PROGRAMA MEJORAMIENTO DE LOS SERVICIOS DE JUSTICIA EN MATERIA PENAL EN EL PERÚ - PMSJMPP

Contrato de Préstamo N° 4959/OC-PE

TÉRMINOS DE REFERENCIA

SERVICIO DE HACKING ÉTICO PARA EVALUAR SISTEMAS DE INFORMACIÓN DEL INPE, PRONACEJ Y MINJUSDH

I. ANTECEDENTES

La República del Perú y el Banco Interamericano de Desarrollo (BID), suscribieron un acuerdo para una operación de endeudamiento externo, para financiar parcialmente el programa "Mejoramiento de los Servicios de Justicia en Materia Penal en el Perú" y que fue aprobada mediante Decreto Supremo N° 172-2020-EF. El financiamiento por parte del BID está sujeto a las disposiciones estipuladas en el "Contrato de Préstamo" y el "Manual de Operaciones del Programa".

El objetivo general del mencionado programa es la "Mejora de la gestión del servicio del Sistema de Administración de Justicia Penal", mediante:

(i) Aumento de la eficiencia del Sistema de Administración de Justicia Penal a través de Medios tecnológicos.
(ii) Aumento de la calidad de la investigación criminal.
(iii) Mejoramiento del acceso a los servicios de administración de justicia penal a través de medios tecnológicos.

Siendo las "Entidades Beneficiarias del Programa": El Ministerio de Justicia y Derechos Humanos (MINJUSDH), el Poder Judicial (PJ) y el Ministerio Público (MP); realizándose la ejecución del programa a través de las unidades ejecutoras del Ministerio de Justicia y Derechos Humanos (UE-MINJUSDH), del Ministerio Público (UE-MP) y del Poder Judicial (UE- PJ).

Para el caso del MINJUSDH, el Organismo Ejecutor es la Unidad Ejecutora del Programa (UEP) denominada "UE 005: Programa Mejoramiento de los Servicios de Justicia en Materia Penal en el Perú — PMSJMPP", ello de conformidad a lo previsto en el "Contrato de Préstamo" y en el "Manual de Operaciones del Programa" aprobado el 27 de enero del 2021 con Resolución N° 0017-2021-JUS.

El PMSJMPP tiene a su cargo la ejecución de un (01) proyecto de inversión, además del componente "Gestión del Programa"; denominándose dicho proyecto como "Mejoramiento de los servicios de información del MINJUSDH para la implementación de la interoperabilidad en materia penal" con CUI 2412557; cuyos beneficiarios son el MINJUSDH, INPE y PRONACEJ.

Para el caso de las entidades beneficiarias PRONACEJ, INPE y MINJUSDH, se llevará a cabo la implementación de sistemas lo cual permitirá la centralización y disponibilidad del servicio en cada una de sus sedes.

En ese marco, dada la sensibilidad de la información manejada en el ámbito penal, es de suma importancia salvaguardar la seguridad y protección de los datos involucrados. Por ello, es necesaria realizar el servicio de Hacking Ético. Este proceso permitirá llevar a cabo una evaluación exhaustiva al Sistema integral de Gestión de Adolescentes

Infractores (PRONACEJ), Sistema integral de Gestión Penitenciaria (INPE), Sistema de Gestión Defensorial y Sistema de Gestión de Extradiciones, Traslados de Personas Condenadas y Revocatorias de Extradiciones (MINJUSDH), asegurando la robustez de las medidas de seguridad implementadas. Además, se buscará detectar posibles vulnerabilidades que puedan comprometer la confidencialidad de la información.

II. OBJETIVO

Contratar a una persona jurídica que brinde el "SERVICIO DE HACKING ÉTICO PARA EVALUAR SISTEMAS DE INFORMACIÓN DEL INPE, PRONACEJ Y MINJUSDH", con la finalidad de garantizar la integridad y confidencialidad de la información en el ámbito penal relacionada con el Sistema Integral de Gestión de Adolescentes Infractores del PRONACEJ, Sistema Integral de Gestión Penitenciaria del INPE, Sistema de Gestión Defensorial y Sistema de Gestión de Extradiciones, Traslado de Personas Condenadas y Revocatorias de Extradiciones del MINJUSDH, beneficiarias del "Programa Mejoramiento de los Servicios de Justicia en Materia Penal del Perú - PMSJMPP".

