TÉRMINOS DE REFERENCIA

Denominación del Servicio	Servicio de Ethical Hacking para las Aplicaciones Informáticas y la Infraestructura Informática de la Junta Nacional de Justicia
Área Usuaria	Unidad de Monitoreo y Supervisión de Proyectos
Entidad Beneficiaria	Junta Nacional de Justicia
Meta	0001
Código Único de Inversión	2412541
Actividad del POI	AOI 01
Componente	Mayor Capacidad de la Plataforma Tecnológica
Sub Componente	Mejor Capacidad de la Infraestructura Tecnológica

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de Ethical Hacking para las aplicaciones informáticas y la infraestructura tecnológica de la Junta Nacional de Justicia, en el marco de la implementación del Expediente Judicial Electrónico – EJE" con CUI 2412541.

2. INTRODUCCIÓN

De acuerdo con la Ley Nº 30916, Ley Orgánica de la Junta Nacional de Justicia se establece que ésta es un organismo constitucionalmente autónomo cuya misión es "nombrar y ratificar a jueces y fiscales probos, idóneos y competentes, así como a los jefes de la ONPE y el RENIEC, y destituir a los que transgredan sus responsabilidades, a través de procesos justos y transparentes, contribuyendo al fortalecimiento de la administración de justicia y la institucionalidad democrática". Constituye un Pliego Presupuestario.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital - SGTD, viene impulsando el proceso de transformación digital en las entidades de la Administración Pública, orientado a un Gobierno Digital que genere valor público e impacte en la mejora de la atención de los ciudadanos y personas en general.

Mediante Decreto Legislativo N° 1412, se aprueba la Ley de Gobierno Digital, el cual define el concepto de Gobierno Digital como "el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación del valor público" y entre otros aspectos, establece "el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno", y, como finalidad establece "la mejora de la prestación y acceso de servicios digitales en condiciones interoperables, seguras, disponibles, escalables, ágiles, accesibles, y que faciliten la transparencia para el ciudadano y personas en general".

En tal sentido, a fin de asegurar dicha prestación de los servicios digitales de la entidad, es necesario contar aplicaciones informáticas robustas que sean resilientes a las amenazas que se presenten en el entorno.

3. ANTECEDENTES

Mediante Decreto Supremo N° 336-2019-EF de fecha 13 de noviembre de 2019, se aprueba la operación de endeudamiento externo entre la República del Perú y el Banco Internacional de Reconstrucción y Fomento – BIRF, hasta por la suma de US $ 85´000,000.00 (ochenta y cinco millones y 00/100 dólares americanos) destinada a financiar parcialmente el programa de inversión "Mejoramiento de los servicios de justicia no penales a través de la implementación del Expediente Judicial Electrónico (EJE)".

El 27 de noviembre de 2019 se firmó el Contrato Préstamo N° 8975/PE con el Banco Internacional de Reconstrucción y Fomento (BIRF) para financiar el Programa "Mejoramiento de los Servicios de Justicia no Penales a través de la implementación del Expediente Judicial Electrónico (EJE)", el mismo que está diseñado para mejorar la eficiencia, el acceso, la transparencia y la satisfacción del usuario en la entrega de los servicios de justicia no penales mediante la implementación del Expediente Judicial Electrónico en materia No Penal, para lo cual las entidades del Sistema de Administración de Justicia involucradas serían el Ministerio de Justicia y Derechos Humanos, el Poder Judicial, la Academia de la Magistratura, el Tribunal Constitucional y el Consejo Nacional de la Magistratura (hoy Junta Nacional de Justicia).

Cabe indicar que el Ministerio de Justicia y Derechos Humanos en su calidad de Prestatario, a través del Programa de Modernización del Sistema de Administración de Justicia (UE- MINJUSDH) ejecutará todas las intervenciones relacionadas al Ministerio de Justicia y Derechos Humanos (MINJUSDH), el Tribunal Constitucional (TC) y la Junta Nacional de Justicia (JNJ).

