DICTAMEN TECNICO N° 13 /2025

OBJETO: En la cual se sustentan las especificaciones técnicas requeridas para el proceso licitatorio de: **"SOLUCION PARA PROTECCION AVANZADA CONTRA AMENAZAS CIBERNETICAS", ID 471946.**

INFORMACIÓN PREVIA

Lugar y fecha: San Lorenzo, 11 de julio de 2025

UOC Convocante: DIRECCION NACIONAL DE TRANSPORTE DINATRAN

Unidad o área requirente: Dirección General de Tecnología de Información y Comunicaciones.

Funcionario o técnico responsable: Lic. Miguel Ángel Ayala Benítez

Dependencia y cargo que desempeña: Director General

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

El presente llamado tiene como objetivo principal el fortalecimiento de la seguridad cibernética institucional. En un entorno digital en constante evolución, donde emergen amenazas cada vez más sofisticadas, se vuelve imperativo proteger nuestra infraestructura tecnológica. En este contexto, se requiere la adquisición de una solución de protección avanzada contra amenazas, con el objetivo de detectar y prevenir una amplia gama de ataques cibernéticos, incluidos aquellos de tipo avanzado, permitiendo identificar comportamientos anómalos y responder en tiempo real ante posibles incidentes de seguridad.

- **Identificar y justificar de forma expresa si algún requerimiento pudiera 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.**

NO APLICA.-

DIRECCIÓN NACIONAL DE TRANSPORTE Dirección General de Contrataciones DINATRAN San Lorenzo Paraguay

Lic. Miguel A. Ayala Director General Dirección General de Tics DINATRAN

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:

Lic. Miguel A. Ayala
Dirección General de Tics
DINATRAN

Aclaración: Lic. Miguel Ángel Ayala Benítez

Firma del responsable UOC:

DIRECCIÓN NACIONAL DE TRANSPORTE Dirección General de Contrataciones DINATRAN San Lorenzo Paraguay

Estela López de Valdez
Directora General
Dirección General de Contrataciones
DINATRAN

Aclaración: Estela Lopez de Valdez

ESPECIFICACIONES TECNICAS.

"SOLUCION PARA PROTECCION AVANZADA CONTRA AMENAZAS CIBERNETICAS", ID 471946

Objetivo

En la Dirección Nacional de Transporte (DINATRAN) reafirmamos nuestro compromiso con el fortalecimiento de la seguridad cibernética institucional. En un entorno digital en constante evolución, donde emergen amenazas cada vez más sofisticadas, se vuelve imperativo proteger nuestra infraestructura tecnológica.

En este contexto, se requiere la adquisición de una solución de protección avanzada contra amenazas, con el objetivo de detectar y prevenir una amplia gama de ataques cibernéticos, incluidos aquellos de tipo avanzado, permitiendo identificar comportamientos anómalos y responder en tiempo real ante posibles incidentes de seguridad.

Lista de Bienes

Ítem	Descripción	Unidad de medida	Cantidad
1	SOLUCION PARA PROTECCION AVANZADA CONTRA AMENAZAS CIBERNETICAS	Unidad	350

Marca	Especificar		
Modelo	Especificar		
Procedencia	Especificar		
Suscripción	Mínimo de 1 (un) año		
Características	**Descripción**	**Exigencia**	**Cumple / No cumple**
Características Generales	Se deberá proveer licencias para 350 dispositivos finales (PC, Notebooks, etc.)	Exigido	
	La solución de utilizar un mecanismo de comunicación seguro basado en protocolo SSL vía puerto 443 para facilidad de operación con capacidad de limitar el acceso a la consola poder grupos de direcciones IP.	Exigido	
	Se requiere que se utilice un único agente EDR/AV en el dispositivo, el cual no requiera ser reiniciado en su instalación como desinstalación	Exigido	
	En caso de requerir activación de funcionalidades adicionales no debe requerir nuevos despliegues de producto	Exigido	
	El consumo de recursos del agente debe ser en promedio 2% de CPU y no debe tener requerimientos de hardware específicos para su funcionamiento. Solo se garantizará los recursos para el funcionamiento de las aplicaciones productivas en los dispositivos	Exigido	