III. ALCANCE

El servicio que se desea contratar implica la realización de un análisis de seguridad ética a nivel de infraestructura y aplicaciones web. Este análisis conocido como Hacking Ético, se llevará con el enfoque de pruebas de seguridad "Black Box", centrándose en la evaluación externa de la seguridad de los sistemas.

Para ello, se debe tener en cuenta que el servicio abarcará las siguientes actividades:

1. Hacking Infraestructura Externa

N°	DESCRIPCIÓN	PRONACEJ	INPE	MINJUSDH
1	Evaluar Infraestructura Externa	1 Unidad	1 Unidad	2 Unidad

2. Hacking a aplicación de web Externa

N°	DESCRIPCIÓN	PRONACEJ	INPE	MINJUSDH
2	Aplicaciones web	1 Sistema	1 Sistema	2 Sistema

3. Capacitación

N°	DESCRIPCIÓN	PRONACEJ	INPE	MINJUSDH
3	Taller de hacking ético	8 horas	8 horas	8 horas

El servicio no implica la corrección de los descubrimientos por parte del **CONTRATISTA**; no obstante, el **CONTRATISTA** deberá proporcionar la información requerida para llevar a cabo dicha corrección.

IV. ACTIVIDADES A REALIZAR

El servicio deberá contemplar las siguientes actividades, las cuales deben ser idénticas para las entidades PRONACEJ, INPE Y MINUDSH. Dichas actividades se detallan a continuación:

1. REALIZAR UN PLAN DE TRABAJO Y CRONOGRAMA – ACTIVIDADES

- El **CONTRATISTA**, tendrá hasta 5 días calendarios a partir del primer día hábil siguiente de suscrito el contrato o notificación de la orden de servicio, para realizar una reunión de inicio (Kick Off), en el cual presentará y se revisará el Plan de trabajo que incluya el cronograma de actividades, herramientas informáticas y/o metodologías a utilizar, formatos de entrega ,organización del equipo de trabajo, las mismas que serán aprobadas por la Jefatura de la Sub-Unidad de tecnologías de la información del PRONACEJ, la Jefatura de la Oficina de Sistemas de Información del INPE, la Jefatura de la Oficina General de Tecnologías de información del MINJUSDH y el Supervisor de tecnologías de Información del Programa de Mejoramiento de los Servicios de Justifica en Materia Penal - PMSJMPP.

- El **CONTRATISTA** deberá solicitar los permisos necesarios al PMSJMPP, en marco al Plan de Trabajo aprobado, para acceder a los Centro de Datos de acuerdo a la Tabla N°1. que son necesarios para las pruebas internas.

N°	Centro de Datos (Sedes)	Dirección
1	Sede Central PRONACEJ	Av. Arequipa N° 2407 - Lince
		Calle Conde N° 232 - Lince
2	Sede Central del INPE	Jirón Carabaya 456, Cercado de Lima
3	Sede Central MINJUSDH	Calle Scipión Llona N° 350, Miraflores.

Tabla 1 Ubicación de Centro de Datos

- El **CONTRATISTA** para la ejecución de las actividades a realizar, deberá coordinar con los supervisores de las entidades beneficiarias PRONACEJ, INPE Y MINJUSDH y el supervisor de Tecnologías de Información del PMSJMPP.

- El **CONTRATISTA** tiene la responsabilidad de proporcionar recomendaciones esenciales que las unidades de tecnología de información de las entidades beneficiarias deben considerar antes de la ejecución del servicio.

2. EVALUAR LA SEGURIDAD DE LA INFRAESTRUCTURA EXTERNA

Se trata de un servicio de pruebas de penetración desde la red externa a la infraestructura de los sistemas de información de las 3 entidades beneficiarias, para identificar vulnerabilidades y realizar recomendaciones. La metodología de Hacking ético a aplicar para la verificación de la seguridad de la infraestructura se centrará en la evaluación de controles de autenticación, configuración segura y aplicación de parches a nivel del sistema operativo, servicios de red y base de datos.
Como producto del servicio, se obtendrán las vulnerabilidades de la infraestructura clasificadas según su nivel de riesgo, las cuales estarán

acompañadas con procedimientos o recomendaciones para su mitigación.