Con documento N° 001-2020-BM de fecha 12 de marzo de 2020, el Banco Mundial otorgó su No Objeción al Manual de Operaciones del Programa "Mejoramiento del Servicio de Justicia no Penales a través de la implementación del Expediente Judicial Electrónico (EJE)".

Mediante Resolución Ministerial N° 102-2020-JUS de fecha 4 de marzo de 2020, se aprobó el Manual de Operaciones del Programa 2413068 "Mejoramiento de los servicios de justicia no penales a través de la implementación del Expediente Judicial Electrónico (EJE)", donde se determina que el Programa de Modernización del Sistema de Administración de Justicia (UE- MINJUSDH) está encargado de ejecutar el Programa Mejoramiento del Servicio de Justicia No Penales a través de la implementación del Expediente Judicial Electrónico (EJE). En dicho Manual se encuentra tipificada la intervención de apoyo a la Junta Nacional de Justicia:

- Proporcionar apoyo a la JNJ para mejorar su modelo de gestión, procesos y sistemas de información para aumentar su eficiencia y transparencia y adaptarse mejor a la reforma del Sistema de Administración de Justicia incluyendo, entre otros: (a) el desarrollo de procesos de gestión para la operación eficiente, transparente y responsable de la JNJ; y (b) fortalecimiento de los sistemas de información de la JNJ para apoyar los nuevos procesos.

El PMSAJ tiene a su cargo la ejecución de tres (03) proyectos de inversión, además del componente de Gestión del Programa. Uno de ellos es el proyecto de inversión "Mejoramiento de los servicios de la Junta Nacional de Justicia- JNJ, en el marco de la

implementación del Expediente Judicial Electrónico" con CUI 2412541, el cual fue declarado viable el 30 de diciembre de 2020, proyecto que pertenece al programa citado anteriormente. El objetivo central del referido proyecto es lograr el Mejoramiento de los servicios de selección, ratificación y de procesos disciplinarios de jueces y fiscales de la JNJ en el marco de la implementación del EJE.

Dentro de dicho Proyecto 2412541, "Mejoramiento de los servicios de la Junta Nacional de Justicia – JNJ, en el marco de la implementación del Expediente Judicial Electrónico – EJE, distrito de San Isidro – Provincia de Lima – Departamento de Lima", se requiere ejecutar el presente servicio contemplado dentro del alcance previsto para la ejecución del componente segundo de dicho Proyecto "Mayor capacidad de la plataforma tecnológica", con la finalidad de realizar un diagnóstico de las amenazas y vulnerabilidades de las aplicaciones en producción a fin de definir las acciones necesarias para su mitigación así como considerar dicha información como insumo para los desarrollos futuros.

4. FINALIDAD PÚBLICA

Mediante la presente contratación, la Junta Nacional de Justicia (JNJ) identificará las vulnerabilidades que puedan afectar la entrega continua y segura de sus servicios digitales a los usuarios como parte de la ejecución de sus procesos institucionales. Dichos servicios son, principalmente, aplicaciones informáticas desarrolladas internamente en la institución ejecutándose en una infraestructura tecnológica propia, las cuales requieren ser evaluadas con cierta regularidad a fin de identificar amenazas y vulnerabilidades en su estructura que puedan ser aprovechadas para generar pérdida de información u otros efectos negativos en los activos de la entidad.

5. OBJETIVO DEL SERVICIO

5.1. Objetivo General

Contar con el servicio de Ethical Hacking para las aplicaciones informáticas de la extranet e intranet y la infraestructura tecnológica de la Junta Nacional de Justicia, con la finalidad de identificar brechas de seguridad existentes a partir del análisis de código fuente y de la configuración de la infraestructura tecnológica, a fin de establecer un plan de acción para su remediación y evaluar su eficacia.

5.2. Objetivos Específicos

5.2.1. Realizar un diagnóstico general de las arquitecturas de aplicaciones y plataforma tecnológica de la JNJ a fin de proponer la estrategia para la ejecución del servicio de Ethical Hacking.

5.2.2. Identificar las amenazas y vulnerabilidades que un atacante malicioso podría encontrar y explotar en las aplicaciones informáticas de la JNJ, en base a las pruebas realizadas.

