Inicio del Expediente
PEEX-CPJ-06-2023

Resolución núm. 001 Inicio del expediente

COMITÉ DE COMPRAS Y LICITACIONES DEL CONSEJO DEL PODER JUDICIAL

Referencia núm.: PEEX-CPJ-06-2023

Conforme a lo establecido en el Reglamento de Compras de Bienes y Contrataciones de Obras y Servicios del Poder Judicial, aprobado mediante resolución núm. 007/2019, de fecha dieciséis (16) de julio de dos mil diecinueve (2019) por el Consejo del Poder Judicial; en la ciudad de Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los catorce (14) días del mes de marzo de dos mil veintitrés (2023), en horas laborables se reunió el Comité de Compras y Licitaciones, integrado por los señores: **Bionni Biosnely Zayas Ledesma**, consejera del Poder Judicial, presidenta del comité, designada mediante acta núm. 12/2021 de fecha trece (13) de abril del año dos mil veintiuno (2021); **Rosa María Magdalena Suárez Vargas**, directora general técnica, representada por **Vanesa María Camacho Melo,** coordinadora técnica de la Dirección General Técnica, según consta en el oficio núm. DGT-008 de fecha primero (1ero) de marzo de dos mil veintitrés (2023); **Ángel Elizandro Brito Pujols**, director general de Administración y Carrera judicial, representado por **Betty Esther Céspedes Torres**, gerente de control operativo de la Dirección General de Administración y Carrera Judicial, según consta en el oficio DGACJ núm. 003-2023, de fecha dos (2) de enero de dos mil veintitrés (2023); **Isnelda R. Guzmán de Jesús**, directora de planificación**; Alicia Angélica Tejada Castellanos,** directora administrativa; **Enmanuel Adolfo Moreta Fermín**, director legal y **Yerina Reyes Carrazana**, gerente de Compras, quien funge como secretaria (con voz, sin voto) para conocer lo siguiente:

AGENDA

PRIMERO: Verificar la existencia del quórum reglamentario, en cumplimiento con lo establecido en el artículo 8 del Reglamento de Compras de Bienes y Contrataciones de Obras y Servicios del Poder Judicial, el cual expresa lo siguiente: *"(…) con la asistencia de por lo menos cuatro (4) de sus miembros con voz y voto (…)".*

SEGUNDO: Determinar y autorizar el procedimiento de selección correspondiente para la *Adquisición de licencias para soluciones de ciberseguridad de Fortinet; gestión de vulnerabilidades Tenable.Io y sistema integral de inteligencia artificial para la ciberdefensa Darktrace*, de referencia núm. PEEX-CPJ-06 -2023.

TERCERO: Revisar y aprobar, si procede, las especificaciones técnicas para la *adquisición de licencias para soluciones de ciberseguridad de Fortinet (lote I),* elaboradas por **Luis Joel Mejía Castillo,** analista senior de Continuidad; **Adderli de la**

Rosa Suárez; coordinador de Seguridad de Infraestructura, y **Emmanuel E. Tejada Lora,** gerente de Seguridad y Monitoreo TIC; las especificaciones técnicas para la a*dquisición de licencias para la solución de gestión de vulnerabilidades TENABLE.IO (lote II)*, elaboradas por **Luis Vargas de la Cruz,** analista de Continuidad; **Adderli de la Rosa Suárez;** coordinador de Seguridad de Infraestructura, y **Emmanuel E. Tejada Lora,** gerente de Seguridad y Monitoreo TIC ; las especificaciones técnicas para la *adquisición de licencias del sistema integral de inteligencia artificial para la ciberdefensa Darktrace, (lote III),* elaboradas por **Luis Joel Mejía Castillo,** analista de Continuidad; **Adderli de la Rosa Suárez;** coordinador de Seguridad de Infraestructura, y **Emmanuel E. Tejada Lora,** gerente de Seguridad y Monitoreo TIC, las 2 primeras elaboradas el nueve (9) de febrero y la última en febrero de dos mil veintitrés (2023); y los términos de referencia elaborados por la Gerencia de Compras en fecha catorce (14) de marzo de dos mil veintitrés (2023), en el marco del procedimiento de excepción por exclusividad para la *adquisición de licencias para soluciones de ciberseguridad de Fortinet; gestión de vulnerabilidades Tenable.Io y sistema integral de inteligencia artificial para la ciberdefensa Darktrace,* de referencia núm. PEEX-CPJ-06-2023.

CUARTO: Designar a los peritos para la evaluación de las ofertas, conforme a la especialidad del requerimiento solicitado.

POR CUANTO: La Dirección Financiera del Consejo del Poder Judicial emitió las siguientes certificaciones de apropiación presupuestaria: 1) PG- 24154 -2023, por un monto de ocho millones seiscientos mil pesos dominicanos con 00/100 (RD$8,600,000.00) para *la renovación de licencias para soluciones de ciberseguridad de Fortinet*; 2) PG-24152-2023, por un monto de seiscientos mil pesos dominicanos con 00/100 (RD$600,000.00) para la *renovación de licencias para solución de gestión de vulnerabilidades Tenable.IO,* y 3) PG-24155-2023, por un monto de dos millones de pesos dominicanos con 00/100 (RD$2,000,000.00), para la *renovación de licencias del sistema integral de inteligencia artificial para la ciberdefensa Darktrace,* todas de fecha siete (7) de febrero de dos mil veintitrés (2023).

