

Consultas Realizadas

Licitación 484364 - ADQUISICIÓN DE LICENCIA PARA EL SERVICIO DE MONITOREO DE VULNERABILIDADES - PLURIANUAL - AD REFERENDUM

Consulta 1 - Cantidad y tipo de activos

Consulta	Fecha de Consulta	15-09-2026
Favor indicar la cantidad total aproximada de activos que deberán ser licenciados y evaluados por la solución durante la vigencia del contrato, detallando en lo posible la distribución entre estaciones de trabajo, notebooks, servidores físicos y/o virtuales, dispositivos de red, appliances y otros activos.		

Consulta 2 - Plantillas preconfiguradas

Consulta	Fecha de Consulta	15-09-2026
Respecto al requisito de "Al menos 400 plantillas listas para usar en diferentes escenarios de escaneo", favor aclarar si se considerarán equivalentes las políticas, perfiles, controles, firmas, plugins, configuraciones o plantillas predefinidas provistas por la solución, siempre que permitan cubrir los distintos escenarios técnicos requeridos.		

Consulta 3 - Arquitectura de implementación

Consulta	Fecha de Consulta	15-09-2026
Respecto a las expresiones "Despliegue del software en infraestructura local de la CSJ" y "Configuración del servidor de administración", favor aclarar si se requiere que la totalidad de la plataforma, incluyendo consola de administración y almacenamiento de datos, se encuentre alojada dentro de la infraestructura de la CSJ, o si se admite una arquitectura SaaS/Cloud con agentes, scanners o appliances instalados localmente. Asimismo, favor indicar si se requiere alta disponibilidad o redundancia de dichos componentes.		

Consulta 4 - Detección de malware

Consulta	Fecha de Consulta	15-09-2026
Respecto al requisito de "Detección de software malicioso conocido", favor aclarar si se requiere detección directa de archivos o procesos maliciosos en los equipos, o si se considera suficiente la identificación de vulnerabilidades, indicadores y exposiciones asociadas a malware conocido dentro del proceso de gestión de vulnerabilidades.		

Consulta 5 - Integraciones requeridas

Consulta	Fecha de Consulta	15-09-2026
Considerando que las EETT requieren "Integración con la infraestructura existente de la CSJ", favor especificar las plataformas o sistemas con los cuales se espera integración, tales como Active Directory, SIEM, SOC, sistemas de tickets u otras herramientas.		

Consulta 6 - Escaneos autenticados

Consulta	Fecha de Consulta	15-09-2026
Favor confirmar si la infraestructura permitirá la realización de escaneos autenticados mediante credenciales o mecanismos equivalentes para la evaluación de vulnerabilidades, parches faltantes y configuraciones de los sistemas operativos y dispositivos.		

Consulta 7 - Uso de agentes

Consulta	Fecha de Consulta	15-09-2026
Considerando que las EETT establecen "Configuración de agentes en estaciones de trabajo (si aplica)", favor confirmar si se admite el uso de agentes instalados en endpoints y servidores como complemento al escaneo de red y, en caso afirmativo, indicar la cantidad aproximada de equipos en los cuales se prevé su instalación.		

Consulta 8 - Activos internos, externos y ubicación

Consulta	Fecha de Consulta	15-09-2026
Favor indicar la cantidad aproximada de activos internos y de direcciones IP públicas que deberán ser objeto de escaneo, así como si los mismos se encuentran concentrados en una única sede o distribuidos entre distintas sedes, circunscripciones judiciales, centros de datos o redes independientes.		

Consulta 9 - Frecuencia y ventana de escaneo

Consulta	Fecha de Consulta	15-09-2026
Favor indicar la periodicidad mínima esperada para los análisis de vulnerabilidades y si existe alguna ventana horaria determinada dentro de la cual deban completarse los escaneos.		