5.2.3. Identificar las amenazas y vulnerabilidades que un atacante malicioso podría encontrar y explotar en la infraestructura tecnológica (servidores, equipos de seguridad, equipos de comunicaciones, entre otros) de la JNJ, en base a las pruebas realizadas.

5.2.4. Proponer las acciones necesarias específicas para fortalecer la seguridad de las aplicaciones informáticas y la infraestructura tecnológica analizadas, así como identificar los riesgos de su no implementación.

6. METODOLOGÍA

Las actividades del presente servicio serán ejecutadas bajo uno o más de los lineamientos siguientes: OWASP (Open Web Application Security Project), PTES (Penetration Testing Excecution Standard), OSSTMM (Open Source Security Test Methodology Manual), NIST SP 800-115 –Technical Guide to Information Security Testing and Assessment, ISSAFF (Information Systems Security Assessment Framework) y CVSS (Common Vulnerability Scoring System). La propuesta metodológica se presenta con el Plan de Trabajo.

7. ACTIVIDADES POR REALIZAR

En el presente servicio, se requiere que el proveedor realice las siguientes actividades:

7.1. Realizar el análisis inicial de la arquitectura de aplicaciones e infraestructura informática.

7.1.1. Realizar un diagnóstico inicial general de la arquitectura de aplicaciones informáticas de la JNJ y sus características (lenguajes de programación empleados, componentes de las aplicaciones, relaciones entre ellas, infraestructura relacionada, entre otros aspectos) y de los componentes de la infraestructura informática; desde el punto de vista de seguridad a fin de proponer la estrategia para la ejecución del servicio de Ethical Hacking que mejor se adapte a la situación actual.

Las aplicaciones informáticas (módulos) para analizar son:

1. Boletín Oficial de la Magistratura
2. Casilla de Notificaciones
3. Selección y Nombramiento para Jefes de la ANC
4. Ficha Única
5. Resoluciones JNJ
6. Página Web JNJ
7. Mesa de Partes Virtual

7.1.2. Realizar un diagnóstico sobre la infraestructura física y virtual del JNJ, en el cual se efectué el análisis de los servidores de la entidad de acuerdo con lo señalado en el anexo 2.

En los anexos del presente documento se describen las características relevantes de las aplicaciones informáticas y la infraestructura tecnológica.

7.2. Elaborar el Plan de Trabajo con base a la información recopilada en el diagnóstico, en el que establezcan los entregables a detalle, actividades a realizar, metodología de análisis de vulnerabilidades y seguridad a aplicar, alcance, plazos y riesgos del servicio.

7.3. Ejecutar los análisis y pruebas de seguridad pasivas y activas sobre las aplicaciones informáticas y la infraestructura tecnológica, las cuales incluirán, sin ser limitativas:

a. Pruebas de inteligencia de fuentes abiertas (se deberá realizar el descubrimiento de subdominios, IPs y servicios asociados por cada subdominio sin intentar buscar vulnerabilidades si no registrar la información que alguien puede encontrar públicamente sobre o acerca de los activos de la entidad y mapear la información que cada uno posee y que podría contribuir a una posible superficie de ataque).
b. Pruebas de gestión de configuración e implementación
c. Pruebas de gestión de identidad
d. Pruebas de autenticación
e. Pruebas de autorización
f. Pruebas de gestión de sesión
g. Pruebas de validación de ingreso
h. Pruebas de inyección NoSQL
i. Pruebas de manejo de errores
j. Pruebas para criptografía débil
k. Pruebas de lógica del negocio
l. Pruebas del punto de vista del cliente
m. Revisión del código fuente
n. Pruebas a nivel de la infraestructura (identificando debilidades en la red, sistemas operativos, software base que puedan ser explotadas, debidamente correlacionadas con el equipo al que hace referencia).
o. Se identificará cualquier deficiencia asociada a la seguridad en el diseño y la estructura de las aplicaciones, evaluando los niveles de seguridad existentes, incluyendo normas básicas de diseño y desarrollo de aplicaciones.