POR CUANTO: En fecha nueve (9) de febrero de dos mil veintitrés (2023), la Dirección de Tecnologías de la Información y la Comunicación del Consejo del Poder Judicial, elaboraron las especificaciones técnicas para la *adquisición de licencias para soluciones de ciberseguridad de Fortinet, gestión de vulnerabilidades Tenable.Io y sistema integral de inteligencia artificial para la ciberdefensa Darktrace,* de referencia núm. PEEX-CPJ-06-2023.

POR CUANTO: En fecha nueve (9) de febrero de dos mil veintitrés (2023), la Dirección de Tecnologías de la Información y la Comunicación del Consejo del Poder Judicial emitió los informes justificativos del uso de la excepción por exclusividad para la *adquisición de licencias para soluciones de ciberseguridad de Fortinet, gestión de vulnerabilidades Tenable.IO y sistema integral*

de inteligencia artificial para la ciberdefensa Darktrace, de referencia núm. PEEX-CPJ-05-2023, los cuales plantean lo siguiente*:*

<u>Con respecto a Adquisición de Licencias para Soluciones de Ciberseguridad de Fortinet:</u>

OBJETIVO

Presentar la justificación técnica para la Adquisición de Licencias para las Soluciones de Ciberseguridad de Fortinet a ser utilizadas para la seguridad perimetral, la interconexión entre localidades, administración centralizada, protección de dispositivos finales y el fortalecimiento de la ciberseguridad de la infraestructura tecnológica del Poder Judicial Dominicano.

ANTECEDENTES

El Poder Judicial ha definido su Plan Estratégico Institucional, el cual ha sido denominado Visión Justicia 20/24. Este, representa un proceso de transformación digital y evolución de todo el sistema de administración de justicia.

Es así como el eje estratégico número dos (2), Servicio Judicial oportuno y eficiente, busca lograr un servicio de justicia eficiente y confiable apoyado en las Tecnologías de la información y Comunicación (TIC'S) que actualmente se refleja a través de los siguientes proyectos en ejecución:

1. *Ruta de Implementación de la Ley y el Reglamento de Aplicación sobre el Uso de Medios Digitales.*
2. *Tareas asociadas con el fortalecimiento de la infraestructura tecnológica existente.*

En ese sentido, es imperativo contemplar el aseguramiento de los activos de información del Poder Judicial, lo que deriva en la necesidad de adquirir las licencias de dichas herramientas y soluciones que permiten la aplicación de controles de seguridad.

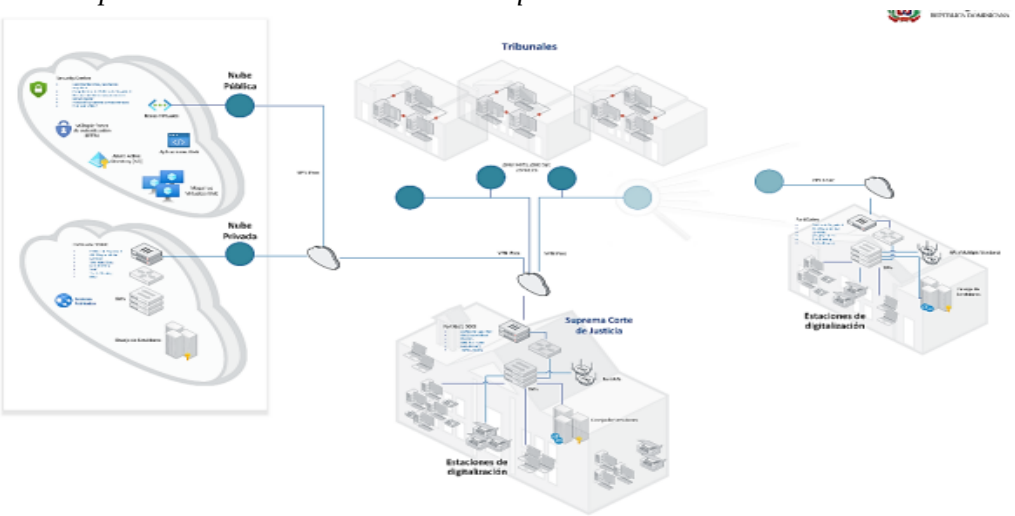
SITUACIÓN ACTUAL

De cara a los proyectos e implementaciones tecnológicas asociados con la Visión Justicia 20-24, el Poder Judicial cuenta con 21 sedes protegidas mediante equipos de seguridad perimetral de gestión de amenazas unificadas (UTM).

No.	Modelo	Localidad	Región
1	FortiGate 300E	Edif. De las Cortes	Distrito Nacional
2	FortiGate 500E	Edif. Suprema Corte de Justicia	Distrito Nacional
3	FortiGate 1100E	NAP del Caribe	Santo Domingo
4	FortiGate 80E	San Juan de la Maguana	Sur
5	FortiGate 100E	San Francisco de Macorís	Norte
6	FortiGate 100E	Puerto Plata	Norte
8	FortiGate 200E	KM22	Santo Domingo
9	FortiGate 300E	Santiago	Norte
10	FortiGate 100E	Sto. Dgo. Este	Santo Domingo Este
11	FortiGate 300E	Ciudad Nueva	Santo Domingo Este
12	FortiGate 100E	San Pedro de Macorís	Este
13	FortiGate 80E	La Romana	Este
14	FortiGate 60E	KM22	Santo Domingo
15	FortiGate 100E	Bonao	Norte
16	FortiGate 100E	Monte Cristi	Norte
17	FortiGate 80E	Jdo. Paz. 1ra.	Santo Domingo Este
18	FortiGate 60E	Juzgado de Trabajo D.N.	Distrito Nacional
19	FortiGate 80E	Barahona	Sur
20	FortiGate 80E	La Vega	Norte
21	FortiGate 100E	San Cristobal	Sur

Cada localidad posee enlaces seguros (VPN) para la interconexión hacia nuestro Datacenter principal para poder acceder a los recursos internos que no se encuentren

publicados y facilitar el acceso remoto a los recursos institucionales de parte del personal técnico especializado u otros colaboradores que lo ameriten.