Consulta 10 - Aplicaciones web, nube y contenedores

Consulta	Fecha de Consulta	15-09-2026
Respecto al requisito de "Identificación de fallas en aplicaciones y sistemas", favor aclarar si el alcance contempla análisis dinámico de aplicaciones web publicadas. Asimismo, favor indicar si deberán ser evaluados activos alojados en nube pública o privada, contenedores, imágenes de contenedores o plataformas de orquestación.		

Consulta 11 - Alcance de CIS Benchmarks

Consulta	Fecha de Consulta	15-09-2026
Respecto al requerimiento de auditoría basada en CIS Benchmarks, favor indicar si dicha evaluación deberá realizarse sobre la totalidad de los activos licenciados o solamente sobre determinados sistemas o dispositivos, indicando en lo posible las principales plataformas involucradas, tales como Windows, Linux, VMware, dispositivos de red, bases de datos u otras.		

Consulta 12 - Segmentación y conectividad de red

Consulta	Fecha de Consulta	15-09-2026
En caso de existir múltiples sedes o redes, favor indicar aproximadamente la cantidad de segmentos, VLAN, subredes o zonas independientes que deberán ser alcanzadas por la solución, así como si existe conectividad entre ellas que permita realizar los escaneos desde componentes centralizados.		

Consulta 13 - Especificaciones Técnicas de la Solución — Capacidades de Escaneo — "Plantillas preconfiguradas"

Consulta	Fecha de Consulta	16-09-2026
Texto / Exigencia Actual:		
"Al menos 400 plantillas listas para usar en diferentes escenarios de escaneo."		
Consulta / Observación / Petición Concreta:		
El umbral de "al menos 400 plantillas preconfiguradas" coincide de manera no casual con la cifra comercial publicada por el fabricante Tenable para su línea Nessus/Tenable Vulnerability Management, que declara públicamente contar con "más de 450 plantillas preconfiguradas" (fuente: ficha técnica oficial del fabricante). El umbral fijado en el pliego se encuentra ubicado inmediatamente por debajo de dicha cifra específica, patrón que evidencia que la especificación técnica fue construida a partir del catálogo de un único proveedor, en abierta contradicción con los Principios de Igualdad, Libre Concurrencia y Transparencia que rigen las contrataciones públicas. Exigimos a la Entidad Convocante fundamento técnico y objetivamente por qué se requiere esa cantidad específica de plantillas para el objeto de la contratación (264 activos de TI) y no una cifra menor igualmente idónea, y en su defecto, solicitamos la eliminación del umbral numérico o su sustitución por un criterio funcional (cobertura demostrable de los ocho tipos de activos listados en el pliego), admitiéndose expresamente como equivalentes soluciones de otros fabricantes reconocidos del mercado (ej. Qualys VMDR, Rapid7 InsightVM) que cumplan dicha cobertura funcional con un número distinto de plantillas.		

Consulta 14 - Especificaciones Técnicas de la Solución — Priorización y Análisis de Riesgos

Consulta	Fecha de Consulta	16-09-2026
Texto / Exigencia Actual:		
"Mecanismos de priorización basados en: CVSS v3.1 o superior; EPSS; Indicadores propietarios de riesgo del fabricante."		
Consulta / Observación / Petición Concreta:		
La estructura de este requisito —exigir simultáneamente CVSS, EPSS y un "indicador propietario de riesgo del fabricante" como tercer componente independiente— reproduce de manera prácticamente literal la descripción comercial que el fabricante Tenable utiliza para promocionar su motor VPR (Vulnerability Priority Rating), presentado siempre junto a CVSS y EPSS como su triada de priorización característica. Otros fabricantes líderes del mercado, como Qualys (TruRisk/QVS) o Rapid7 (Real Risk Score), estructuran sus mecanismos de priorización de forma distinta, sin presentar un "tercer indicador paralelo" en esos mismos términos, por lo que la redacción actual restringe injustificadamente la participación de soluciones técnicamente equivalentes que cumplen la misma función de priorización de riesgo con arquitecturas propias distintas. En consecuencia, exigimos que la Entidad Convocante modifique la redacción del requisito, sustituyendo la exigencia por: "Mecanismo de priorización que combine, como mínimo, CVSS v3.1 o superior y EPSS, pudiendo incorporar adicionalmente cualquier score, indicador o algoritmo propietario de riesgo desarrollado por el propio fabricante de la solución ofertada, cualquiera sea su denominación comercial o metodología", de forma que no se favorezca a un fabricante en particular por sobre otros que ofrecen igual funcionalidad de priorización de riesgo.		