DIRECCIÓN NACIONAL DE TRANSPORTE
Dirección General de Planificación
DINATRAN
Asunción - Paraguay

Lic. Miguel A. Ayala
Director General
Dirección General de Tics
DINATRAN

	No debe requerir actualizaciones de patrones/ firmas/comportamientos. La solución debe estar basada en AI/ML (Inteligencia Artificial / Machine Learning) se aceptan combinaciones de modelo de firmas/heurística u otros mecanismos no especificados, que deben trabajar en línea o fuera de línea	Exigido	
	La plataforma debe tener la capacidad de poder instalarse en presencia de otra plataforma de antivirus sin interferir en la operación como también no debe requerir reiniciar equipos tanto en laptop como en servidores. Como no requerir configurar exclusiones/excepciones en el proceso de despliegue inicial	Exigido	
	La solución debe tener la capacidad de integración vía API REST. Esta API debe ser Bidireccional.	Exigido	
	La plataforma debe tener la capacidad de configuración de IOCs para su bloqueo o permiso de ejecución de forma personalizada o automatizada vía API	Exigido	
	La plataforma debe tener la capacidad de dar el detalle de la telemetría de las alertas y detecciones para poder tener un contexto de los ataques mediante análisis retrospectivos y reconstrucción de los eventos y procesos mediante un árbol de procesos de forma: Gráfica, listado de actividades entre otros	Exigido	
	La plataforma debe poder establecer control u comunicación directa por medio de línea de comandos con los sensores (win/linux/Mac) a fin de poder ejecutar comandos, correr scripts, saber el estado de procesos, conexiones, sacar archivos, o llevar archivos, reiniciar y otros comandos que permitan acelerar un análisis forense con el acceso directo a los equipos sin herramientas de terceros	Exigido	
	El despliegue de agentes/sensores se debe hacer sobre sistemas operativos:	Exigido	
	- Windows 7SP1 y superiores		
	- Windows 2008 R2 S1 y superiores.		
	- Linux en distribuciones soportadas (Amazon, CentOS, Oracle, RHEL, SUSE, open SUSE, Ubuntu, Debian, elrepo, Flatcar, IBM, Alma, rocky).		
	- MAC (Monterey, Ventura).		
	La solución ofertada debe haber sido calificada en últimos reportes como líder en los siguientes ámbitos:	Exigido	
	Líder "Gartner EPP", líder "The Forrester Wave – MDR", Líder "The Forrester Wave – EDR y líder - "The Forrester WaveThreat Intelligence" en los años 2023 y/o 2024.		
	Uso de la inteligencia de amenazas basado en la identificación de como los adversarios actúan en sus campañas para poder identificar TTPs atribuibles a grupos de ciberataques	Exigido	