La ejecución de análisis de vulnerabilidades deberá comprender el uso de herramientas comerciales, comunitarias y open source de ser el caso, sin embargo, se requiere que para el caso de la herramienta para escaneo de vulnerabilidades automatizada se deberá considerar una herramienta comercial que incluya una base de datos actualizada de CVEs, así como la información para la mitigación del servicio vulnerable. Se deberá mostrar la evidencia del uso de esta herramienta comercial.

Asimismo, en caso se utilice herramientas gratuitas, estas, deberán ser compartidas con la JNJ como parte de la transferencia metodológica y posibilidad de replicación que ayude a la mitigación.

Se deberán combinar técnicas avanzadas de ataque como la simulación de adversarios, emulando un ataque real y en profundidad contra los activos que forman parte del alcance del servicio con el fin de verificar posibles vectores de ataque, así como comprobar y testear los controles de seguridad que tiene desplegados y hasta dónde podría llegar un eventual atacante.

La Metodología y buenas prácticas implementadas durante el desarrollo del servicio deben ser transferidas hacia la JNJ (de tal forma que el personal de la JNJ

pueda observar las tareas que se ejecuten como parte de la transferencia de conocimiento por parte del contratista).

7.4. Elaborar el informe detallado sobre los hallazgos (incluyendo evidencias) en base a la información obtenida de las pruebas, estimando el riesgo actual de las vulnerabilidades identificadas. Asimismo, se deberán evaluar las fortalezas y debilidades de los controles de seguridad existentes.

7.5. Identificar, caracterizar a detalle y priorizar las acciones necesarias para mitigar las vulnerabilidades identificadas, lo cual incluirá: nombre de la acción, alcance (entregables), plazo estimado, tareas a realizar por cada acción, recursos requeridos (personas, tecnología, normatividad, entre otros).

7.6. Reevaluar de las amenazas y vulnerabilidades luego de 06 meses de haber presentado las recomendaciones resultantes de la primera evaluación. Esta reevaluación debe culminar con la presentación de un informe técnico en el que se detallen las vulnerabilidades residuales y las acciones necesarias para su mitigación.

8. PERFIL DE LA FIRMA

8.1. El postor deberá acreditar:

- Ser persona jurídica.
- Permanencia en el mercado dedicándose a actividades de similar naturaleza de al menos cuatro (4) años mediante el acta de constitución o documento equivalente.
- Facturación no menor a S/ 350,000 (Trescientos Cincuenta Mil y 00/100 Soles) en la ejecución de servicios de Ethical Hacking, sea en la administración pública y/o en entidades privadas, en los últimos 06 años., cuya acreditación se realizará a través de la presentación de contratos y/u órdenes de servicios acompañadas de sus respectivas constancias de prestación de servicios, o en su defecto a la presentación de estas últimas.
- Estar inscrito y con vigencia en el Registro Nacional de Proveedores.
- No tener impedimento de ninguna índole para contratar con el Estado (presentar Declaración Jurada).
- Contar con RUC activo y habido.

9. PERFIL DEL PERSONAL CLAVE

El postor deberá acreditar el siguiente perfil del personal que ejecutará el servicio:

9.1. Un (01) Jefe de Proyecto

Formación académica:

- Profesional titulado en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería Industrial o Ingeniería de Computación o afines.

Cursos y/o especializaciones:

- Curso en dirección de proyectos, gestión de proyectos o afines.
- Curso en seguridad de la información o seguridad informática.

Experiencia laboral:

- Experiencia general mínima de tres (03) años en la administración pública o privada.
- Experiencia específica mínima de tres (03) servicios realizando actividades vinculadas a ciber seguridad.

9.2. Tres (03) Especialistas en Ethical Hacking

Formación académica:

- Profesional titulado o bachiller en Ingeniería de Sistemas, Informática, Industrial, Computación o afines.