Consulta 15 - Especificaciones Técnicas de la Solución — Capacidades de Escaneo — "Cobertura de CVEs"

Consulta	Fecha de Consulta	16-09-2026
Texto / Exigencia Actual: "Capacidad de detectar al menos 100.000 vulnerabilidades conocidas contra estándar internacional (CVE)." Consulta / Observación / Petición Concreta: Si bien este umbral es alcanzado por más de un fabricante del mercado (Tenable y Qualys, entre otros), su inclusión conjunta con los requisitos observados en las Consultas N.º 1 y N.º 2 —ambos calzados de manera específica a la ficha comercial de Tenable— refuerza el patrón de direccionamiento del EETT en su conjunto. Solicitamos que la Entidad Convocante confirme expresamente que el cumplimiento de este ítem podrá acreditarse mediante declaración jurada o documentación oficial de cualquier fabricante reconocido internacionalmente en el rubro de gestión de vulnerabilidades, sin restricción a un proveedor en particular, y que la sumatoria de fuentes propias más integraciones de terceros (feeds CVE/NVD) será considerada válida a los efectos de acreditar la cobertura mínima exigida.		

Consulta 16 - Implementación Inicial — Obligaciones del Proveedor

Consulta	Fecha de Consulta	16-09-2026
Texto / Exigencia Actual: "La empresa adjudicada deberá proveer todos los elementos necesarios para la puesta a punto de la solución de software estable actual incluyendo, pero no limitándose a: (...) Integración con la infraestructura existente de la CSJ." Consulta / Observación / Petición Concreta: El presente numeral impone al adjudicatario la obligación de "integrar" la solución con "la infraestructura existente de la CSJ" sin especificar el alcance técnico de dicha integración ni identificar los sistemas concretos con los que deberá interoperar. Esta indeterminación genera una obligación de alcance indefinido que impide a los oferentes dimensionar correctamente el esfuerzo técnico, los recursos y, en consecuencia, el precio de su oferta, en contravención del Principio de Economía y de la exigencia de que las bases de la contratación contengan especificaciones claras, precisas y no ambiguas. En consecuencia, solicitamos a la Entidad Convocante precise expresamente: Qué sistemas o plataformas específicas componen "la infraestructura existente de la CSJ" con los que se exige integración (a modo enunciativo: directorio activo/LDAP para autenticación de usuarios, SIEM institucional, plataforma de mesa de ayuda/ticketing, sistema de gestión de activos —CMDB—, plataformas de virtualización, correo corporativo, u otros). Qué tipo de integración se exige en cada caso (ej. autenticación federada SSO/SAML, sincronización LDAP/Active Directory, envío de alertas vía API/Syslog/webhook a un SIEM, exportación automatizada de reportes a un repositorio determinado), dado que cada modalidad implica desarrollo, licenciamiento y horas de implementación distintos. Si dichas integraciones específicas deben considerarse incluidas dentro de la implementación inicial sin costo adicional, o si —al no estar predefinidas— quedan comprendidas dentro del banco de 270 horas de soporte técnico especializado, conforme lo previsto en el numeral correspondiente. De no precisarse este punto, solicitamos la eliminación de la frase abierta "incluyendo, pero no limitándose a", sustituyéndola por un listado taxativo y cerrado de integraciones exigidas, a fin de garantizar condiciones de igualdad, previsibilidad y comparabilidad entre las ofertas, evitando que la indeterminación del alcance se traduzca en un riesgo económico y contractual desproporcionado para el adjudicatario y en una fuente de eventuales controversias durante la ejecución contractual.		