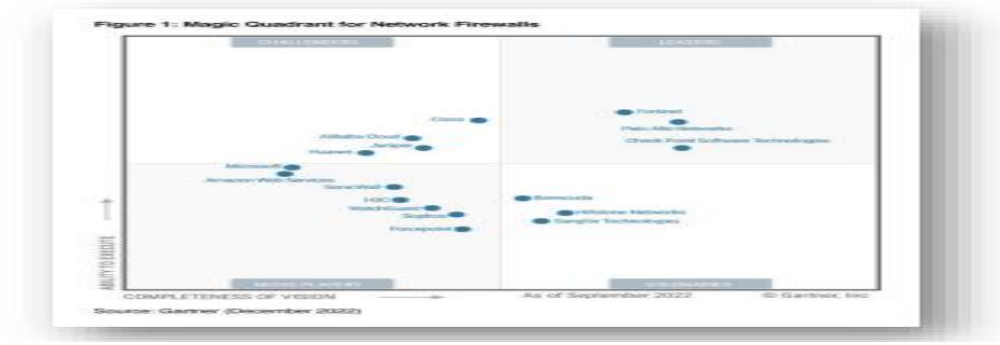


JUSTIFICACIÓN TÉCNICA

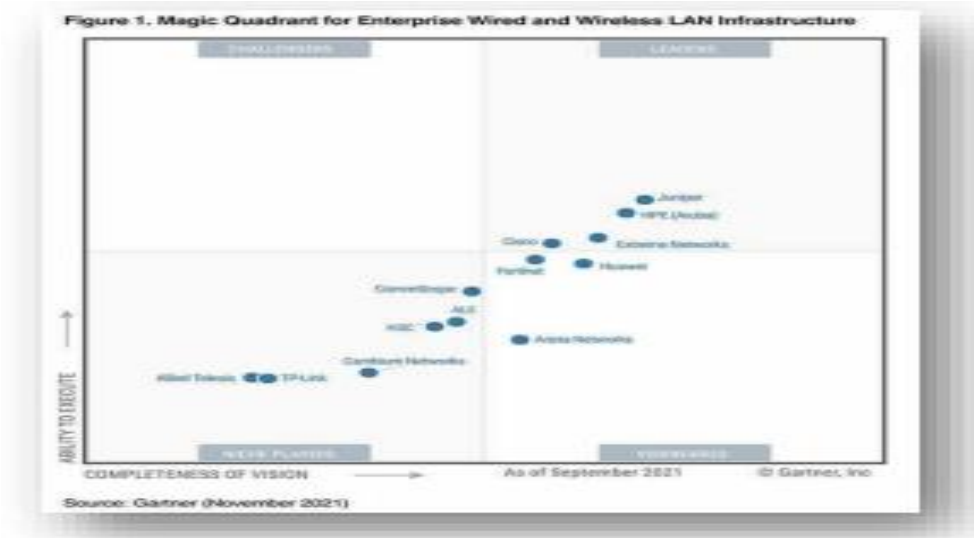
Actualmente, contamos con soluciones de ciberseguridad que nos ayudan a mitigar los riesgos asociados con la seguridad de la información y las redes de comunicación en general, y a su vez, se encuentran aplicando controles de seguridad que nos brindan la visibilidad necesaria para actuar de manera proactiva ante situaciones que pudieran comprometer a la institución.

El 4 de agosto del 2020, fue adjudicado el proceso de Excepción Por Exclusividad para la Adquisición de Equipos de Gestión Unificada de Amenazas (UTM) para el Poder Judicial Dominicano, Ref. PEEXCPJ-007-2020. En este proceso fueron adquiridos equipos de seguridad de la marca Fortinet y están siendo utilizados para integrar las sedes judiciales a través de la implementación de canales seguros y otros controles de seguridad. ***Los servicios de suscripción (licenciamiento) de estos equipos vencen en el mes de septiembre del 2023.***

El Cuadrante Mágico de Gartner para cortafuegos de red reconoció como líder por treceava vez a la empresa Fortinet, destacada por sus soluciones de ciberseguridad. Ver https://www.fortinet.com/solutions/gartner-network-firewalls



Fortinet también ha sido seleccionado por segunda vez consecutiva en infraestructuras de interconectividad entre sedes de empresas distribuidas. Ver https://www.fortinet.com/solutions/gartner-wired-wireless-lan



Es importante destacar, que en este momento el Poder Judicial en su centro de datos principal, así como en sus sedes, tiene estos equipos soportando los siguientes servicios:

a) Acceso directo a través de enlaces seguros a las plataformas: Sistema de Gestión de Casos, Plataforma de Firma Electrónica y el Acceso Digital, que están alojados en la nube de Microsoft.
b) Publicación de correo electrónico.
c) Publicación de aplicaciones institucionales.
d) Red desmilitarizada.
e) Acceso a internet protegido a través del uso de antivirus, sistema de prevención de intrusos, filtrado WEB basado en perfiles de acceso y niveles de riesgo.

f) Acceso remoto a las facilidades de la institución a través de redes privadas virtuales (VPN), facilitando el teletrabajo y la asistencia técnica de los especialistas

En este sentido, nuestros especialistas han sido entrenados y certificados como expertos en la gestión de estos equipos y han estado desarrollando las destrezas necesarias para la gestión de estos, apoyando el resguardo de toda la infraestructura tecnológica.

