

DE DICTAMEN TÉCNICO.
(Art 40 inc a) Res DNCP N° 230/25)

Lugar y fecha: 28/08/2026

UOC Convocante (*): SECRETARIA NACIONAL DE ADMINISTRACION DE BIENES INCAUTADOS Y COMISADOS

Unidad o área requirente (*): DIRECCION DE TECNOLOGIA DE LA INFMACION Y COMUNICACION

Funcionario o técnico responsable (*): DAVID FERNANDO DUARTE BRIZUELA

Dependencia y cargo que desempeña (*): DIRECCION DE TECNOLOGIA DE LA INFMACION Y COMUNICACIÓN – DIRECTOR TIC

- Justificación técnica que respalda la objetividad, imparcialidad, regularidad y la razonabilidad o proporcionalidad de los requerimientos técnicos solicitados (*).

La presente contratación tiene por objeto dotar a la SENABICO de una solución integral de respaldo, administración, monitoreo y protección de la infraestructura tecnológica institucional. El alcance comprende una Solución de Respaldo, una Solución de Controlador de Dominio, herramientas de Monitoreo de Red y de Aplicaciones, Gestión de Activos de TI y una Herramienta de Antimalware XDR para 70 endpoints. Estos componentes responden a funciones complementarias y críticas: asegurar la disponibilidad y recuperación de la información, centralizar la autenticación y administración de usuarios, obtener visibilidad continua del estado de la infraestructura y de las aplicaciones, mantener inventario y trazabilidad de activos, y detectar y responder oportunamente ante amenazas de seguridad. En consecuencia, las especificaciones no constituyen requerimientos aislados, sino controles técnicos orientados a continuidad operativa, seguridad, administración y trazabilidad de los servicios TIC.

Las especificaciones de la Solución de Respaldo se consideran razonables por cuanto contemplan protección de cargas de trabajo locales, híbridas y multicloud; soporte para plataformas de virtualización, sistemas operativos, bases de datos, NAS y servicios en nube; creación de respaldos con reconocimiento de aplicaciones; replicación con cifrado; integración mediante APIs; instalación, configuración y transferencia tecnológica; y vigencia de tres años con actualizaciones y soporte del fabricante. Estas capacidades permiten que la institución disponga de mecanismos de copia, recuperación y restauración aplicables a entornos heterogéneos, reduciendo el riesgo de pérdida de información, indisponibilidad prolongada o imposibilidad de recuperación ante fallas, errores operativos, incidentes de seguridad o contingencias.

La incorporación del Controlador de Dominio mediante licencias de servidor y licencias de acceso de usuario se fundamenta en la necesidad de disponer de una plataforma actualizada para autenticación, administración centralizada de identidades, políticas, recursos y servicios institucionales. Su licenciamiento permite regularizar el acceso de los usuarios autorizados y mantener una infraestructura soportada, segura y escalable. De manera complementaria, las herramientas de monitoreo de red y aplicaciones permiten supervisar disponibilidad, rendimiento, tráfico, enlaces, configuraciones, vulnerabilidades de firmware, direcciones IP, puertos de switches, logs de firewall, servidores, bases de datos, servicios web, virtualización y experiencia de usuario, con dashboards, alertas, reportes, análisis histórico y automatización. Tales capacidades son proporcionales a la necesidad de anticipar fallas, identificar causas raíz, administrar capacidad y disminuir tiempos de indisponibilidad.

La Gestión de Activos de TI se justifica por la necesidad de contar con un repositorio centralizado para inventario, descubrimiento, clasificación y seguimiento de activos y licencias, incluyendo CMDB, relaciones entre elementos de configuración, contratos, proveedores, garantías y procesos asociados. La Herramienta de Antimalware XDR para 70 endpoints resulta necesaria para centralizar la detección, investigación y respuesta frente a actividades sospechosas, realizar caza de amenazas, aplicar acciones de contención y disponer de integración mediante APIs. La posibilidad de integración futura con soluciones de seguridad de la misma marca se orienta a obtener visibilidad correlacionada y respuesta coordinada frente a amenazas, disminuyendo la fragmentación operativa de los controles de ciberseguridad.

- Identificar y justificar de forma expresa si algún requerimiento podría limitar la participación de potenciales oferentes.

“NO APLICA”

- Si en las bases licitatorias se indica una marca específica u otro derecho intelectual exclusivo, mencionar la justificación que respalda lo solicitado o que no existe otro modo de identificarlo. Se aclara que, en caso de incluirlos, los mismos tendrán carácter referencial.

El PBC contiene referencias a productos, plataformas y tecnologías identificables por marca o derecho intelectual, entre ellas Windows Server 2025, Microsoft Hyper-V, y otras denominaciones utilizadas en las matrices técnicas. Estas menciones deben interpretarse conforme a su finalidad técnica y al carácter referencial que corresponda, salvo aquellos componentes de licenciamiento que respondan a infraestructura institucional existente y cuya continuidad tecnológica sea necesaria.