El **CONTRATISTA** como mínimo debe realizar lo siguiente:

2.1 Reconocimiento de objetivos:

- Obtención de información DNS.
- Búsquedas de URLs internas u ocultas de los sistemas a evaluar y extracción de información.
- Evaluar el manejo del aumento significativo en la carga de trabajo o el número de usuarios concurrentes.

2.2 Exploración

- Exploración de protocolos que se ejecutan sobre en la red IP.
- Exploración de puertos: syn scan, ack scan, UDP scan, xmas scan, fin scan, null scan, RPC scan, idle scan.
- Identificación de servicios y obtención de banners.
- Identificación de sistemas operativos utilizando técnicas activas de estímulo/respuesta.

2.3 Identificación de vulnerabilidades a nivel de sistema operativo

- Enumeración de recursos de sistemas operativos de cada entidad beneficiaria con showmount y rpcinfo o equivalente para enumerar recursos compartidos.
- Enumeración de recursos de sistemas operativos mediante sesiones nulas.
- Verificación de configuraciones inseguras.
- Identificación de parches no aplicados.

2.4 Identificación de vulnerabilidades a nivel de servicios

- Identificación de servicios mediante captura de banners.
- Identificación de servidores HTTP.
- Verificación de configuraciones inseguras.
- Identificación de parches no aplicados.
- Identificación de todos los puntos finales (endpoints) expuestos por cada microservicio y validar la existencia de posibles puntos de entrada no autorizados.
- Identificar la versión de los servicios y verificada que estén actualizadas y parcheadas contra vulnerabilidades conocidas.
- Realizar pruebas de inyección (SQL, Comandos) para evaluar la resistencia de los microservicios a ataques de este tipo.
- Realizar escaneo de vulnerabilidades automatizadas para identificar debilidades en el código y configuraciones.
- Evaluar el manejo de errores y excepciones para asegurar no revelar información sensible en las respuestas.
- Evaluar la resistencia de los microservicios frente a ataques de denegación de servicio y recomendar medidas de mitigación.

2.5 Verificación de vulnerabilidades

- Verificación de vulnerabilidades mediante la explotación de la mismas utilizando herramientas propietarias y de fuente de libre disponibilidad como Metasploit Framework, Exploit-DB e Inject0r, u otros.

2.6 Obtención de Acceso

- Obtención de acceso shell al servidor mediante la explotación de vulnerabilidades.

- Creación de cuentas de usuario en el sistema operativo o servicio atacado.

2.7 Post Explotación

- Obtención de credenciales de acceso de personal de las entidades beneficiarias.

3. EVALUAR LA SEGURIDAD DE LAS APLICACIONES WEB

La metodología para llevar a cabo la auditoría de seguridad en aplicaciones mediante Hacking ético se enfocará en la evaluación de los controles empleados para autenticación, gestión de sesiones y validación de datos de entrada. Además, se detectarán posibles problemas relacionados con la configuración, la transmisión no segura de datos y la revelación de información sensible.

El test de las aplicaciones web accesibles desde internet se realizará de manera externa. Todas las evaluaciones realizadas en las aplicaciones seguirán el enfoque Black Box.

El servicio de ethical hacking se enfocará en analizar diversos aspectos de los sistemas mencionados, garantizando su seguridad y óptimo funcionamiento. Los aspectos a ser revisados incluyen, pero no se limitan a, la autenticación, autorización, registros/actualización de archivos, uso de APIs externas, entre otros.

Los sistemas a evaluar son los siguientes:

N°	DESCRIPCIÓN	BENEFICIARIA
1	Sistema Integral de Gestión Penitenciaria	INPE
2	Sistema Integral de Gestión de Adolescentes Infractores	PRONACEJ
3	Sistema de Gestión de Extradiciones, Traslado de Personas Condenadas y Revocatoria de Extradiciones del MINJUSDH.	MINJUSDH
4	Sistema de Gestión Defensorial	MINJUSDH

Tabla 2 Sistemas a evaluar

Estos sistemas son vitales para gestionar de manera óptima, segura y veraz toda la información relacionada con los procesos penales.
Como resultado de la evaluación, se buscará identificar vulnerabilidades en la aplicación web, clasificándolas según su nivel de riesgo. Se proporcionarán recomendaciones aplicables para mitigar dichas vulnerabilidades.

La metodología cubrirá como mínimo los aspectos recomendados por el Top Ten del OWASP (2021)

El **CONTRATISTA** como mínimo debe realizar lo siguiente:

3.1. Mapeo de Contenido

- Exploración de contenido visible y oculto.
- Exploración de rutas predeterminadas.
- Búsqueda de recursos públicos.