Por las razones antes descritas, solicitamos la adquisición de las licencias para los equipos de ciberseguridad descritos en las especificaciones técnicas. Emitimos este informe para sus consideraciones.

Aseguramos que los criterios utilizados en la elaboración de este documento están basados en los principios éticos, de transparencia, de imparcialidad y de procurar proteger los intereses del Poder Judicial.

Este documento sustituye, deroga y deja sin efecto cualquier otro relativo al informa de justificación para la Adquisición de Licencias de para equipos de Ciberseguridad Fortinet.

Con respecto Renovación de Licencias para Solución de Gestión de Vulnerabilidades Tenable. IO:

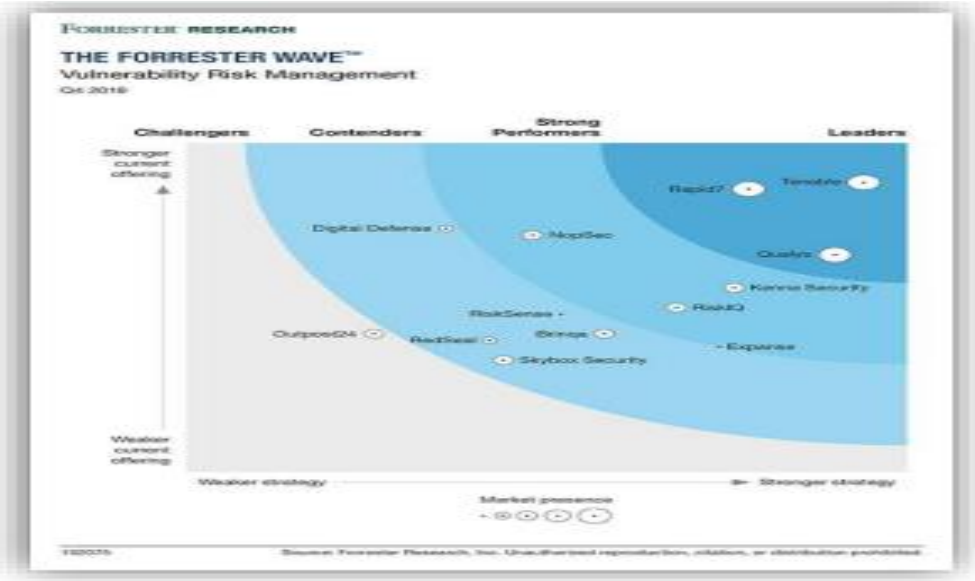
OBJETIVO

Presentar la justificación técnica para la Adquisición de Licencias de uso de la Plataforma de Gestión y Análisis de Vulnerabilidades Tenable.io a los fines de incluir la característica Web App Scanning

ANTECEDENTES

El Poder Judicial inició un proceso abierto para la selección de un proveedor de soluciones de gestión y análisis de vulnerabilidades a finales del año 2019, resultado adjudicatario el Grupo Tecnológico Adexsus, SRL, representante y proveedor de la solución Tenable.io en el país, de conformidad con lo dispuesto en la ley 340-06. En el año 2022 las licencias de uso de esta solución fueron renovadas a través del proceso de referencia no. CSM-2022-038.

Esta solución de gestión de vulnerabilidades es reconocida internacionalmente como líder en el mercado. Durante su implementación y uso ha brindado los resultados esperados por la Institución. Gracias a esta han sido mitigadas alrededor de 300 vulnerabilidades, altas y críticas, en el transcurso del año 2022.



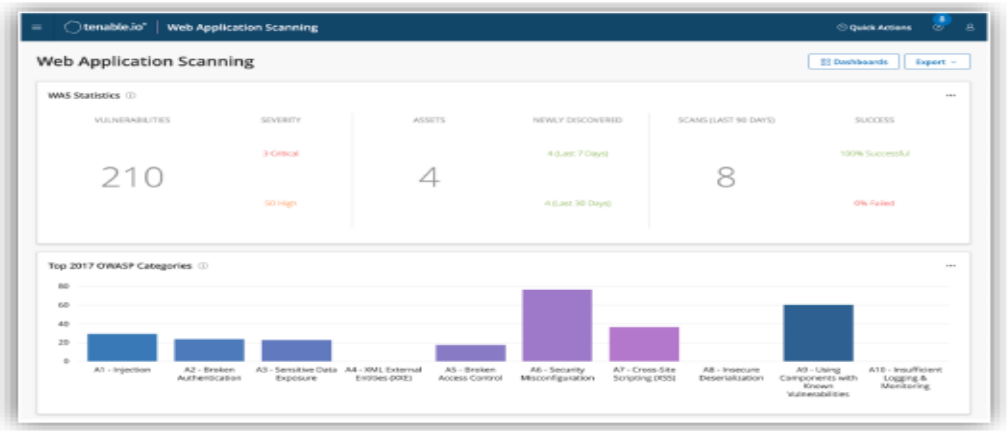
Todo esto alineado con el eje estratégico número 2 de nuestro Plan Estratégico Institucional (PEI), Servicio Judicial oportuno y eficiente, que busca lograr un servicio de justicia eficiente y confiable apoyado en las Tecnologías de la Información y Comunicación (TIC'S) utilizando herramientas que nos permitan el desarrollo de las operaciones críticas de la institución de una manera segura y confiable.

