CAPACIDAD FINANCIERA.

a. Para contribuyente de IRE GENERAL.

- Deberán cumplir con los siguientes parámetros:
  - Ratio de Liquidez: activo corriente / pasivo corriente
    - Deberá ser igual o mayor que 1, en promedio, en los años 2023, 2024, 2025.
  - Endeudamiento: pasivo total/ activo total
    - No deberá ser mayor a 0,80 en promedio, en los años 2023, 2024, 2025.
  - Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital.
    - El promedio de la sumatoria de los años 2023, 2024, 2025, no deberá ser negativo.

b. Para contribuyentes de IRE SIMPLE.

- Deberán cumplir el siguiente parámetro:
  - Eficiencia: (Ingreso/Egreso)
    - Deberá ser igual o mayor que 1, el promedio de la sumatoria de los años 2023, 2024, 2025.

c. Para contribuyentes de IRP

- Deberán cumplir el siguiente parámetro:
  - Eficiencia: (Ingreso/Egreso).
    - Deberá ser igual o mayor que 1, el promedio de la sumatoria de los años 2023, 2024, 2025.

d. Para contribuyentes de exclusivamente IVA General

- Deberán cumplir el siguiente parámetro:
  - Eficiencia: (Ingreso/Egreso).
    - Deberá ser igual o mayor que 1, el promedio de la sumatoria de los años 2023, 2024, 2025.

OFERENTES EN CONSORCIO: CADA MIEMBRO DEBE CUMPLIR CON CADA UNO DE ESTOS REQUISITOS.

REQUISITOS DOCUMENTALES PARA LA EVALUACIÓN DE LA CAPACIDAD FINANCIERA.

1. Balance General y Estados de Resultados de los años 2023, 2024, 2025, firmados por el contador, propietario y/o representante legal si correspondiere, acorde a las normas contables y a los modelos establecidos en las Normativas Vigentes de la Dirección Nacional de Ingresos Tributarios (www.dnit.gov.py).
2. Formulario 500 de los años 2023, 2024, 2025, correspondientes a la Declaración Jurada del Impuesto a la Renta.
3. Formulario 501 de los años 2023, 2024, 2025, correspondientes a contribuyentes del IRE SIMPLE.

4. Formulario 515 para contribuyentes de Renta Personal y Formulario 516 IRP RGC de los años 2023, 2024, 2025.
5. Formulario 120 solo para contribuyentes del IVA General de los 36 (TREINTA Y SEIS) meses, correspondiente a los años 2023, 2024, 2025.

EXPERIENCIA REQUERIDA.

El oferente deberá contar con contratos ejecutados y/o facturas de ventas relacionados a **SERVICIOS GESTIONADOS DE CIBERSEGURIDAD Y/O AUDITORIAS DE VULNERABILIDADES Y/O SERVICIOS DE SOC Y/O RESPUESTAS A INCIDENTES Y/O PRUEBAS DE INTRUSIÓN (PENTEST)**, que podrán corresponder tanto a instituciones públicas como privadas. Dichos contratos deberán corresponder al periodo comprendido entre los últimos 5 (cinco) años **2021, 2022, 2023, 2024, 2025**, y deberá ser como mínimo el 40% (cuarenta por ciento) del monto total de la oferta. Se aclara que no es necesario contar con un contrato y/o facturas por año.

- **OFERENTES EN CONSORCIO: EL SOCIO LÍDER DEBE CUMPLIR AL MENOS CON EL 60% (SESENTA POR CIENTO) DEL REQUISITO Y EL RESTO DE LOS SOCIOS AL MENOS EL 40% (CUARENTA POR CIENTO) DE ESTE REQUISITO.**

REQUISITOS DOCUMENTALES PARA LA EVALUACIÓN DE LA EXPERIENCIA.

Copia de contratos ejecutados y/o facturas de ventas relacionados a **SERVICIOS GESTIONADOS DE CIBERSEGURIDAD Y/O AUDITORIAS DE VULNERABILIDADES Y/O SERVICIOS DE SOC Y/O RESPUESTAS A INCIDENTES Y/O PRUEBAS DE INTRUSIÓN (PENTEST),** que podrán corresponder tanto a instituciones públicas como privadas. Dichos contratos deberán corresponder al periodo comprendido entre los últimos 5 (cinco) años 2021, 2022, 2023, 2024, 2025, y deberá ser como mínimo el 40% (cuarenta por ciento) del monto total de la oferta. Se aclara que no es no es necesario contar con un contrato y/o facturas por año.