Cursos y/o especializaciones:

- Cada especialista debe contar, como mínimo, con dos (02) de las siguientes certificaciones vigentes:

  - OSCP (Offensive Security Certified Professional)
  - OSCE (Offensive Security Certified Expert)
  - OSWE (Offensive Security Web Expert)
  - Certificación eLearnSecurity infraestructura: eJPT, eCPPT
  - Certificación eLearnSecurity aplicaciones web: eWPT, eWPTX
  - Certificación CEH: Certified Ethical Hacker
  - Certificación MILE2: Certified Penetration Testing Engineer
  - Certificación MILE2: Certified Secure Web Application Engineer
  - OSWP: Offensive Security Wireless Professional

Experiencia laboral:

- Experiencia general mínima de tres (03) años en la administración pública o privada.
- Experiencia de haber participado en mínimo tres (03) servicios realizando actividades de Ethical Hacking.

10. CONTENIDO, PLAZO Y PRESENTACIÓN DE LOS ENTREGABLES

10.1. Entregables

- Primer entregable: Informe que contenga lo vertido en los puntos 7.1 y 7.2 del presente TDR.
- Segundo entregable: Informe que contenga lo vertido en los puntos 7.3, 7.4 y 7.5 del presente TDR.
- Tercer entregable: Informe que contenga lo vertido en el punto 7.6.

10.2. Plazo y presentación de entregables

El plazo de ejecución del servicio será de **doscientos setenta (270) días calendario efectivos**, contados desde el día siguiente de la fecha de suscripción del contrato.

Entregable	Plazo
Primer Entregable	Hasta los treinta (30) días calendario desde el día siguiente de suscrito el contrato.
Segundo Entregable	Hasta los sesenta (60) días calendario contados desde la aprobación del primer entregable
Tercer Entregable	Hasta los ciento ochenta (180) días calendario contados desde la aprobación del segundo entregable

La Junta Nacional de Justicia tendrá un plazo máximo de diez (10) días calendario para evaluar, otorgar la conformidad u observar los entregables que sean presentados por la firma consultora. La firma consultora dispondrá de diez (10) días calendario contados desde el día siguiente de la notificación de dichas observaciones para levantar las observaciones formuladas.

La Junta Nacional de Justicia no podrá realizar nuevas observaciones al entregable revisado, en ese sentido, si hubiere más observaciones estas deben relacionarse con las observaciones anteriores remitidas, en ese caso la firma consultora dispondrá de un plazo no mayor a cinco (05) días calendario para su subsanación.

Los entregables deberán ser entregados en medios digitales (CD y/o USB con los archivos MS Excel, Word, formatos PDF y los que correspondan), presentados por mesa de partes de la UE 003-Programa de Modernización del Sistema de Administración de Justicia – PMSAJ, o a través de la mesa de partes digital de la Junta Nacional de Justicia, en archivos digitales de ser el caso, según convenga al estado de emergencia declarado por el Gobierno al momento de dichas circunstancias.

11. LUGAR DE LA EJECUCIÓN

La Ejecución del servicio se realizará en modalidad remota. En caso se requiera realizar coordinaciones presenciales, estas se llevarán a cabo en la ciudad de Lima, en las instalaciones de la Junta Nacional de Justicia sito en Paseo de la República 3285- San Isidro, para lo cual la firma deberá cumplir con los protocolos sanitarios y de bioseguridad de conformidad con la normativa vigente.

12. CONFORMIDAD DE LA PRESTACIÓN

La conformidad del servicio estará a cargo del Enlace Institucional del Programa en la Junta Nacional de Justicia, previo informe favorable de su Oficina General de Tecnologías de Información y Gobierno Digital.

Dicha conformidad de servicio y las aprobaciones de los entregables estarán referidas al cumplimiento de los aspectos técnicos y de la ejecución de las actividades señaladas en el presente.

13. COORDINACIÓN Y SUPERVISIÓN

La coordinación y supervisión de la prestación y ejecución del servicio, será llevada a cabo por los funcionarios que el Coordinador de Enlace de la JNJ designe.

La supervisión contractual será realizada por el Supervisor del Proyecto de la JNJ de la Unidad de Monitoreo y Supervisión de Proyectos del "Programa de Modernización del Sistema de Administración de Justicia para la Mejora de los Servicios brindados a la Población Peruana (PMSAJ)" en la UE-MINJUSDH, en coordinación con la entidad beneficiaria.