SITUACIÓN ACTUAL

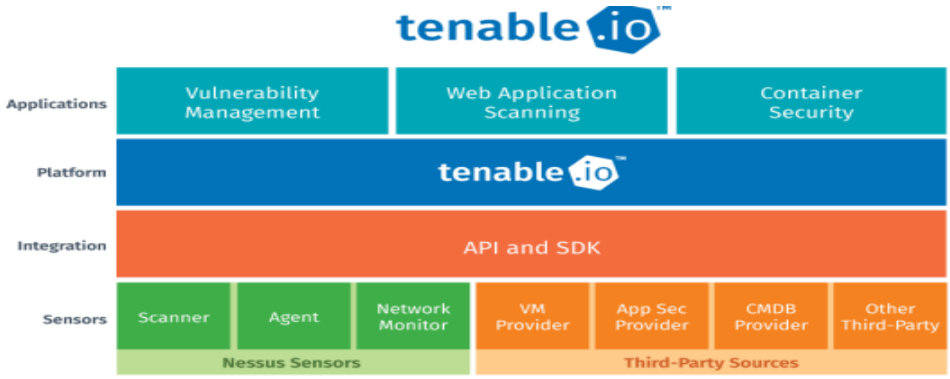
En la actualidad el proceso para la gestión de vulnerabilidades es ejecutado por la Gerencia de Seguridad de la Información, este proceso consiste en la detección de vulnerabilidades y la aplicación oportuna de controles a la infraestructura tecnológica.

Los activos de información críticos del Poder Judicial son escaneados de manera periódica a través de la plataforma Tenable.io (vulnerability management), brindándonos visibilidad sobre el estado de la seguridad de estos. Actualmente, se están escaneando más de 200 activos de información críticos y continuamos con la integración de otras soluciones, a continuación, una imagen que nos muestra su distribución:

De cara a la implementación de la ley 339-22 sobre el uso de medios digitales en el Poder Judicial y la implementación del Sistema de Gestión de Casos y el Acceso Digital, hemos identificado algunas oportunidades de mejora para el análisis de vulnerabilidades de aplicaciones web. En ese sentido, Tenable.io nos ofrece el módulo de ***Web App Scanning****. Este nos ofrece un análisis de vulnerabilidades seguro y automatizado que cubre todos nuestros servicios en línea. Además, nos proporciona detección de vulnerabilidades de manera completa y precisa, este escanea desde los 10 principales riesgos de OWASP hasta los componentes vulnerables de las aplicaciones web. Además, nos permite tener visibilidad completa de las vulnerabilidades de los activos de TI, de la nube y de aplicaciones web en una única plataforma.*



Esta herramienta nos brinda la confianza de que nuestros equipos de desarrollo no perderán el tiempo con falsos positivos ni pasarán por alto vulnerabilidades de alto riesgo. Además, nos permite comprender el mapa del sitio y el diseño de las aplicaciones web, esto para poder ver y evaluar las aplicaciones web globalmente. El escaneo de aplicaciones web altamente automatizado nos permite aumentar la visibilidad con facilidad. Esto nos brinda un alto grado de automatización lo cual se traduce en una reducción del trabajo manual.



RECOMENDACIONES TÉCNICAS

La recomendación técnica es que se proceda con la adquisición de la licencia de Tenable.io para incluir la funcionalidad de web application scanning a través de los procesos institucionales correspondientes, protegiendo así las operaciones y mitigando las vulnerabilidades de nuestros servicios tecnológicos.

Algunos de los beneficios de incluir este licenciamiento son:

1. *Este es un producto de ciberseguridad reconocido internacionalmente.*
2. *El personal que constituye el soporte técnico ya posee el conocimiento de manejo de esta herramienta.*
3. *Constituye un ahorro en el costo de implementación ya que el mismo se encuentra instalado en nuestra plataforma tecnológica.*
4. *El equipo de desarrollo identificará y remediará las vulnerabilidades de aplicaciones web de manera más eficiente.*
5. *El Sistema de Gestión de Casos y el Acceso Digital serán analizados automáticamente y de manera periódica en busca de vulnerabilidades en la seguridad. Permitiéndonos tomar acción inmediata y evitando que estas plataformas sean comprometidas.*

Aseguramos que los criterios utilizados en la elaboración de este documento están basados en los principios éticos, de transparencia, de imparcialidad y de procurar proteger los intereses del Poder Judicial.

Este documento sustituye, deroga y deja sin efecto cualquier otro relativo para la Adquisición del Licenciamiento para Solución de Gestión de Vulnerabilidades Tenable.io para el Poder Judicial.

<u>Por último, Licencias del Sistema Integral de Inteligencia Artificial para la Ciberdefensa DARKTRACE:</u>

OBJETIVO

Presentar la justificación técnica para la Adquisición de Licencias del Sistema Integral de Inteligencia Artificial para la Ciberdefensa DARKTRACE. A ser utilizado para la detección automática y respuesta a incidentes ante ataques maliciosos o robo de información de la infraestructura crítica del Poder Judicial con la finalidad de salvaguardar los recursos que en dicha infraestructura se encuentran.

ANTECEDENTES

El Poder Judicial ha definido su Plan Estratégico Institucional, el cual ha sido denominado Visión Justicia 20/24. Este Plan Estratégico Institucional representa un proceso de transformación digital y evolución de todo el sistema de administración de justicia.

Es así como el eje estratégico número dos (2), Servicio Judicial oportuno y eficiente, busca lograr un servicio de justicia eficiente y confiable apoyado en las Tecnologías de la información y Comunicación (TIC'S) que actualmente se refleja a través de los siguientes proyectos en ejecución:

1. *Desarrollo del Servicio Judicial en un ambiente completamente digital, contemplando el depósito de documentos, las solicitudes, las notificaciones, el centro de citaciones y las audiencias virtuales. Todo esto está siendo implementado a través de servicios en la nube.*
2. *Digitalización de expedientes.*

3. Firma Electrónica de documentos jurisdiccionales y administrativos. 4. Nueva página web del Poder Judicial.
5. Tareas asociadas con el fortalecimiento de la infraestructura tecnológica existente.
En ese sentido es imperativo contemplar el aseguramiento de los activos de información del Poder Judicial, lo que deriva en la necesidad de adquirir las licencias de dichas herramientas y soluciones que permiten la aplicación de controles de seguridad.