CAPACIDAD TÉCNICA.

1. Deberá contar con al menos 1 (un) técnico referente para las horas de soporte, con certificación en la herramienta ofertada y con experiencia comprobable de al menos 2 (dos) años en seguridad de la información y/o ciberseguridad; 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.
2. El oferente deberá contar con certificación ISO 9001 de Sistema de Gestión de la Calidad, vigente.
3. El oferente será responsable ante daños a los bienes de la convocante.
4. El oferente deberá comprometerse a no utilizar, disponer, divulgar, difundir a ninguna otra institución o persona, ni antes ni durante ni después de la prestación de servicios, información alguna a la que haya podido tener acceso mediante esta contratación, debiendo ser considerada toda esta información como de estricta y absoluta confidencialidad sobre los datos almacenados y la arquitectura tecnológica de Corte Suprema de Justicia.
5. Deberá realizar una visita e inspección a las instalaciones.
6. Deberá cumplir con las especificaciones técnicas.
7. El oferente deberá presentar catálogos de la herramienta ofertada.

- **OFERENTES EN CONSORCIO: LOS INTEGRANTES DEL CONSORCIO EN FORMA COMBINADA DEBEN CUMPLIR CON TODOS LOS REQUISITOS SOLICITADOS.**

REQUISITOS DOCUMENTALES PARA EVALUAR EL CRITERIO DE CAPACIDAD TÉCNICA.

1. Planilla de Instituto de Previsión Social correspondiente al mes anterior vencido a la fecha de la etapa competitiva en donde figure el personal solicitado que deberá formar parte del plantel de la empresa y se deberá acompañar con la siguiente documentación:

a. Copia de cédula de identidad.
b. Certificación oficial en el uso de la herramienta, expedido por el fabricante o centro autorizado de capacitación.
c. Currículum Vitae acompañado de todos los documentos respaldatorios que avalen la formación profesional (títulos y certificados) y la experiencia (constancias laborales y/o contratos) en cualquiera de los siguientes rubros de seguridad de la información y/o ciberseguridad: SIEM, Forensica digital (Forensic Tools), Respuesta a Incidentes (Incident Response Tools), Inteligencia de amenazas, orquestación y automatización de respuesta, auditoría de vulnerabilidades, administración de logs (Log Management tools), Virtualización, Gestión de identidad y Accesos, Emulación de adversarios, SOAR, UTM, Firewalls, Vulnerability Management tools, Cyberthreat Intelligence Platform, Security by Deception tools, Traffic Capture & Flow Analyses, Adversary Emulation/Simulation tools, DFIR stacks/tools, SASE, plataformas o herramientas de Zero Trust, IAM, CASB, Native Virtualization Platforms, Switching/Routing Intermediate, et u otros tipos de herramientas/tecnologías asociados.

2. ISO 9001 de Sistema de Gestión de la Calidad, vigente, emitido por un organismo acreditado y a nombre del oferente.

3. Declaración Jurada en la cual manifieste que serán de entera responsabilidad del oferente, todos los daños a los bienes de la convocante, provenientes de hechos u omisiones de sus empleados, sin cargo alguno para la convocante.
4. Declaración Jurada en la cual el oferente se compromete a no utilizar, disponer, divulgar, difundir a ninguna otra institución o persona, ni antes ni durante ni después de la prestación de servicios, información alguna a la que haya podido tener acceso mediante esta contratación, debiendo ser considerada toda esta información como de estricta y absoluta confidencialidad sobre los datos almacenados y la arquitectura tecnológica de la Corte Suprema de Justicia.
5. Constancia de visita técnica de las instalaciones expedida por la Dirección General de Tecnología de la Información y Comunicación.
6. Especificaciones técnicas debidamente firmadas y llenadas, indicando cómo cumple en la columna correspondiente.
7. Catálogo de la herramienta ofertada.