Consulta 17 - Implementación Inicial — Obligaciones del Proveedor

Consulta	Fecha de Consulta	16-09-2026
Texto / Exigencia Actual: "(...) incluyendo, pero no limitándose a: Instaladores y manuales (...); Configuración del servidor de administración; Configuración de agentes en estaciones de trabajo (si aplica); Definición de políticas de escaneo personalizadas; Integración con la infraestructura existente de la CSJ." Consulta / Observación / Petición Concreta: La locución "incluyendo, pero no limitándose a" que encabeza la totalidad del listado de obligaciones del proveedor introduce una cláusula de alcance abierto e indeterminado, que permite a la Convocante exigir, durante la ejecución contractual, prestaciones adicionales no previstas ni presupuestadas al momento de la oferta, sin mecanismo de ajuste de precio ni de plazo. Ello vulnera el Principio de Economía y el equilibrio contractual que debe primar entre las partes. Solicitamos a la Entidad Convocante confirme que el listado de obligaciones del proveedor bajo el rubro "Implementación Inicial" es taxativo y cerrado, o en su defecto, elimine la expresión "pero no limitándose a", de modo que las obligaciones del adjudicatario queden circunscriptas exclusivamente a las tareas expresamente enumeradas en el pliego, garantizando así previsibilidad presupuestaria y trato igualitario entre los oferentes al momento de estructurar sus ofertas técnicas y económicas.		

Consulta 18 - Especificaciones Técnicas de la Solución — Funcionalidades de Detección — "Malware"

Consulta	Fecha de Consulta	16-09-2026
Texto / Exigencia Actual: "Malware — Detección de software malicioso conocido." Consulta / Observación / Petición Concreta: La detección de malware no constituye una función nativa y estándar de las plataformas de escaneo y gestión de vulnerabilidades (VM), sino una capacidad propia de soluciones de tipo EDR/Antivirus/EPP, que en las herramientas de vulnerability management suele ofrecerse —cuando existe— como un módulo adicional, complementario o de licenciamiento separado, y con alcances metodológicos muy distintos entre fabricantes (detección de indicadores de compromiso mediante escaneo credenciado de archivos/hashes conocidos, versus motores de detección en tiempo real propios de un antivirus). La redacción actual del requisito, al no precisar el alcance ni la metodología exigida, genera ambigüedad sobre el nivel de cumplimiento esperado y puede favorecer indebidamente a aquellos fabricantes cuya plataforma de VM incluye de forma nativa un módulo de detección de malware, en desmedro de otras soluciones igualmente idóneas para el objeto principal de la contratación (descubrimiento y evaluación de vulnerabilidades). En consecuencia, solicitamos a la Entidad Convocante: Precisar el alcance técnico exigido para "detección de software malicioso conocido": si se refiere a la identificación de indicadores de compromiso (IOCs), hashes de archivos maliciosos conocidos o binarios/procesos sospechosos detectados durante el escaneo credenciado del activo, o si se exige una capacidad de motor antivirus/antimalware en tiempo real equiparable a una solución EDR. Confirmar si dicha funcionalidad debe ser nativa de la plataforma de vulnerability management ofertada, o si resulta aceptable que se cumpla mediante la integración de la solución con el motor antivirus/EDR ya existente en la infraestructura de la CSJ, dado que esta última es una arquitectura frecuente en el mercado y evita duplicar capacidades ya cubiertas por otra herramienta institucional. Indicar la fuente y periodicidad de actualización de la base de firmas de malware exigida, y si se aceptan fuentes de inteligencia de amenazas de terceros integradas a la plataforma, o si se exige que dicha base sea desarrollada y mantenida exclusivamente por el propio fabricante del software de vulnerability management.		