SITUACIÓN ACTUAL

El 17 de octubre de 2022, El Pleno de la Suprema Corte de Justicia (SCJ) aprobó el Reglamento de aplicación de la Ley núm. 339-22 que habilita el Uso de Medios Digitales en el Poder Judicial, normativa que tiene por objeto la implementación y regulación de las herramientas tecnológicas en los procesos judiciales y administrativos de cara a las competencias de los tribunales.

En ese sentido, para la implementación de dicha ley, a través de su reglamento de aplicación, fue necesaria la contratación de los siguientes servicios orientados a la ciberseguridad:

a. Servicios de auditoría a la calidad del software y pruebas de penetración, con el fin de identificar y solventar cualquier vulnerabilidad que presenten los activos que soportan el Sistema de Gestión de Casos y el Acceso Digital.
b. Herramienta para el registro de usuarios (servicios de Onboarding digital), que facilitará el registro de los ciudadanos y la verificación de su identidad para el acceso al portal de Acceso Digital, donde podrán realizar sus trámites.
c. Centro de Operaciones de Seguridad (SOC), facilitando el monitoreo de la infraestructura tecnológica critica 24/7 y la respuesta a incidentes cibernéticos a través de un primer nivel de soporte y su oportuna escalación a los especialistas de ciberseguridad del Poder Judicial cuando esto sea necesario.
*d**. Solución de monitoreo y respuesta a incidentes cibernéticos basada en Inteligencia Artificial**. Sistema que permite responder a cualquier actividad sospechosa de manera proactiva, aplicando controles de seguridad específicos para cada caso. Este sistema aprende los patrones de comportamiento de la red institucional para mantener los servicios e infraestructura tecnológicas que son accedidos a través de internet protegidos ante amenazas.*

Inicio del Expediente
PEEX-CPJ-06-2023

JUSTIFICACIÓN TÉCNICA

A fin de mitigar los riesgos asociados con la seguridad de la información y los recursos institucionales, en fecha 28 de agosto del 2022 fue adjudicado a la empresa NAP del Caribe el proceso ***CSM-2022-184.*** *A través de este proceso fue implementada la solución Darktrace, un sistema que de manera proactiva protege los activos de información de amenazas avanzadas, entre las que se incluyen software malicioso, así como ataques en la nube y en SaaS. El enfoque fundamentalmente de DarkTrace es el uso de Inteligencia Artificial (IA) de autoaprendizaje para conocer el comportamiento de nuestras redes de datos y defenderlas de manera autónoma, la misma ha sido implementada para el monitoreo y protección de los activos tecnológicos que conforman el Sistema de Gestión de Casos y el portal de Acceso Digital.*

En este sentido, nuestros especialistas han sido entrenados en la gestión de esta plataforma y han estado desarrollando las destrezas necesarias para su administración, apoyando el resguardo de toda la infraestructura tecnológica.

Es importante destacar, que los servicios de suscripción (licencias) de esta plataforma, expiran el 31 de octubre del 2023*.*

Por las razones antes descritas solicitamos la adquisición de las licencias para solución de ciberseguridad descrita en las especificaciones técnicas. Emitimos este informe para sus consideraciones.

Aseguramos que los criterios utilizados para la realización de este documento están basados en los principios éticos, de transparencia, de imparcialidad y de procurar proteger los intereses del Poder Judicial.

Este documento sustituye, deroga y deja sin efecto cualquier otro relativo al informe de justificación para la adquisición de Licencias del Sistema Integral de Inteligencia Artificial para la Ciberdefensa DARKTRACE,

POR CUANTO: Para la designación de los peritos evaluadores se deberá tomar en cuenta su capacidad y experiencia técnica en este tipo de especialidad.

POR CUANTO: En fecha dos (2) de marzo de dos mil veintitrés (2023), el ingeniero **Welvis Beltrán Matos,** director de Tecnologías de la Información y la Comunicación del Consejo del Poder Judicial, hizo la recomendación de los señores: **Luis Joel Mejía Castillo,** analista senior de Continuidad; **Adderli de la Rosa Suárez;** coordinador de Seguridad de Infraestructura; **Luis Vargas de la Cruz,** analista de Continuidad y **Emmanuel E. Tejada Lora,** gerente de Seguridad y Monitoreo TIC.; todos pertenecientes a la Dirección de Tecnologías de la Información y la Comunicación del Consejo

del Poder Judicial, como peritos para evaluar las propuestas que se recibirán en el marco del procedimiento de excepción por exclusividad para la *adquisición de licencias para soluciones de ciberseguridad de Fortinet, gestión de vulnerabilidades Tenable.IO y sistema integral de inteligencia artificial para la ciberdefensa Darktrace,* de referencia núm. PEEX-CPJ-06-2023.

POR CUANTO: En fecha tres (3) de marzo de dos mil veintitrés (2023), la Dirección de Tecnologías de la Información y la Comunicación del Consejo del Poder Judicial presentó vía la Dirección Administrativa los formularios de requerimientos de compras y contrataciones números **DTIC-025, 026 y 027,** a través de los cuales solicitan: *adquisición de licencias para soluciones de ciberseguridad de Fortinet, gestión de vulnerabilidades Tenable.IO y sistema integral de inteligencia artificial para la ciberdefensa Darktrace,* de referencia núm. PEEX-CPJ-06-2023.