3.2. Análisis de Aplicación

- Identificación de funcionalidades.

- Identificación de puntos de entrada de datos.
- Identificación de parámetros de depuración.
- Identificación de tecnologías client-side y server-side.

3.3. Verificación de Controles Client-Side

- Aplicación de pruebas sobre campos ocultos, cookies y parámetros preestablecidos.
- Aplicación de pruebas sobre controles de seguridad aplicados a la entrada de usuario.
- Aplicación de pruebas sobre controles de seguridad basados en componentes.

3.4. Verificación de los Mecanismos de Autenticación

- Identificación de los mecanismos de autenticación.
- Pruebas de la calidad de contraseñas
- Pruebas de enumeración de cuentas de usuario.
- Pruebas de recuperación de contraseñas.
- Pruebas de funcionalidades de fijación de usuarios.
- Pruebas de suplantación de usuarios.
- Análisis de credenciales generadas automáticamente.
- Verificación de transmisión y distribución insegura de credenciales.

3.5. Verificación de la Validación de Datos de Entrada

- Pruebas de inyección SQL.
- Pruebas de cross-site-scripting (inyección HTML/JavaScript).
- Pruebas de inyección de comandos de S.O.
- Pruebas de recorridos de rutas (path traversal).
- Pruebas de inyección de scripts.
- Pruebas de inclusión de archivos.
- Pruebas de inyección SOAP, LDAP y XPATH.

4. REEVALUAR LA SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

El **CONTRATISTA** deberá realizar una revisión de la seguridad de los sistemas informáticos después de 30 días de haber concluido con el primer producto en cada entidad beneficiaria. Este seguimiento tiene como objetivo evaluar la efectividad de las medidas correctivas implementadas.

Las actividades a llevar a cabo incluirán, pero no se limitarán a:

- Realizar nuevamente las actividades mencionadas en la infraestructura externa y aplicaciones web externas (puntos 2 y 3), con el objetivo de verificar la resolución de hallazgos previos y detectar nuevos posibles.
- Realizar recomendaciones para subsanar los hallazgos.
- Detallar los comandos y /o herramientas empleadas durante la verificación y explotación de las vulnerabilidades informadas, indicándolos dentro del informe correspondiente a cada vulnerabilidad.
- Presentar informes generados por las herramientas, junto con evidencias, notas de sesión, documentos y programas utilizados en el proceso.

5. TALLER DE HACKING ÉTICO

El **CONTRATISTA** debe de llevar a cabo capacitaciones, así como de proporcionar manuales y guías prácticas orientadas a la formación en seguridad de la información. Además, estas sesiones deben ser grabadas, lo que permitirá a los colaboradores de las entidades beneficiarias descargarlas posteriormente para su revisión y referencia.

Estas sesiones deben destacarse por su enfoque didáctico y práctico, centrándose en la protección de los recursos de información. Se abordarán las mejores prácticas en ciberseguridad y seguridad de la información, asegurando así la custodia y una protección efectiva de los recursos informáticos.

Las capacitaciones tendrán una duración mínima de 8 horas, distribuidas en 4 sesiones de 2 horas cada una. La cantidad de personal que asistirá será determinada según el siguiente cuadro:

DESCRIPCIÓN	PRONACEJ	INPE	MINJUSDH
Capacitación	6	6	6

Además, como parte de la capacitación el CONTRATISTA deberá realizar actividades de apoyo al personal de las oficinas de tecnologías de la información de cada entidad beneficiaria durante la ejecución del levantamiento de vulnerabilidades identificadas.

6. CONSIDERACIONES ADICIONALES:

Dado que el Hacking ético utiliza herramientas automatizadas para descubrir posibles vulnerabilidades, es posible que algunas de estas se clasifiquen como "falsos positivos", es decir, identificaciones de vulnerabilidades que no son genuinas. Por lo tanto, es necesario verificar estas identificaciones de manera adicional:

El **CONTRATISTA** como mínimo debe realizar lo siguiente:

- ✔ La comprobación adicional se realizará mediante el uso de herramientas especializadas que permitan interceptar el tráfico, analizarlo e incluso modificarlo y aplicar técnicas de ataques comunes y fuzzing (alteración de información respecto a los protocolos y mecanismos utilizados).
- ✔ También, se deben utilizar técnicas de ataque de forma manual mediante ingreso por teclado o scripts.
- ✔ Asimismo, dicha comprobación adicional deberá permitir encontrar “falsos negativos”, es decir, vulnerabilidades que no fueron descubiertas por las herramientas automatizadas.