Consulta 19 - Especificaciones Técnicas de la Solución — Funcionalidades de Detección — "Malware"

Consulta	Fecha de Consulta	16-09-2026
Texto / Exigencia Actual: "Malware — Detección de software malicioso conocido." Consulta / Observación / Petición Concreta: Solicitamos a la Entidad Convocante fundamente técnicamente la inclusión de esta funcionalidad dentro del objeto de una contratación cuyo alcance principal, según el numeral "Objeto Técnico de la Contratación", es la adquisición de "licenciamiento de software especializado en descubrimiento y evaluación de vulnerabilidades", y no de detección o remediación de malware, la cual corresponde a un dominio de ciberseguridad distinto (protección de endpoint) con soluciones, arquitecturas y criterios de evaluación propios. De mantenerse el requisito, solicitamos se aclare si su incumplimiento —o su cumplimiento mediante integración con herramientas de terceros ya presentes en la CSJ— será causal de descalificación de la oferta, o si se trata de una funcionalidad deseable no eliminatoria, a efectos de que los oferentes puedan estructurar su propuesta técnica y económica con la debida certeza jurídica.		

Consulta 20 - Requisitos de capacidad técnica, Punto 1 (Técnico referente para horas de soporte).

Consulta	Fecha de Consulta	24-09-2026
Texto / Exigencia actual: "...el mismo deberá formar parte del plantel de la empresa y deberán figurar en la Planilla del Instituto de Previsión Social correspondiente al mes anterior vencido a la fecha de la etapa competitiva." Consulta / Observación / Petición concreta: Solicitamos a la Convocante eliminar la exigencia de que el técnico referente figure en la planilla del IPS y admitir, como medio válido de vinculación, el contrato de prestación o locación de servicios profesionales vigente con el oferente. El fundamento es que el tipo de vínculo jurídico entre el oferente y su técnico no tiene relación con la cantidad de horas de soporte, la calidad técnica del servicio ni su continuidad. La idoneidad del profesional ya queda garantizada por los demás requisitos de la misma cláusula: la certificación en la herramienta ofertada y la experiencia comprobable de al menos dos años en seguridad de la información o ciberseguridad. Además, la responsabilidad frente a la Convocante por el cumplimiento de las horas de soporte y de los niveles de servicio recae siempre sobre el oferente adjudicado, cualquiera sea la figura con la que haya vinculado a su personal. Las garantías de fiel cumplimiento y el régimen de penalidades del contrato protegen suficientemente los intereses de la Entidad. En el mercado de ciberseguridad es habitual que los profesionales certificados presten servicios de forma independiente, con RUC y facturación propia. Exigir relación de dependencia restringe artificialmente el universo de oferentes y favorece a empresas de mayor tamaño, sin beneficio técnico alguno para la Convocante. Ello contraría los principios de igualdad, libre competencia, economía, eficiencia y transparencia que rigen las contrataciones públicas conforme a la Ley N° 7021/2022 "De Suministro y Adquisiciones Públicas".		

Consulta 21 - Requisitos de Capacidad Técnica - Oferentes en Consorcio

Consulta	Fecha de Consulta	24-09-2026
Consulta: En el apartado de Requisitos de Capacidad Técnica, el PBC establece para oferentes en consorcio que "LOS INTEGRANTES DEL CONSORCIO EN FORMA COMBINADA DEBEN CUMPLIR CON TODOS LOS REQUISITOS SOLICITADOS". La redacción admite dos interpretaciones. Según la primera, el consorcio en su conjunto debe reunir la totalidad de los requisitos, y basta que cada uno sea cumplido por al menos uno de sus integrantes. Según la segunda, todos y cada uno de los integrantes deben cumplir individualmente con todos los requisitos de los puntos 1 al 7. La segunda interpretación desnaturalizaría la figura del consorcio, cuya finalidad es precisamente complementar capacidades técnicas, financieras y operativas entre empresas, y restringiría injustificadamente la participación de consorcios en la presente licitación. Ello contraría los principios de igualdad, libre competencia y transparencia consagrados en la Ley N° 7021/2022 "De Suministro y Adquisiciones Públicas". Solicitamos a la Convocante aclarar expresamente que la expresión "en forma combinada" significa que los requisitos de capacidad técnica se consideran cumplidos cuando el consorcio en su conjunto los acredita, siendo suficiente que cada requisito sea cumplido por al menos uno de sus integrantes, y no que cada miembro deba cumplirlos en forma individual.		

