

## TERMINOS DE REFERENCIA

### “Servicio de consultoría para la identificación y evaluación de vulnerabilidades y brechas existentes en los controles de seguridad de los sistemas y activos de información críticos de la SUNAT”

#### DENOMINACION DE LA CONTRATACIÓN

#### Descripción del proceso

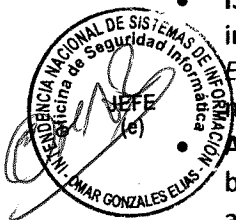
Servicio de consultoría especializada para la identificación y evaluación de vulnerabilidades de seguridad existentes en sistemas informáticos críticos de la SUNAT, así como para la identificación y evaluación de brechas existentes en los controles de seguridad de activos de información críticos de la entidad, con respecto a los controles establecidos en el Anexo A de la NTP-ISO/IEC 27001:2014.

#### Descripción del ITEM

Item	Descripción	Cantidad
1	Identificación e inventario de los activos de información relacionados con diez (10) sistemas informáticos críticos.	1
	Identificación y evaluación de brechas existentes en los controles de seguridad de los activos de información previamente identificados, con respecto a la Norma ISO/IEC 27001:2014.	1
	Identificación y evaluación de vulnerabilidades existentes en diez (10) sistemas informáticos críticos, mediante la ejecución de pruebas de penetración o “ethical hacking”.	1

#### DEFINICIONES

- **ISO/IEC 27001:** Estándar para la seguridad de la información aprobado y publicado como estándar internacional por la *International Organization for Standardization* y por la comisión *International Electrotechnical Commission*. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI).
- **ACTIVOS DE INFORMACION:** Elementos que contienen o manipulan información, como archivos, bases de datos, aplicaciones, equipos informáticos, etc, para los cuales se deben garantizar niveles adecuados de disponibilidad, integridad y confidencialidad.
- **ETHICAL HACKING:** Conjunto de técnicas de ataque o penetración con el fin de encontrar fallas o vulnerabilidades de seguridad en los sistemas informáticos de una entidad, con su autorización previa, para mejorar la seguridad de los mismos.



- **PRUEBAS DE CAJA NEGRA:** Pruebas de penetración en las cuales los ejecutores de las mismas no tienen conocimiento del funcionamiento del sistema a atacar y trabajan con la información que pueden conseguir por sus propios medios, del mismo modo que lo haría un delincuente informático.
- **PRUEBAS DE CAJA BLANCA:** Pruebas de penetración en las cuales los ejecutores de las mismas tienen conocimiento del funcionamiento interno del sistema a atacar y trabajan con la información a la que puede tener acceso uno o varios empleados de la organización.
- **FIRMA CONSULTORA:** Postor a quien se ha adjudicado la Buena Pro del presente proceso y suscribe el contrato.
- **SUNAT:** Superintendencia Nacional de Aduanas y de Administración Tributaria.
- **INSI:** Intendencia Nacional de Sistemas de Información.
- **GOSU:** Gerencia de Operaciones y Soporte a Usuarios, perteneciente a la INSI.

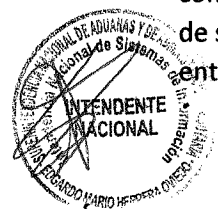
## FINALIDAD PÚBLICA

El presente proceso de selección busca contar con una consultoría especializada para obtener información relevante sobre la situación actual de los procesos y controles de seguridad de información de la SUNAT, respecto a los requisitos que establece la NTP-ISO/IEC 27001:2014, y para identificar y evaluar las vulnerabilidades de los sistemas informáticos críticos, a fin de elevar y fortalecer los niveles de seguridad de los servicios que la SUNAT brinda a los contribuyentes.

## ANTECEDENTES

La SUNAT tiene la misión de servir al país proporcionando los recursos necesarios para la sostenibilidad fiscal y la estabilidad macroeconómica. En ese contexto, la administración tiene como prioridad maximizar el cumplimiento tributario, o minimizar las brechas de incumplimiento, manteniendo la confianza en el sistema tributario y su administración.

La República del Perú suscribió con el Banco Interamericano de Desarrollo - BID el 29 de agosto de 2014 el Contrato de Préstamo N° 3214/OC-PE para financiar el proyecto de inversión pública "Mejoramiento de la Efectividad del Control Tributario y Aduanero del Universo de Administrados a Nivel Nacional", cuya ejecución está a cargo de la SUNAT. Uno de los objetivos del proyecto es el fortalecimiento de la arquitectura informática de la SUNAT, y para ello la entidad ha definido la contratación de un servicio especializado de identificación y evaluación de brechas y vulnerabilidades de seguridad de la información, a fin de mejorar y fortalecer la seguridad de los sistemas críticos de la entidad y de sus respectivos controles.