Las Pruebas deben considerar lo siguiente:

- ✔ Penetrar los sistemas externos descritos en la tabla 2 publicados en internet.
- ✔ Denegación de servicio distribuido, en un horario permitido y que no afecte la disponibilidad de los servicios.
- ✔ Ataques a servicios web, bases de datos, etc. que se encuentren en ejecución en las IP seleccionadas para esta evaluación.

Para la evaluación de las aplicaciones web, se considerará específicamente cumplir con los siguientes Criterios de Aplicación Segura, los cuales determinan que una aplicación es considerada segura sí:

- ✔ Está protegida contra ataques populares que incluyen, pero, no se limita a los documentados por el Top Ten del OWASP e ISECOM.
- ✔ Cuenta con mecanismos de defensa para protegerse del "perfil de amenazas" definidas como pueden ser accesos no autorizados, destrucción, divulgación, modificación y/o denegación de servicios
- ✔ Protege los datos sensibles mientras se están transmitiendo
- ✔ Almacena los passwords de forma segura.
- ✔ Protege los passwords de ataques de diccionario.
- ✔ Protege las "preguntas secretas" de ataques de "adivinación".
- ✔ Protege los archivos de configuración y del listado de directorios.
- ✔ No almacena datos sensibles en el cliente.
- ✔ No oculta datos sensibles en las páginas web.
- ✔ No muestra datos sensibles en los mensajes de error.
- ✔ Usa algoritmos de encriptación fuertes y conocidos.
- ✔ Utiliza ofuscación para la información sensible en el código de programas que se ejecuta en los clientes (Javascript, ActiveX, applets).
- ✔ Establece un tiempo máximo de inactividad de sesión.
- ✔ Se requiere una nueva autenticación después de haber terminado una sesión.
- ✔ Advierte los problemas de seguridad sí se entregan opciones como "Recordarme".
- ✔ Se requieren los passwords actuales antes de un cambio en los mismos.
- ✔ No se envía datos sensibles en requerimientos a sitios externos.
- ✔ Utiliza tokens aleatorios para mantener un control sobre las sesiones autenticadas (como cookies).
- ✔ Cuenta con un acceso filtrado.
- ✔ No mantiene aplicaciones de ejemplo ni de pruebas. ↔ No entrega datos sensibles en el programa fuente.

V. REQUISITOS DE CALIFICACIÓN

El **CONTRATISTA**, debe estar habilitado para contratar con el estado peruano.

El **CONTRATISTA**, debe tener en los últimos cinco (5) años, experiencia mínima de cinco (05) de servicios iguales o similares al objeto de la contratación. Se considera similares a los siguientes:

- Servicios de Seguridad Perimetral.
- Servicios de Sistema de Protección de Intrusos.
- Servicios de Sistema de Detección de Intrusos.
- Servicios de Firewall de Aplicación Web.
- Servicio de Correlación de Eventos (SIEM).
- Servicio de Monitoreo de Incidentes de Seguridad Informática.
- Servicios de Seguridad Informática.

- Servicio de Centro de Operaciones de Seguridad (SOC).
- Servicio de Penetración Test. - Servicio de Ethical Hacking (EH).
- Servicio de Evaluación o Análisis de Vulnerabilidades.

PERSONAL CLAVE

EL CONTRATISTA deberá contar con el personal que cumpla con las siguientes condiciones:

❖ **Coordinador del Servicio**
- Profesional técnico y/o universitario.
- Experiencia mínima de tres (03) de servicios iguales o similares al objeto de la contratación, en los últimos 5 años.

✔ Las responsabilidades del Coordinador del Servicio, como mínimo, son los siguientes:
- Será el principal responsable de la correcta y segura ejecución del servicio.
- Planificar y organizar la ejecución del servicio.
- Realizar las coordinaciones y comunicación correspondientes.
- Administrar los recursos propios y de terceros asignados para la ejecución del servicio.