DIRECCION NACIONAL DE TRANSPORTE Dirección General de Comunicaciones

Lic. Miguel A. Ayala
Director General
Dirección General de Tics
DINATRAN

	Capacidades de detección y prevención de:	Exigido	
	-Detección y prevención de virus/malware conocido y desconocido o día cero		
	-Detección y prevención de TTPs (mitre) en la explotación de vulnerabilidades		
	- Detección y prevención por indicadores de ataque (File-less attacks)		
	- Capacidad de independizar la detección de la prevención por políticas		
	- Identificación y prevención de actividad sospechosa (procesos, registro, script, comandos, drivers)		
	- Identificación y prevención de procesos de borrado de backup, cifrado, borrado de copias de volúmenes usado por los ataques de Ransomware basado en comportamiento		
	- Identificación y prevención de movimientos laterales y Accesos a credenciales		
	- Identificación y prevención de ataques y explotación de vulnerabilidades día cero		
	Capacidades de detección de TTPs en post ejecución como:	Exigido	
	- Capacidad de realizar remediación por indicadores de ataques para evitar persistencia de procesos maliciosos (ASEP)		
	-Administración de cuarentena de artefactos para liberar o eliminar de los dispositivos		
	La plataforma debe tener capacidad de desarrollar actividades forenses como:	Exigido	
	-Contar con un acceso remoto (vía línea de comando) a los equipos que tengan el agente instalado con perfil de administrador validado vía MFA para incorporar un control dual.		
	- Permitir la ejecución de comandos ya integrados de forma remota, y a través de una lista muestre el uso de cada uno de ellos.		
	- Contar con comandos de colección de datos que permitan dar paso a investigaciones. Los comandos requeridos son:		
	a) Explorar el sistema de archivos y extraer archivos.		
	b) Lista de procesos en ejecución.		
	c) Extraer el registro de eventos de Windows.		
	d) Consultar registro de Windows.		
	e) Enumere las conexiones de red actuales y la configuración de la red.		
	f) Extraer la memoria de un proceso (memory dump).		
	- Que cuente con comandos de remediación que permitan reacción sobre una acción puntual. Los comandos requeridos son:		
	a) Eliminar un archivo.		

DIRECCION NACIONAL DE TRANSPORTE
Dirección General de Contrataciones
San Lorenzo

Lic. Miguel A. Ayala
Director General
Dirección General de Tics
DINATRAN

	b) Terminar un proceso (Kill process)		
	c) Eliminar o modificar la clave o el valor del registro de Windows.		
	d) Enviar scripts programados		
	e) Enviar y recibir archivos por demanda		
	La solución deberá contar con la capacidad de aislar un activo (Endpoint/Server) de forma remota, bloqueando así cualquier comunicación externa a la computadora con excepción a la comunicación con la propia consola de gestión de la solución.	Exigido	
	La solución deber tener la capacidad de crear grupos con la finalidad de ser utilizados en la definición de políticas al menos por dominio, Sistema Operativo, Unidad Organizacional, versión del agente, tipo de equipo, ubicación, esto basado en la metadata del dispositivo registrado.	Exigido	
	La organización en grupos de forma automática o manual basado en reglas o filtros de acuerdo con los atributos de los dispositivos		
	La plataforma debe tener la capacidad de integración con plataforma de inteligencia de terceros de forma nativa como Virus total	Exigido	
	La solución debe contar con un módulo de antivirus de próxima generación con la capacidad de detección y bloqueo de nuevas tácticas, técnicas y procedimientos empleados por los grupos de cibercriminales.	Exigido	
	La solución debe contar como mínimo los siguientes elementos de análisis y características:		
	• Capacidad de bloqueo de la ejecución de código malicioso, bloqueo exploits de día cero, terminación (Kill) procesos y actividades de comando y control.		
	• Capacidad de protección aun cuando los equipos no cuenten con conectividad a la nube.		
	• Capacidad de protección de antimalware sin la necesidad de utilizar firmas de Antivirus, ni actualizaciones de IOCs de comportamiento. No se permiten soluciones basadas en firmas o detección de IOC únicamente.		
	• Aprendizaje maquina (machine learning en inglés) de forma local en cada punto final con Sistema operativo Microsoft Windows y Mac OS		
	• Bloqueo de procesos identificados por la inteligencia del fabricante como maliciosos.		
	• Detección y prevención de explotaciones de tipo Force DEP, Heap Spray preallocation, Force ASLR, SEH Ovewrite protection, NULL Page Allocation, Remote library Loading, Untrusted font.		