## OBJETIVO GENERAL

El objetivo de este proceso es contratar una firma consultora que se encargue de la identificación y evaluación de las brechas existentes en los controles de seguridad de los activos de información críticos de la SUNAT, tomando como referencia lo establecido en el Anexo A de la NTP-ISO/IEC 27001:2014, así como de la identificación y evaluación de las vulnerabilidades de seguridad existentes en sistemas informáticos críticos de la entidad.

## OBJETIVOS ESPECIFICOS

1. Identificar e inventariar los activos de información relacionados con diez (10) sistemas informáticos críticos de la SUNAT.
2. Identificar y evaluar las brechas existentes en los controles de seguridad de los activos de información previamente identificados, con respecto a la Norma ISO/IEC 27001:2014
3. Identificar y evaluar las vulnerabilidades de seguridad existentes en diez (10) sistemas informáticos críticos, mediante la ejecución de pruebas de penetración o "ethical hacking".

## ALCANCES Y ENTREGABLES DEL SERVICIO

A continuación, se detallan los entregables esperados del servicio.

### 1. Plan de gestión

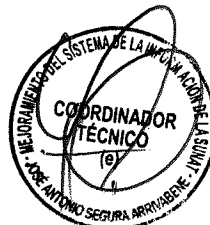
La firma consultora deberá entregar un plan de trabajo, el cual debe incluir:

- Definición, objetivos y alcance del servicio.
- Descripción detallada de la metodología a emplear.
- Entregables.
- Cronograma de actividades.
- Organización.
- Plan de comunicaciones.
- Plan de riesgos.
- Actividades de control y aseguramiento de calidad de los entregables.
- Requisitos a cumplir/entregar por SUNAT.
- Factores críticos de éxito del proyecto.

### 2. Inventario de activos de información críticos

La firma consultora deberá elaborar el inventario de activos de información, relacionados con diez (10) sistemas informáticos críticos de la SUNAT. Dicho inventario deberá contener toda la información relevante que permita identificar de forma clara cada uno de los activos, como por ejemplo:

- Información básica del activo (nombre, proceso de negocio, descripción).



- Tipo de activo: base de datos, archivo, etc.
- Nivel de clasificación de la información (por ejemplo, pública, clasificada, reservada).
- Información relacionada con su ubicación (sistema informático relacionado, infraestructura tecnológica, centro de datos).
- Propietario.
- Usuarios y niveles de acceso.

Los activos de información corresponderán únicamente a aquellos que son gestionados por la Intendencia Nacional de Sistemas de Información (INSI), principalmente por la Gerencia de Operaciones y Soporte a Usuarios (GOSU), pero sin limitarse a dicha gerencia.

La INSI proporcionará a la firma consultora toda la documentación disponible, relacionada con los diez sistemas informáticos críticos, a fin de poder elaborar el inventario de activos de información. La información que no esté disponible en documentos, deberá ser relevada por la firma consultora mediante reuniones y entrevistas con el personal de la INSI.

La firma consultora deberá tomar en cuenta que la plataforma informática de SUNAT considera las siguientes tecnologías:

- Sistemas operativos: Linux para servidores de aplicaciones y AIX para servidores de BD.
- Motores de Base de Datos: Informix versión 11 y 12 y Oracle versión 11.
- Servidor de Aplicaciones: Web Logic.
- Servidor web: Iplanet y NGINX.

Para los sistemas críticos materia del alcance de la presente consultoría, la cantidad aproximada de equipos involucrados es: ocho (08) servidores web, dieciséis (16) servidores de aplicación y cuatro (04) servidores de base de datos.

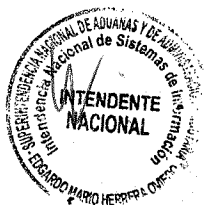
### 3. Informe de diagnóstico de brechas existentes en los controles de seguridad de los activos de información.

La firma consultora deberá identificar y clasificar, según su nivel de criticidad, las brechas existentes en los controles de seguridad de los activos de información previamente identificados e inventariados. Las brechas deberán identificarse, tomando como referencia los controles establecidos en el Anexo A de la NTP-ISO/IEC 27001:2014.

