloud. Proponemos exigir: “El oferente deberá contar con certificación vigente en una norma internacional de seguridad para servicios en la nube, que cubra aspectos como protección de datos, responsabilidad compartida, control de accesos, segregación lógica y monitoreo de entornos virtualizados. La certificación deberá ser emitida directamente al oferente por el ente certificador y anexada a la propuesta.” Dicha medida permitirá garantizar la seguridad, confiabilidad y continuidad operativa de los servicios en entornos de nube.	NO	El documento ya establece controles y obligaciones de seguridad para la operación en modelo SaaS y en entornos de nube, sin requerir una certificación cloud adicional específica (p. ej., ISO/IEC 27017, ISO/IEC 27018 o CSA-STAR). En consecuencia, no procede modificar las condiciones del pliego.
204	IO SERVICES	ITEM 6 – INDICADORES FINANCIEROS De manera respetuosa, solicitamos a la Entidad revisar y ajustar los indicadores financieros actualmente exigidos en el proceso, los cuales se encuentran establecidos así: •Nivel de Endeudamiento (Pasivo Total/Activo Total): Menor o igual al 75%. •Índice de Liquidez (Activo Corriente/Pasivo Corriente): Mayor o igual a 1.2. Sin embargo, con el fin de fortalecer la capacidad financiera de los futuros contratistas y asegurar una adecuada estabilidad económica durante la ejecución contractual, solicitamos que estos parámetros sean reemplazados por los siguientes: •Endeudamiento: Menor o igual al 62%. •Liquidez: Mayor o igual a 1.5. La modificación propuesta establece umbrales más estrictos que permiten garantizar que los oferentes cuenten con una estructura financiera más sólida, reduciendo riesgos asociados a problemas de solvencia o falta de respaldo económico en el desarrollo del objeto contractual. Esto contribuye a la adecuada gestión del riesgo financiero por parte de la Entidad y favorece la selección de proponentes con mayor estabilidad y capacidad de cumplimiento.	NO	La capacidad financiera definida por Previsora se fundamenta en un estudio de mercado realizado conforme al objeto del contrato. Este análisis consideró variables como el valor, duración, complejidad y forma de pago del contrato, con el objetivo de asegurar que el proveedor cuente con la liquidez y solidez necesarias para su adecuada ejecución. Para establecer los indicadores financieros requeridos, se tuvo en cuenta lo estipulado en el documento de condiciones, especialmente en lo relacionado con la forma de pago y el plazo de ejecución. Los proponentes deben demostrar una capacidad financiera mínima que les permita cumplir con las actividades previstas durante la ejecución contractual. En este sentido, se definieron indicadores que permiten evaluar la idoneidad financiera de los proponentes, considerando dimensiones como el capital de trabajo, nivel de endeudamiento, patrimonio e índice de liquidez. Estos indicadores, en conjunto, permiten verificar la solvencia necesaria para garantizar el cumplimiento del objeto contractual. Teniendo en cuenta lo anterior, y dado que los indicadores solicitados responden a las necesidades específicas de Previsora, se mantiene la definición de capacidad financiera establecida.