❖ **Especialista de la Implementación del Servicio**
- Profesional técnico y/o universitario, en informática, electrónica, sistemas, telecomunicaciones y/o afines.
- Experiencia mínima de tres (03) de servicios iguales o similares al objeto de la contratación, en los últimos 5 años

✔ Las responsabilidades del Especialista de la Implementación, como mínimo, son los siguientes:
- Comprender a fondo el alcance del servicio de ethical hacking, incluyendo los sistemas, aplicaciones, redes y objetivos que serán evaluados.
- Preparar y configurar el entorno de pruebas, asegurando que las herramientas y plataformas necesarias estén operativas y listas para el ataque simulado.
- Emplear una variedad de herramientas de hacking ético (escáneres de vulnerabilidades, frameworks de explotación, herramientas de análisis de red, etc.) para identificar debilidades de seguridad.
- Documentar meticulosamente cada vulnerabilidad encontrada, incluyendo capturas de pantalla, logs, y cualquier otra evidencia que demuestre la existencia y el impacto de la debilidad.
- Ejecutar pruebas de penetración para explotar vulnerabilidades y evaluar el nivel de acceso o impacto que un atacante real podría lograr.
- Analizar los resultados de las pruebas para determinar la severidad y el riesgo de cada vulnerabilidad.

- Presentar los hallazgos al cliente de manera comprensible, explicando los riesgos de seguridad y las soluciones propuestas

El equipo de trabajo propuesto deberá participar en todas las etapas de la ejecución del servicio. Cualquier modificación del equipo de trabajo deberá ser notificada con 5 días de anticipación al EJE Penal, previa autorización del supervisor de cada entidad beneficiaria. El reemplazo deberá contar con el perfil de los requisitos mínimos solicitados en los puntos anteriores y ser aprobado por el supervisor de cada entidad beneficiaria.

VII. PRODUCTO/ENTREGABLE

El CONTRATISTA presentará dos (02) producto/entregable por cada entidad beneficiaria (PRONACEJ, INPE, MINJUSDH), según el siguiente detalle:

ETAPAS DEL SERVICIO	PRODUCTO/ENTREGABLE	PLAZO
ETAPA 01	**PRIMER PRODUCTO/ENTREGABLE:** Contiene la siguiente documentación: ✔ Niveles de seguridad, criterios de clasificación, accesos encontrados, y resumen de vulnerabilidades. ✔ Priorización de las acciones correctivas y recomendaciones. ✔ Hallazgos y recomendaciones de seguridad. ✔ Listado de comandos y/o herramientas utilizadas durante la comprobación, explotación de las vulnerabilidades reportadas y dentro del reporte de cada vulnerabilidad. ✔ Recomendaciones para el aseguramiento (hardening) de los dispositivos evaluados. ✔ Reportes de las herramientas, evidencias, notas de sesión, documentos y programas utilizados por los consultores.	Hasta quince (15) días calendario a partir del día siguiente hábil a la comunicación de inicio de actividades.
ETAPA 02	**SEGUNDO PRODUCTO/ENTREGABLE:** Informe técnico conteniendo el siguiente detalle: ✔ Hallazgos subsanados respecto al primer informe y nuevos hallazgos identificados en esta etapa. ✔ Niveles de seguridad, criterios de clasificación, accesos encontrados, y resumen de vulnerabilidades. ✔ Priorización de las acciones correctivas y recomendaciones. ✔ Hallazgos y recomendaciones de seguridad. ✔ Listado de comandos y/o herramientas utilizadas durante la comprobación,	Hasta treinta (30) días calendario a partir del día siguiente hábil de haber concluido con el producto/entregable de la Etapa 01.

ETAPAS DEL SERVICIO	PRODUCTO/ENTREGABLE	PLAZO
	explotación de las vulnerabilidades reportadas y dentro del reporte de cada vulnerabilidad. ✔ Recomendaciones para el aseguramiento (hardening) de los dispositivos evaluados. ✔ Reportes de las herramientas, evidencias, notas de sesión, documentos y programas utilizados por los consultores.	

VIII. SEGUIMIENTO Y SUPERVISIÓN

La supervisión y seguimiento de la ejecución del Contrato estará a cargo de la la Jefatura de la Sub-Unidad de tecnologías de la información del PRONACEJ, la Jefatura de la Oficina de Sistemas de Información del INPE, la Jefatura de la Oficina General de Tecnologías de información del MINJUSDH y el Supervisor de Tecnologías de Información para el PMSJMPP.