Lic. Miguel A. Ayala
Director General
Dirección General de Tics
DINATRAN

	Detección y prevención de scripts o comandos maliciosos vía powershell o CMD, entre otros incluyendo al menos lo siguiente:		
	• Cadenas ejecutadas dinámicamente vía el cmdlet "invoke-expression"		
	• Comandos vía –EncodedCommand.		
	• Detección y prevención de intentos de borrado de respaldos del sistema (volume shadow copy por sus siglas en inglés) comúnmente realizado por ataques de ransomware.		
	• Detección y prevención de los procesos de cifrado de archivos relacionados a extensiones usadas por ransomware.		
	• Detección y prevención de procesos asociados a accesos indiscriminados al sistema de archivos asociados a ransomware.		
	• Detección y prevención de movimientos laterales.		
	• Detección y prevención de intentos de robo de credenciales.		
	• Detección y prevención de intentos de elevación de privilegios.		
	• Detección y prevención de intentos de uso de "sticky keys".		
	• Detección y prevención de intentos de ejecución de archivos sospechosos y/o código malicioso creados por los programas de navegación a internet (web browsers por sus siglas en inglés).		
	• Detección y prevención de intentos de ejecución de rutinas de javascript por línea de comandos vía rundll32.exe		
	La plataforma debe incluir un módulo de automatización tipo SOAR nativo que permita desarrollar Playbooks, para la automatización de actividades de respuesta como: Aislamiento automático de dispositivos, enriquecimiento de inteligencia, auto triage notificaciones personalizadas, plugins con plataformas de inteligencia, ITSM como ServiceNow, Google Slack, Microsoft Teams, email, Webhooks, lanzar scripts de forma remota, entre otros	Exigido	
	La plataforma debe permitir la definición de roles personalizados para cumplir con los controles de acceso asignados a los administradores, auditores o terceros que deben ingresar a la consola como permitir el acceso mediante MFA e integración con SSO.	Exigido	
	La plataforma debe contar con un portal de ayuda, webinar y base de conocimiento integrado a la consola para poder ampliar los conocimientos sobre los módulos o webinar para poder aplicar buenas prácticas en el desarrollo de la solución. Como también hacer el escalamiento de casos en caso de requerirse con el fabricante en modalidad 7x24	Exigido	

DIRECCION NACIONAL DE TRANSPORTE Dirección General de Concesiones Asunción Paraguay

Lic. Miguel A. Ayala
Director General
Dirección General de Tics
DINATRAN

	La consola debe incorporar un mecanismo de autodepuración para eliminar los dispositivos que no se gestionan en un periodo mayor a 45 días calendario	Exigido	
	El licenciamiento de la plataforma se debe basar por el promedio de sensores activos en un periodo de un mes y no por el número de sensores desplegados.	Exigido	
	Los procesos de desinstalación de los sensores deben usar un token de autorización aleatorio, no se acepta el uso de passwords o contraseñas para proteger ante la desinstalación de los agentes	Exigido	
Consola de Administración	Se requiere de una solución cien por ciento (100%) nube, la cual permita la administración centralizada de estaciones de trabajo y servidores, inclusive si estos se encuentran distribuidos de forma remota. No se aceptan soluciones que involucren hardware o virtualización. La solución no debe generar costos operacionales en las premisas, DC o infraestructura de proveedores cloud que pertenezcan a la compañía. Como también si se requieren módulos o funcionalidades adicionales no se tenga que desplegar una consola adicional o agentes adicionales	Exigido	
	La solución debe contar con dos componentes generales para su operación y correcto desempeño:	Exigido	
	- Consola única central 100% nube (cloud) para administración y operación de todos los módulos ofrecidos y futuros.		
	- Sensores/software que serán instalados en estaciones de trabajo y servidores.		
	La consola de gestión debe dar visibilidad, detalles y reportes de información de alertas, detecciones, de toda la actividad de los dispositivos hasta 90 días.	Exigido	
Control de Dispositivos USB y Periféricos	Tener la capacidad de controlar los dispositivos USB en su ejecución, lectura o escritura como su bloqueo completo para evitar el movimiento de archivos no autorizados, para sistemas Windows y MAC	Exigido	
	Tener la capacidad de consultar que tipos de objetos son copiados o escritos en los dispositivos de almacenamiento	Exigido	
	Tener la capacidad de configuración de políticas de auditoria para monitoreo de toda la actividad de dispositivos externos, esto no debe requerir el despliegue de software adicional sobre los despliegues iniciales	Exigido	
	Tener la capacidad de crear reglas por clase y excepciones por ID de proveedor, ID de producto o número de serie.	Exigido	
	Debe tener la capacidad de informar automáticamente el tipo de dispositivo conectado con información del fabricante, nombre del producto y número de serie.	Exigido	