14. CONDICIONES DE PAGO

El pago del presente servicio se realizará en **tres (03) armadas**, previa revisión y aprobación del producto (entregable) en el plazo que se especifica en el punto 10.2 del presente documento.

Entregable	Porcentaje de pago
Primer Entregable	15 % del monto total del servicio
Segundo Entregable	60 % del monto total del servicio
Tercer Entregable	25 % del monto total del servicio

El pago del servicio se realizará previa entrega del informe conteniendo los entregables que correspondan contando con la respectiva conformidad del servicio, así como contra la presentación del comprobante de pago correspondiente. Asimismo, el abono respectivo se realizará en la cuenta bancaria proporcionada al momento de la firma del contrato.

El precio de la oferta incluye todos los tributos, seguros, transporte, inspecciones y, de ser el caso, los costos laborales conforme la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre el costo del servicio a contratar, excepto de aquellos postores que gocen de alguna exoneración legal, no incluirán en el precio de su oferta los tributos respectivos.

Requisitos para el pago:

- Copia simple del contrato.
- Copia del entregable, correspondiente al tramo, armada y/o etapa del servicio.
- Comprobante del pago.
- Autorización de depósito en cuenta (CCI).
- Conformidad de servicio.

15. ADELANTOS

La Entidad otorgará un (01) adelanto directo por el 25 % del monto del contrato original, previa presentación de la garantía correspondiente la misma que será equivalente al porcentaje a otorgar.

El contratista deberá solicitar el adelanto a través de mesa de partes ubicada en Jr. Roberto Ramírez del Villar (Ex Calle 32) Nro. 325 dentro de los siete (07) días calendario, contados desde el día siguiente de suscrito el contrato adjuntando a su solicitud la garantía por adelantos mediante carta fianza acompañada del comprobante de pago correspondiente. Vencido dicho plazo no procede la solicitud.

El PROGRAMA entregará el monto solicitado dentro de los ocho (08) días calendario siguientes a la presentación de la solicitud del contratista".

Los requisitos y condiciones para el otorgamiento de dicho Adelanto se ceñirán a lo estipulado en los numerales de los artículos 153 y 156 del Reglamento de la Ley de contrataciones del Estado.

16. FÓRMULA DE REAJUSTE

La presente contratación no considera la aplicación de fórmulas de reajuste.

17. CONFIDENCIALIDAD

La información y documentación a la que tendrá acceso tiene carácter de confidencialidad estando prohibido revelar dicha información a terceros. El proveedor deberá dar cumplimiento a todas las políticas y estándares definidos por la entidad en materia de seguridad de información, tanto de la información que se le entregue como la que genere durante la realización y a la conclusión de las actividades como informes, datos recopilados o recibidos.

18. OBLIGACIONES DE LAS PARTES

18.1. De la Entidad:

a. La JNJ, a través del Oficina de Tecnologías de la Información y Gobierno Digital, pondrá a disposición del proveedor toda la información y documentación disponible referente al objeto del servicio.
b. Gestionar la participación de los usuarios en las sesiones programadas.
c. Disponer de un coordinador del servicio a lo largo de la ejecución del proyecto.
d. Proporcionar al proveedor, la documentación de las políticas, procedimientos, modelos, estándares y lineamientos que sean relevantes a la ejecución del servicio, y que pueden variar durante el transcurso de este.

18.2. Del proveedor:

a. Desarrollar todas las actividades requeridas en los presentes términos de referencia.
b. Cumplir con todo lo establecido en los presentes términos de referencia, en su propuesta técnica y, en general, con lo estipulado en el contrato del servicio.
c. Cumplir con los entregables, plazos y cronogramas establecidos.
d. Cumplir con las políticas y procedimientos definidos por la JNJ.

19. PENALIDADES

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día

de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo en días}}$$

Donde F tiene los siguientes valores:

a) Para plazos menores o iguales a sesenta (60) días,
   Para bienes, servicios en general, consultorías y ejecución de obras: F = 0.40.
b) Para plazos mayores a sesenta (60) días:
   Para bienes, servicios en general y consultorías: F = 0.25.