En el caso de Windows Server 2025 Standard y sus User CAL, la referencia se encuentra vinculada al controlador de dominio y al esquema de licenciamiento requerido para usuarios institucionales, por lo que su identificación responde a compatibilidad, continuidad de administración, autenticación y regularización de acceso a servicios de servidor. En las herramientas de monitoreo, las referencias a fabricantes, hipervisores, bases de datos, sistemas operativos, protocolos o plataformas se utilizan principalmente para definir compatibilidad e interoperabilidad y no deben entenderse como exigencia de adquisición de esas marcas, salvo que el PBC disponga expresamente lo contrario.

La mención a integración con ManageEngine ServiceDesk Plus y la exigencia de integración futura de la solución XDR con plataformas de seguridad de la misma marca se justifican por necesidades de interoperabilidad, correlación y administración unificada. No obstante, toda referencia marcaría incluida para identificar una tecnología, ecosistema o compatibilidad deberá aplicarse con carácter referencial cuando exista otro modo técnicamente equivalente de satisfacer la funcionalidad requerida, preservando el principio de concurrencia sin sacrificar la integración necesaria para la operación institucional.

- Fundamentar criterios de evaluación y/o condiciones de ejecución contractual sugeridos (*).

La adjudicación POR EL TOTAL se fundamenta en que los seis componentes forman parte de una arquitectura funcional integrada de continuidad, monitoreo, administración y seguridad. Un único adjudicatario facilita la coordinación de la implementación, evita incompatibilidades entre herramientas, unifica la responsabilidad por la puesta en marcha, permite gestionar integraciones y escalamiento sin dispersión contractual y reduce controversias sobre la causa de incidentes entre múltiples proveedores. Esta modalidad resulta especialmente razonable cuando existen dependencias entre respaldo, identidades, monitoreo, activos y protección de endpoints.

La Planilla de Especificaciones Técnicas, los catálogos y anexos técnicos se requieren para comprobar de manera documental que las soluciones ofertadas cumplen las funcionalidades mínimas. La autorización del fabricante, las certificaciones y los documentos del plantel técnico constituyen medios de verificación de autenticidad, especialización y capacidad efectiva de soporte. La aceptación de documentación técnica en inglés y/o castellano es coherente con la naturaleza del mercado TIC y evita restricciones innecesarias derivadas de traducciones de documentación oficial de fabricante.

Las condiciones de instalación, configuración, puesta en funcionamiento y coordinación mediante cronograma se justifican porque la sola provisión de licencias no satisface el objeto institucional: las herramientas deben quedar operativas, parametrizadas e integradas en el entorno de SENABICO. La capacitación mínima de 10 horas para dos funcionarios busca transferir conocimiento suficiente para administración básica, operación, generación de reportes, seguimiento de alertas y utilización de las capacidades adquiridas, reduciendo dependencia operativa del proveedor.

La obligación de confidencialidad se considera esencial debido a que durante la implementación y soporte el proveedor podrá acceder a información sobre usuarios, configuraciones, direccionamiento, vulnerabilidades, respaldos, activos, logs y eventos de seguridad. Por ello, las tareas deben ejecutarse preservando reserva, integridad y confidencialidad, en coherencia con la certificación de gestión de seguridad exigida.

El Acuerdo de Nivel de Servicio se fundamenta en la criticidad de las funciones cubiertas. La matriz establece para S1 una respuesta máxima de 1 hora y restablecimiento de 8 horas; para S2, 2 horas y 16 horas; para S3, 3 horas y 3 días; y para S4, 4 horas y 5 días. Los incidentes S1 y S2 reciben atención 24x7 porque pueden comprometer respaldos, autenticación, visibilidad de infraestructura o protección XDR, mientras que S3 y S4 admiten plazos mayores por presentar impacto parcial o bajo. Los tiempos de respuesta, restablecimiento, escalamiento, documentación del incidente, medidas de contingencia y cierre con conformidad permiten medir objetivamente la calidad del soporte y establecer responsabilidades verificables durante la ejecución.

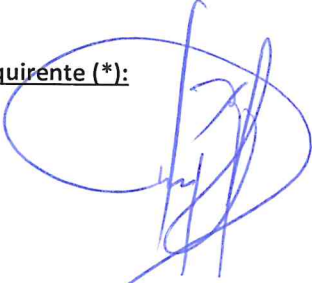
El plazo máximo de 60 días calendario desde el día siguiente de la Orden de Compra para entrega, instalación y puesta en funcionamiento se considera razonable frente al alcance, pues comprende provisión de licencias, coordinación, configuración, integración, pruebas y capacitación. La vigencia de 36 meses para las soluciones de respaldo y monitoreo, y la vigencia prevista para la solución antimalware, responden a la necesidad de asegurar continuidad de actualizaciones, soporte y operación durante un horizonte suficiente para amortizar la implementación y mantener la plataforma protegida y soportada.

Obs.:

En caso de citar o remitirse al análisis o argumentos contenidos en otra documentación, se debe adjuntar la misma al presente dictamen.

Podrán formar parte de los argumentos técnicos de este dictamen, el análisis previo citado en el artículo 25 de la Ley N° 7021/22, los resultados de dicho análisis o los documentos que lo integran.

Firma del técnico o responsable del área requirente (*):



Aclaración (*): DAVID FERNANDO DUARTE BRIZUELA

Dependencia y cargo que desempeña (*): DIRECCIÓN DE TECNOLOGIA DE LA INFMACION Y COMUNICACIÓN – DIRECTOR TIC