DIRECCIÓN NACIONAL DE TRANSPORTE Dirección General de Contrataciones DINATRAN San Lorenzo Paraguay

Lic. Miguel A. Ayala
Director General
Dirección General de Tics
DINATRAN

	Se deben contar con dashboards para poder ver la actividad de dispositivos externos.	Exigido	
Automatización	La solución debe tener la capacidad de correlacionar eventos de seguridad a escala global para detectar patrones de ataques sofisticados.	Exigido	
	La solución debe contar con la capacidad de integrar datos de diversas fuentes (endpoint, red, nube) para ofrecer una vision unificada de amenazas.	Exigido	
	Deberá tener la capacidad de recopilar y analizar datos de actividades en tiempo real y de forma continua, incluso cuando los dispositivos están fuera de línea.	Exigido	
	La solución deberá permitir la ejecución de acciones como aislamiento de red, eliminación de procesos o archivos maliciosos y la ejecución de scripts personalizados.	Exigido	
Control de Acceso	Capacidad de tomar el control del Firewall nativo de estaciones para sistemas Windows y MAC para la restricción o permisos de puertos, IPs y procesos	Exigido	
	Tener la capacidad de configuración de políticas de auditoria para monitoreo de toda la actividad de red esto no debe requerir el despliegue de software adicional sobre los despliegues iniciales	Exigido	
	Deberá utilizar el control de acceso basado en roles para asegurarse de que únicamente los administradores apropiados vean y administren las reglas del firewall.	Exigido	
	Deberá permitir la creación de un grupo de reglas vacío y construirlo, o comenzar con un grupo de reglas preestablecidas, una colección de reglas básicas que puede editar según sus necesidades.	Exigido	
	Las reglas de Firewall deben poder definir la localización del dispositivo con ello aplicar políticas de forma contextual, para identificar la ubicación se debe hacer con la definición de:	Exigido	
	- Tipo de conexión & SSID, IP Gateway, Servidor DHCP, Prueba de resolución DNS, Prueba de certificado Https, Prueba de ping, dirección IP		
	Capacidad de incorporar listas de URLs para poder hacer restricción sobre sitios no autorizados para la navegación, esto puede ser utilizando "Wild cards"	Exigido	
Busqueda de Amenazas	Deberá ofrecer un servicio administrado de cacería de amenazas capaz de detectar intrusiones, actividades maliciosas y adversarios, realizado directamente por el fabricante por medio de un equipo capacitado y certificado sin necesidad de realizar ningún tipo de VPN o instalación de plataforma de terceros para obtener la información	Exigido	
	Como parte del servicio deberá buscar de manera proactiva campañas de malware sigilosas y en caso de existir alguna se	Exigido	