POR CUANTO: En fecha catorce (14) de marzo de dos mil veintitrés (2022), la gerencia de Compras elaboró los términos de referencia para el procedimiento de excepción por exclusividad para la *adquisición de licencias para soluciones de ciberseguridad de Fortinet, gestión de vulnerabilidades Tenable.IO y sistema integral de inteligencia artificial para la ciberdefensa Darktrace,* de referencia núm. PEEX-CPJ-06-2023.

POR CUANTO: El criterio de evaluación establecido en el numeral 19 de los términos de referencia del presente procedimiento para la: *adquisición y/o renovación de softwares para las operaciones del 0*, establece que: *"El Comité de Compras y Licitaciones comparará y evaluará únicamente las Ofertas Económicas de los oferentes que hayan sido habilitados para tales fines. En ese sentido se verificará que las propuestas cumplan con los requerimientos establecidos en los numerales 17 y 18, de los términos de referencia"*

EN RELACIÓN CON LO ANTES EXPUESTO Y EN ATENCIÓN AL DERECHO:

CONSIDERANDO: El artículo 138 de la Constitución de la República Dominicana, proclamada en fecha trece (13) de junio de dos mil quince (2015), establece lo siguiente: *"Principios de la Administración Pública. La Administración Pública está sujeta en su actuación a los principios de eficacia, jerarquía, objetividad, igualdad, transparencia, economía, publicidad y coordinación, con sometimiento pleno al ordenamiento jurídico del Estado (…)".*

CONSIDERANDO: El artículo 4 numeral 8 del Reglamento de Compras y Contrataciones del Poder Judicial establece que: "*A condición de que no se utilicen como medios para vulnerar sus principios y se haga uso de los procedimientos establecidos en los reglamentos, serán considerados casos de excepción y no una violación a la norma: (…) 3. Las compras y contrataciones de bienes y servicios con exclusividad que sólo puedan ser suplidas por un número limitado de personas naturales o jurídicas".*

Inicio del Expediente
PEEX-CPJ-06-2023

CONSIDERANDO: El párrafo del artículo 4 del Reglamento de Compras y Contrataciones del Poder Judicial establece que, para los casos de excepción se regirán por los siguientes procedimientos: *"1) (…) se iniciarán con la resolución motivada, emitida por el Comité de Compras y Licitaciones, recomendando el uso de la excepción, previo informe pericial que lo justifique; 2) (…) con la Certificación de Existencia de Fondos emitida por el Director Financiero del Poder Judicial (…); 4) En los casos de bienes y servicios con exclusividad, se debe garantizar la oportunidad de participar de todos los oferentes beneficiados con la exclusividad. Deberá incluirse en el expediente los documentos justificativos de la exclusividad".*

CONSIDERANDO: El artículo 9, numerales 1 y 5 del citado reglamento establecen que corresponde al Comité de Compras y Licitaciones aprobar los pliegos de condiciones o términos de referencias y designar los peritos evaluadores en los procedimientos de compras y contrataciones de bienes, obras y servicios.

CONSIDERANDO: Que es obligación del Consejo del Poder Judicial, garantizar que las compras de bienes y servicios que realice la institución sean realizadas con irrestricto apego a la normativa vigente y a los principios de transparencia, libre competencia e igualdad de condiciones para todos los oferentes, entre otros; establecidos en el artículo 2 de la Resolución núm. 007/2019, que establece el Reglamento de Compras de Bienes y Contrataciones de Obras y Servicios del Poder Judicial de fecha dieciséis (16) de julio de dos mil diecinueve (2019).

VISTA: la Constitución de la República Dominicana proclamada el trece (13) de junio de dos mil quince (2015).

VISTA: la Ley núm. 340-06, sobre Compras y Contrataciones Públicas de Bienes, Servicios y Obras, promulgada en fecha dieciocho (18) del mes de agosto de dos mil seis (2006) y su posterior modificación contenida en la Ley núm. 449-06, de fecha seis (6) del mes de diciembre de dos mil seis (2006).

VISTO: la Resolución núm. 007/2019, que establece el Reglamento de Compras y Contrataciones del Poder Judicial establece que el Comité de Compras y Licitaciones de fecha dieciséis (16) de julio de dos mil diecinueve (2019).

VISTA: las certificaciones de apropiación presupuestaria números 1) PG- 24154 -2023, por un monto de ocho millones seiscientos mil pesos dominicanos con 00/100(RD$8,600,000.00) para *la Renovación de Licencias para Soluciones de Ciberseguridad de Fortinet*; 2) PG-24155-2023, por un monto de dos millones pesos dominicanos con 00/100 (RD$ 2,000,000.00) la *Renovación de Licencias del Sistema Integral de Inteligencia Artificial para la Ciberdefensa Darktrace.*; 3) PG-24152-2023, por un monto de seiscientos mil pesos dominicanos con 00/100 (RD$600,000.00) para la

Inicio del Expediente
PEEX-CPJ-06-2023

Renovación de Licencias para Solución de Gestión de Vulnerabilidades Tenable., todas de fecha siete (7) de febrero de dos mil veintitrés (2023).

VISTOS: las especificaciones técnicas de fecha nueve (9) de febrero de dos mil veintitrés (2023), elaborados por Dirección de Tecnologías de la Información y la Comunicación del Consejo del Poder Judicial.