DETALLE DE LOS BIENES Y/O SERVICIOS

OBJETO TÉCNICO DE LA CONTRATACIÓN

La presente licitación tiene por objeto la adquisición de licenciamiento de software especializado en descubrimiento y evaluación de vulnerabilidades de ciberseguridad, incluyendo la implementación inicial y horas de soporte técnico especializado para la Corte Suprema de Justicia del Paraguay.

ALCANCE DE LA CONTRATACIÓN

La contratación comprende un único ítem que incluye:

Componente	Especificaciones técnicas mínimas.	ESPECIFICACIONES TÉCNICAS OFERTADAS.
Denominación del Software	Indicar nombre y versión.	INDICAR
Licencia de Software	Licenciamiento por 36 meses para escaneo y descubrimiento de vulnerabilidades en 264 activos de TI, con capacidad de crecimiento de hasta un 30% adicional.	INDICAR
Tipos de Activos Soportados	El software debe poder escanear los siguientes tipos de activos: • Sistemas operativos (Windows Server, Linux, Unix) • Dispositivos de red (routers, switches, firewalls) • Hipervisores y entornos virtualizados • Bases de datos • Servidores web y aplicaciones • Dispositivos de almacenamiento (SAN, NAS) • Infraestructura crítica • Contenedores Dockers.	INDICAR
Implementación Inicial	Instalación, configuración, puesta a punto y trasferencia tecnológica al personal DCPI (sin costo adicional)	INDICAR
Soporte Técnico Especializado	270 horas para soporte, consultas y eventos posteriores a la implementación, durante la vigencia del contrato	INDICAR

ESPECIFICACIONES TÉCNICAS DE LA SOLUCIÓN

Características Generales del Software

El software de descubrimiento de vulnerabilidades debe ser una solución líder en el mercado, con reconocimiento internacional y amplia trayectoria en el sector de ciberseguridad. Debe contar con una base de conocimiento amplia y actualizada de forma permanente y de corta periodicidad para la detección precisa de amenazas.

Debe cumplir con los siguientes requisitos mínimos:

Capacidades de Escaneo

Requisito	Especificaciones técnicas mínimas.	Especificaciones técnicas ofertadas.
Escaneo ilimitado	**Sin restricción en la cantidad de escaneos a realizar sobre los activos licenciados**	INDICAR
Base de vulnerabilidades	**Acceso a biblioteca de firmas, plugins, scripts de detección o equivalentes**	INDICAR
Cobertura de CVEs	**Capacidad de detectar al menos 100.000 vulnerabilidades conocidas contra standard internacional (CVE)**	INDICAR
Plantillas preconfiguradas	**Al menos 400 plantillas listas para usar en diferentes escenarios de escaneo**	INDICAR

Funcionalidades de Detección

Funcionalidad	Especificaciones técnicas mínimas.	Especificaciones técnicas ofertadas.
Vulnerabilidades de software	Identificación de fallas en aplicaciones y sistemas	INDICAR
Parches faltantes	Detección de actualizaciones de seguridad no aplicadas	INDICAR
Errores de configuración	Análisis de configuraciones inseguras	INDICAR
Malware	Detección de software malicioso conocido	INDICAR
Cumplimiento normativo	Auditoría basada en estándares CIS Benchmarks y mejores prácticas	INDICAR

Priorización y Análisis de Riesgos

El software debe incluir mecanismos de priorización basados en:

Funcionalidad	Especificaciones técnicas mínimas.	Especificaciones técnicas ofertadas.
Mecanismos de priorización basados en:	**- CVSS** (Common Vulnerability Scoring System) v3.1 o superior. - **EPSS** (Exploit Prediction Scoring System) para predicción de explotabilidad. - Indicadores propietarios de riesgo del fabricante.	INDICAR

Reportería y Exportación

Característica	Especificaciones técnicas mínimas	Especificaciones técnicas ofertadas.
Formatos de exportación	CSV, PDF, XML, HTML	INDICAR
Reportes personalizables	Capacidad de adaptar informes a necesidades específicas	INDICAR
Reportes gerenciales	Resúmenes ejecutivos para niveles directivos	INDICAR
Reportes técnicos	Detalle completo con pasos de remediación	INDICAR

IMPLEMENTACIÓN INICIAL

Obligaciones del Proveedor

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:

- Instaladores y manuales en formato digital de la última versión disponible.
- 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.