IX. PLAZO DE EJECUCIÓN Y FORMA DE PAGO

El pago se realizará en dos (02) armadas (correspondiente al segundo y tercer entregable), según el siguiente detalle:

PRODUCTO/ENTREGABLE	PLAZO MÁXIMO	PAGO
PRIMER PRODUCTO/ENTREGABLE	Hasta quince (15) días calendario a partir del día siguiente hábil a la comunicación de inicio de actividades.	50% del monto total
SEGUNDO PRODUCTO/ENTREGABLE:	Hasta treinta (30) días calendario a partir del día siguiente hábil de haber concluido con el producto/entregable de la Etapa 01	50% del monto total

Asimismo, el pago se efectuará a la presentación del Producto/Entregable y emisión del comprobante de pago dirigido a la Unidad Ejecutora UE 005: Programa Mejoramiento de los Servicios de Justicia en Materia Penal en el Perú — PMSJMPP y previa conformidad de acuerdo con lo establecido en el punto XI.

X. LUGAR DE EJECUCIÓN

De acuerdo con la naturaleza del servicio, la prestación del servicio se ejecutará en las instalaciones coordinadas por le entidad Contratante.

XI. CONFORMIDAD

La conformidad del servicio será emitida por la Supervisión de Sistemas de la Información del PMSJMPP previo informe técnico del/la supervisor/a designado/a,

que estará facultado a exigir al proveedor la aplicación y cumplimiento de las especificaciones técnicas mínimas establecidas.

En caso de existir observaciones, el Supervisión de Sistemas de la Información del PMSJMPP, gestionará la notificación al contratista; cuando se considere que no se han subsanado las observaciones, se podrá reiterar hasta en dos ocasiones, de otro modo se aplicará la penalidad correspondiente. Los plazos para reiterar las observaciones son las siguientes:

ENVÍO	PLAZO PARA COMUNICAR LAS OBSERVACIONES AL CONTRATISTA	PARA PRESENTAR SUBSANACIÓN DE OBSERVACIONES
Observaciones	No mayor de 10 días calendarios de recibido el producto.	No mayor a diez (10) días calendarios.
Primera reiteración de observaciones	No mayor de 05 días calendarios de haber recibido la primera subsanación de observaciones.	No mayor a cinco (05) días calendario.
Segunda reiteración de observaciones.	No mayor de 05 días calendarios de haber recibido la segunda subsanación de observaciones.	No mayor a cinco (05) días calendario.

XII. CONFIDENCIALIDAD Y PROPIEDAD INTELECTUAL

La información y documentación a la que tendrá acceso tiene carácter de confidencial siendo prohibido revelar dicha información a terceros. El CONTRATISTA 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 entrega como la que genere durante la realización y a la conclusión de las actividades como informes, datos recopilados o recibidos. Todos los entregables elaborados dentro del contrato son de propiedad exclusiva de la Entidad, por lo que el contratista no podrá hacer uso de los mismos en forma total o parcial, fuera de la Entidad.

XIII. OBLIGACIONES DEL PMSJMPP

Proporcionar las facilidades necesarias, información y documentación pertinente requerida por el CONTRATISTA para el cumplimiento de sus actividades.

XIV. RESPONSABILIDAD DEL CONTRATISTA

El CONTRATISTA será responsable por la calidad ofrecida y por los vicios ocultos del servicio, prestaciones y demás componentes de la contratación, por un plazo de un (01) año contado a partir de la conformidad por el cumplimiento de los aspectos técnicos y de la ejecución de las actividades del servicio, según lo indicado en los presentes términos de referencia. Dicha conformidad no enerva el derecho a reclamar posteriormente por defectos y/o vicios ocultos.

XV. PENALIDADES

Si el CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, el Programa le aplicará automáticamente una penalidad por cada día de atraso, hasta por un monto máximo equivalente al diez

por ciento (10%) del monto de la contratación vigente o, de ser el caso, del monto del ítem que debió ejecutarse.

En todos los casos, la penalidad se aplicará automáticamente y se calculará de acuerdo con la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

Donde:

F = 0.40 para plazos menores o iguales a sesenta (60) días o;

F = 0.25 para plazos mayores a sesenta (60) días;

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 presentación parcial que fuera materia de retraso.

Para efectos 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. La calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado.

Finalmente, se cuenta con el derecho de exigir, además de la penalidad, el cumplimiento de la obligación.