Lic. Miguel A. Ayala
Director General
Dirección General de Tics
DINATRAN

	notificar según corresponda. El proceso de notificación debe ser via correo electrónico.		
	El servicio deberá ir más allá de la detección pasiva y automatizada, deberá investigar e incluso responder a indicadores que apunten a ataques. Alertar con recomendaciones de remediación, con un análisis detallado que permita determinar ¿qué sucedió? y ¿cómo? responder al incidente.	Exigido	
	Deberá contar con investigaciones retroactivas revisando datos históricos en busca de evidencia de una intrusión. Recopilar artefactos de investigación como direcciones IP, dominios, hashes y otros. Estos artefactos deberán ser cargados a una base de inteligencia propietaria del fabricante y generar alertas en la interfaz de usuario de la plataforma de seguridad ofertada.	Exigido	
	El servicio deberá estar disponible 24x7x365.	Exigido	
	El proceso de investigación debe contar con un playbook de investigación y análisis para poder clasificar las detecciones como mínimo: Falso positivo, verdadero positivo, indeterminado, sospechoso.	Exigido	
	Se debe tener en la consola de gestión de EDR un dashboard que muestre el número de investigaciones realizadas el equipo de cacería de amenazas	Exigido	
Capacitación	Se deberá incluir el acceso a herramientas y cursos oficiales enfocados en la configuración y gestión de la plataforma de seguridad ofertada. Esta capacitación se debe incluir para al menos 5 técnicos de la DINATRAN.	Exigido	
	El proveedor adjudicado deberá realizar el traspaso de conocimiento de lo que concierne a los parámetros y características de la solución implementada en la convocante.	Exigido	
Soporte	Debe incluir el soporte técnico del tipo 24/7 tanto por parte del fabricante como por parte del Proveedor durante 12 meses. Esta garantía deberá ser provista directamente por el fabricante de la solución ofertada, no serán aceptadas garantías solamente del partner o distribuidor local.	Exigido	
	El Proveedor deberá contar con al menos 2 técnicos certificados en la marca ofertada, no se aceptarán certificación del tipo comercial o preventa.	Exigido	
	El proveedor deberá contar con soporte telefónico, correo electrónico y sistema de gestión de casos (web) para gestión de incidentes (críticos y no críticos).	Exigido	
	Debe cumplir con SLA de respuesta técnica:	Exigido	
	- Critico: El soporte debe asistir al cliente en un tiempo menor a 2 horas ya sea de forma presencial o remota de acuerdo a la necesidad de la contratante.	Exigido	

DIRECCIÓN NACIONAL DE TRANSPORTE Dirección General de Contrataciones DINATRAN San Lorenzo Paraguay

Lic. Miguel A. Ayala
Director General
Dirección General de Tics
DINATRAN

	- No Crítico: El soporte debe asistir al cliente en un tiempo menor a 4 horas ya sea de forma presencial o remota de acuerdo a la necesidad de la contratante.	Exigido	
	La definición respecto al nivel de criticidad será determinada exclusivamente por la DINATRAN en la solicitud de soporte.	Exigido	
	El proveedor deberá dar asistencia técnica en el sitio declarado por la convocante, una vez reportado el problema, y si la solución al mismo así lo requiere. Esta asistencia comprende la solución de incidencias de funcionamiento lógico, para metrización o configuración del equipo proveído en este llamado, así como de cualquiera de los módulos del mismo que se encuentren bajo la cobertura del soporte	Exigido	
	Debe incluir el acceso a las documentaciones, configuración y mejores prácticas.	Exigido	
Licenciamiento	Se deben incluir las licencias y/o suscripciones necesarias por un periodo mínimo de 1 año.	Exigido	
Implementación	Se debe incluir la implementación y configuración del software.	Exigido	
	El Proveedor deberá contar con al menos 2 técnicos certificados en la marca ofertada, no se aceptarán certificación del tipo comercial o preventa.	Exigido	
	Se debe demostrar experiencia técnica en el despliegue y desarrollo de proyectos de ciber seguridad focalizados en EPP - EndPoint Protection. Se debe considerar mínimamente lo solicitado en la sección "Experiencia y capacidad técnica"	Exigido	

DIRECCIÓN NACIONAL DE TRANSPORTE
Dirección General de Contrataciones
DINATRAN
Asunción Paraguay

Lic. Miguel A. Ayala
Director General
Dirección General de Tics
DINATRAN