Consulta 22 - Requisitos de Capacidad Técnica Punto 1 - Oferentes en Consorcio

Consulta	Fecha de Consulta	24-09-2026
Consulta: En el Punto 1 de los Requisitos de Capacidad Técnica se exige contar con "al menos 1 (un) técnico referente para las horas de soporte" que forme "parte del plantel de la empresa". Para el caso de consorcios, el pliego no aclara si el técnico debe pertenecer a un integrante determinado, si cada integrante debe contar con su propio técnico referente, o si basta con que el técnico esté vinculado a cualquiera de los miembros. Dado que el requisito se refiere a un único técnico para la prestación del soporte, exigir un técnico por integrante carecería de relación con el objeto del llamado y limitaría la concurrencia. Solicitamos a la Convocante aclarar que, en caso de consorcio, el requisito se considera cumplido con al menos un técnico referente que reúna la certificación y experiencia exigidas y que esté vinculado a cualquiera de los integrantes del consorcio.		

Consulta 23 - Requisitos de Capacidad Técnica Punto 2 - Oferentes en Consorcio

Consulta	Fecha de Consulta	24-09-2026
Consulta: En el Punto 2 de los Requisitos de Capacidad Técnica se exige que "El oferente deberá contar con certificación ISO 9001 de Sistema de Gestión de la Calidad, vigente". Para oferentes en consorcio, el pliego exige cumplir los requisitos "en forma combinada", sin precisar si la certificación debe ser presentada por todos los integrantes o si basta con que la posea uno de ellos. Exigirla a todos los miembros impondría una barrera de entrada desproporcionada, pues la calidad del servicio queda garantizada cuando el integrante que ejecuta o gestiona el servicio cuenta con dicho sistema de gestión certificado. Además, la responsabilidad solidaria de los consorciados frente a la Convocante protege plenamente sus intereses. Solicitamos a la Convocante aclarar que, en caso de consorcio, la certificación ISO 9001 vigente se considera cumplida con la presentación del certificado de al menos uno de sus integrantes.		

Consulta 24 - Cantidad de dominios para escaneo

Consulta	Fecha de Consulta	24-09-2026
Solicitamos a la convocante aclarar al realizar el escaneo cuantos dominios deberán estar incluidos?, ya que solo figura la cantidad de activos.		

Consulta 25 - consultas

Consulta	Fecha de Consulta	24-09-2026
Referencia: Sección "ESPECIFICACIONES TÉCNICAS DE LA SOLUCIÓN" > "Capacidades de Escaneo", ítem "Plantillas preconfiguradas" (Página 32), donde se exige: "Al menos 400 plantillas listas para usar en diferentes escenarios de escaneo". Consulta: Considerando que las tecnologías más avanzadas de ciberseguridad evolucionan hacia enfoques más inteligentes, ¿se considerará como CUMPLIDO este punto si el oferente presenta una solución que no depende de "plantillas" o reglas fijas, sino que utiliza un motor de descubrimiento proactivo y dinámico que identifica y evalúa las vulnerabilidades basándose de manera automatizada en la tecnología y configuración detectada en el entorno?		

Consulta 26 - consulta

Consulta	Fecha de Consulta	24-09-2026
Referencia: Sección "ESPECIFICACIONES TÉCNICAS DE LA SOLUCIÓN" > "Funcionalidades de Detección", ítem "Malware" (Página 32), donde se exige: "Detección de software malicioso conocido". Consulta: Entendiendo que el objeto principal del llamado es el monitoreo y gestión de vulnerabilidades (y no la adquisición de un antimalware/antivirus tradicional), solicitamos a la Convocante aclarar si se considerará como CUMPLIDO este requerimiento mediante soluciones que detectan vulnerabilidades y riesgos de explotación independientemente de si el software alojado es catalogado estrictamente como "malware" o si es una aplicación productiva legítima del ambiente que presenta brechas de seguridad.		