VISTOS: los informes de justificación del uso de procedimiento de excepción por exclusividad para la: *adquisición de licencias para soluciones de ciberseguridad de fortinet, gestión de vulnerabilidades tenable.io y sistema integral de inteligencia artificial para la ciberdefensa darktrace,* de referencia núm. PEEX-CPJ-06-2023, *de* fecha nueve (9) febrero de dos mil veintitrés (2023), elaborado por la Dirección de Tecnologías de la Información y la Comunicación del Consejo del Poder Judicial.

VISTA: la recomendación de designación de peritos, de fecha dos (2) de marzo de dos mil veintitrés (2023), suscrita por el ingeniero **Welvis Beltrán Matos,** director de Tecnologías de la Información y la Comunicación del Consejo del Poder Judicial, donde recomienda a los señores: **Luis Joel Mejía Castillo,** analista Senior de Continuidad; **Adderli de la Rosa Suárez;** coordinador de Seguridad de Infraestructura; **Luis Vargas de la Cruz**, analista de Continuidad y **Emmanuel E. Tejada Lora,** gerente de Seguridad y Monitoreo TIC; todos pertenecientes a la Dirección de Tecnologías de la Información y la Comunicación del Consejo del Poder Judicial.

VISTOS: los requerimientos de solicitud de compra números DTIC-025, 026 y 027 de fecha tres (3) de marzo de dos mil veintitrés (2023).

VISTOS: los términos de referencia elaborados por la Gerencia de Compras del Consejo del Poder Judicial, de fecha catorce (14) de marzo de dos mil veintitrés (2023).

Por lo anteriormente expuesto, y vistos los documentos que forman parte del expediente, el Comité de Compras y Licitaciones, conforme a las atribuciones que le confiere la Resolución número 007/2019, de fecha dieciséis (16) de julio de dos mil diecinueve (2019), contentiva del Reglamento de Compras de Bienes y Contrataciones de Obras y Servicios del Poder Judicial y las demás normativa vigente en materia de contratación pública y derecho administrativo, por unanimidad de votos, decide adoptar las siguientes resoluciones:

Inicio del Expediente
PEEX-CPJ-06-2023

Resolución número uno (1):

ADMITE como válida la existencia del quórum reglamentario para sesionar en la presente reunión, conforme al artículo 8 del Reglamento de Compras de Bienes y Contrataciones de Obras y Servicios del Poder Judicial, el cual expresa lo siguiente: *"(…) con la asistencia de por lo menos cuatro (4) de sus miembros con voz y voto (…)".*

Resolución número dos (2):

AUTORIZA el procedimiento de selección de excepción por exclusividad correspondiente para la *adquisición de licencias para soluciones de ciberseguridad de Fortinet, gestión de vulnerabilidades Tenable.IO y sistema integral de inteligencia artificial para la ciberdefensa Darktrace.* de referencia núm. PEEX-CPJ-06 -2023.

Resolución número tres (3):

APRUEBA los documentos contentivos de las especificaciones técnicas de fecha nueve (9) de febrero de dos mil veintitrés (2023), elaboradas por: **Luis Joel Mejía Castillo,** analista Senior de Continuidad; **Adderli de la Rosa Suárez;** coordinador de Seguridad de Infraestructura, y **Emmanuel E. Tejada Lora,** gerente de Seguridad y Monitoreo TIC; todos pertenecientes a la Dirección de Tecnologías de la Información y la Comunicación del Consejo del Poder Judicial; y los términos de referencia elaborados por la Gerencia de Compras de fecha catorce (14) de marzo de dos mil veintitrés (2023), en el marco del procedimiento de excepción por exclusividad para *adquisición de licencias para soluciones de ciberseguridad de fortinet, gestión de vulnerabilidades tenable.io y sistema integral de inteligencia artificial para la ciberdefensa darktrace,* de referencia núm. PEEX-CPJ-06-2023.

Resolución número cuatro (4):

DESIGNA a los señores: **Luis Joel Mejía Castillo,** analista Senior de Continuidad; **Adderli de la Rosa Suárez;** coordinador de Seguridad de Infraestructura; **Luis Vargas de la Cruz**, analista de Continuidad y **Emmanuel E. Tejada Lora,** gerente de Seguridad y Monitoreo TIC como peritos para evaluar las ofertas correspondientes al procedimiento de excepción por exclusividad para *adquisición de licencias para soluciones de ciberseguridad de fortinet, gestión de vulnerabilidades tenable.io y sistema integral de inteligencia artificial para la ciberdefensa darktrace,* de referencia núm. PEEX-CPJ-06-2023.

Inicio del Expediente
PEEX-CPJ-06-2023

Resolución número cinco (5):

ORDENA a la Gerencia de Compras la publicación de la convocatoria, certificación de apropiación presupuestaria, el informe justificativo del uso del procedimiento de excepción por exclusividad, y los términos de referencia del presente procedimiento, en la página web del Poder Judicial www.poderjudicial.gob.do, además de cursar invitaciones a todos los oferentes que califiquen para ofrecer el servicio requerido.

La presente acta ha sido levantada en la ciudad de Santo Domingo, Distrito Nacional, el día catorce (14) de marzo de dos mil veintitrés (2023).

Firmada por: Bionni Biosnely Zayas Ledesma, consejera del Poder Judicial, presidenta del comité; **Vanesa María Camacho Melo,** coordinadora técnica; **Betty Esther Céspedes Torres**, gerente de control operativo; **Isnelda R. Guzmán de Jesús**, directora de planificación; **Alicia Angélica Tejada Castellanos,** directora administrativa; **Enmanuel Adolfo Moreta Fermín**, director legal; y **Yerina Reyes Carrazana**, gerente de Compras, como secretaria con voz, pero sin voto.