Actividades de Implementación

Actividad	Descripción	Plazo Máximo
Entrega de licencias	Suministro de claves de activación y acceso a actualizaciones	**30 días corridos**
Instalación	Despliegue del software en infraestructura local de la CSJ.	
Configuración	Ajuste de parámetros, políticas y plantillas de escaneo	
Trasferencia tecnológica	Entrenamiento al personal DCPI en uso y operación	
Puesta en producción	Sistema completamente funcional y operativo con las actividades anteriores completas	

Observación: Todos los plazos se cuentan desde la orden de ejecución. La implementación inicial es **obligación del proveedor sin costo adicional** y **no consume horas del banco de soporte técnico especializado**.

Transferencia de Conocimientos

La transferencia técnica inicial debe incluir como mínimo:

- Uso y navegación de la interfaz del software.
- Configuración y ejecución de escaneos.
- Interpretación de resultados y severidades.
- Generación y personalización de reportes.
- Mejores prácticas de remediación de vulnerabilidades.

Garantía de Compatibilidad.

El adjudicatario debe garantizar el correcto funcionamiento del software con la infraestructura existente de la CSJ, asumiendo la responsabilidad de resolver cualquier incompatibilidad sin costo adicional para la institución.

SOPORTE TÉCNICO ESPECIALIZADO

Soporte Técnico de Horas

Parámetro	Valor
Total de horas disponibles	270 horas
Vigencia	Durante los 36 meses del contrato
Alcance	Consultas y eventos POSTERIORES a la implementación inicial

Cobertura del Soporte

El soporte técnico especializado cubre:

- Resolución de dudas técnicas sobre el uso del software.
- Asistencia en configuración de escaneos especiales.
- Apoyo en interpretación de resultados complejos.

- Diagnóstico y resolución de problemas operativos.
- Asesoría en mejores prácticas de gestión de vulnerabilidades.

No incluye: La implementación inicial.

Tiempos de Respuesta (SLA)

Severidad	Descripción	Tiempo de asistencia.
Crítica	Sistema inoperativo	4 horas
Alta	Funcionalidad degradada	8 horas
Media	Consultas técnicas	24 horas
Baja	Solicitudes generales	48 horas

El oferente adjudicado deberá proveer horas de Soporte Técnico On Site o Remoto durante la vigencia del contrato, según demanda del contratante. El Soporte Técnico contemplará como mínimo lo establecido en su cobertura para los incidentes que pudieran ocurrir o en su defecto a requerimiento de la convocante.

Metodología de utilización de las horas

El proveedor realizará la verificación del requerimiento técnico de la DGTIC y posteriormente elaborará un informe técnico de los trabajos e indicaciones pertinentes, además realizará la transferencia tecnológica al equipo técnico de la DGTIC sobre el soporte realizado.

La asistencia técnica se realizará conforme a la comunicación con el plazo máximo establecido según severidad correspondiente.

El mismo se realizará en formato 5x8 de lunes a viernes de 07:00 a 15:00, remotamente o en las oficinas de la Dirección General de Tecnología de la Información y Comunicaciones del Poder Judicial, ubicada en las calles Mariano Roque Alonso y Pedro Blasio Testanova.

Entregables
El proveedor deberá presentar los siguientes documentos para certificar su gestión:

Tipo de Entregable	Contenido / Indicador	Plazo
Entregable Inicial	Claves de licencia, credenciales de acceso, manuales oficiales, Acta de trasferencia tecnológica y Acta de Recepción de la implementación.	Única vez (Día 30)
Informe de Incidente	Detalle de tickets de soporte: problema reportado, diagnóstico, solución aplicada y tiempo consumido (cantidad de horas de soporte).	Por evento (Post-soporte)
Reporte Gerencial	Resumen ejecutivo del estado de vulnerabilidades, tendencias de riesgo y saldo de horas de soporte.	Anual