Tanto el monto como el plazo se refieren, según corresponda, al contrato o ítem que debió ejecutarse o, en caso de que estos involucraran obligaciones de ejecución periódica, a la prestación parcial que fuera materia de retraso.

Para efectos del cálculo de la penalidad diaria se considera el monto del contrato vigente.

Se considera justificado el retraso, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. Esta calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.

ANEXO 1. INVENTARIO DE APLICACIONES INFORMÁTICAS INCLUIDAS EN EL ALCANCE DEL SERVICIO

Aplicaciones	¿Intranet o extranet?	Lenguaje de programación	Base de datos	¿Se cuenta con el código fuente?	¿Se cuenta con manual técnico?	¿Se cuenta con manual de usuario?	Tamaño de los archivos ejecutables
1. Boletín Oficial de la Magistratura	Ambos	PHP	Oracle	Sí	No	No	454 KB
2. Casilla de Notificaciones	Ambos	PHP	Oracle	Sí	No	No	373 KB
3. Selección y Nombramiento para Jefes de la ANC	Ambos	PHP	Oracle	Sí	Sí	Algunos módulos	5,23 MB*
4. Ficha Única	Ambos	PHP	Oracle	Sí	No	Sí	4,15 MB
5. Resoluciones JNJ	Ambos	PHP	Oracle	Sí	Sí	Sí	108 KB
6. Página Web JNJ	Ninguno	PHP	Oracle	Sí	No	Sí	9,57 MB
7. Mesa de Partes Virtual	Ambos	PHP	Oracle	Sí	Sí	Sí	353 KB

(*) Algunos Script usan APIs de librería que no han sido medidos en peso.
(**) Todas las aplicaciones son web.
(***) Las aplicaciones de intranet cuentan con un módulo común de autenticación. Las aplicaciones de extranet cuentan con un módulo de autenticación particular para cada uno.
(****) Todas las aplicaciones cuentan con los perfiles: Administrador, Usuario, Intranet (de corresponder), Extranet (de corresponder), Reporte y Consulta.

ANEXO 2. INVENTARIO DE LA INFRAESTRUCTURA TECNOLÓGICA INCLUIDA EN EL ALCANCE DEL SERVICIO

Tipo	Marca y modelo	Memoria y disco	Sistema operativo	Detalle
SERVIDOR	DELL R650	384/600	VmWare Esxi 7.0	Utilizado como ambiente de producción, soporte 87 máquinas virtuales con sistemas operativos Windows y Linux
SERVIDOR	DELL R650	384/600	VmWare Esxi 7.0	
SERVIDOR	DELL R650	384/600	VmWare Esxi 7.0	
SERVIDOR	DELL R650	384/600	VmWare Esxi 7.0	
SERVIDOR	DELL R640	256/600	Oracle Linux 7.9	Utilizado como servidores de base de datos en alta disponibilidad
SERVIDOR	DELL R640	256/600	Oracle Linux 7.9	
SERVIDOR	HP Proliant DL560 G8	256/300	Vmware esxi 5.1	Utilizado como ambientes de test/desarrollo
SERVIDOR	HP Proliant DL560 G8	256/300	Vmware esxi 5.1	
SERVIDOR	HP Proliant DL360 G9	64/4TB	Oracle Linux 7.9	Utilizado como base de datos de test
SERVIDOR	HP Proliant DL380	128/7.2TB	Vmware esxi 5.1	Servidores de Backup
SERVIDOR	HP Proliant DL380	128/7.2TB	Vmware esxi 5.1	Servidores de Backup
STORAGE	DELL	111TB	DELL Unity	Storage de almacenamiento
BACKUP	DELL	50TB	DELL	Copia de Seguridad de máquinas virtuales
STORAGE	NETAPP FAS 2240	45TB	ONTAP 8.1	Storage de almacenamiento de respaldo
Vmware	Vmware 7 standar	*	*	Se debe contemplar el análisis de seguridad de 30 servidores virtuales bajo plataforma vmware esxi 7, los sistemas operativos son Windows y Linux.