La evaluación de las brechas y niveles de cumplimiento de los controles se deberá realizar mediante:

- Revisión de los controles técnicos e informáticos aplicados a la infraestructura tecnológica.
- Entrevistas a personal clave que forme parte del alcance del servicio.
- Revisión de la documentación existente.

Otros mecanismos que considere la firma consultora.



La criticidad de cada brecha (alta, media, baja) deberá ser asignada por la firma consultora, en función a la probabilidad de ocurrencia de algún evento que ponga en riesgo la seguridad del activo de información, y del impacto que dicho evento podría generar en la SUNAT.

#### 4. Informe de diagnóstico de vulnerabilidades de seguridad en los sistemas informáticos críticos.

La firma consultora deberá ejecutar pruebas de penetración sobre las aplicaciones e infraestructura tecnológica relacionada con diez sistemas informáticos críticos de la SUNAT. Estas pruebas deberán ser del tipo "caja negra" y "caja blanca". Así mismo, las pruebas deberán contemplar:

- Pruebas externas para servidores expuestos hacia internet, a nivel de sistema operativo y software base.
- Pruebas internas para servidores, equipos de red y estaciones de trabajo, a nivel de sistema operativo y software base.
- Pruebas para aplicaciones web (con y sin credenciales), tanto a través de internet como desde la red interna.
- Pruebas a nivel de red interna (evaluación de la correcta segmentación de la red).

La SUNAT proporcionará a la firma consultora la información necesaria sobre los servidores e infraestructura tecnológica relacionada con los diez sistemas críticos, a fin de poder realizar las pruebas de penetración.

La criticidad de cada vulnerabilidad (alta, media, baja) deberá ser asignada por la firma consultora, en función a la probabilidad de ocurrencia de algún evento que ponga en riesgo la seguridad del activo de información, y del impacto que dicho evento podría generar en la SUNAT.

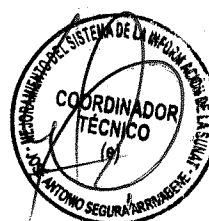
#### 5. Plan de acción para la remediación de brechas y vulnerabilidades identificadas

La firma consultora deberá elaborar un plan de acción para la remediación de cada una de las brechas y vulnerabilidades identificadas en los entregables 3 y 4. Cada brecha/vulnerabilidad deberá tener su respectiva remediación, la cual debe contener:

- Descripción de la remediación, detallando todas las actividades correctivas necesarias.
- Naturaleza de la remediación, especificando si se trata, por ejemplo, de cambio de procedimientos, cambio organizacional, adquisición o cambio tecnológico, etc.
- Nivel de complejidad de la remediación (alto, medio, bajo).
- Impacto de la remediación (alto, medio, bajo).

El plan de acción deberá tener una priorización de actividades, basada en:

- La criticidad de cada brecha/vulnerabilidad.
- El nivel de complejidad de la remediación de cada brecha/vulnerabilidad.
- El impacto de la remediación de cada brecha/vulnerabilidad.



Se deberán priorizar las acciones correctivas relacionadas a las brechas/vulnerabilidades de mayor criticidad, y que tengan un alto impacto y una baja complejidad de ejecución.

El plan de acción también deberá contener las principales recomendaciones y conclusiones de la firma consultora respecto al servicio ejecutado y respecto a las acciones a priorizar por parte de la SUNAT.

## ORGANIZACIÓN PARA LA PRESTACIÓN DEL SERVICIO

### PERSONAL CLAVE

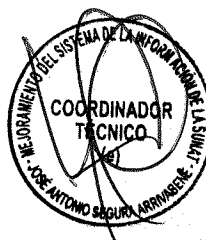
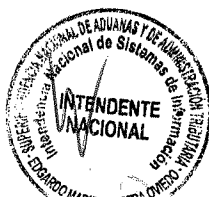
La firma consultora deberá proveer el personal idóneo para la óptima ejecución del servicio. El personal clave debe estar conformado por:

- Un Jefe de Proyecto.
- Como mínimo un especialista en Sistemas de Gestión de Seguridad de Información (SGSI).
- Como mínimo un especialista en pruebas de penetración o "ethical hacking".

### PERFILES DEL PERSONAL CLAVE

El personal clave de la firma consultora deberá cumplir los siguientes requisitos. La experiencia deberá ser detallada a través del formato indicado en el Anexo A, y acreditada con copias simples de constancias o contratos donde se indiquen las labores realizadas.

Gerente de Proyecto	
Formación académica	<ul style="list-style-type: none"><li>• Título Profesional en Ingeniería de Sistemas, Informática, Industrial, o profesiones afines.</li></ul>
Certificaciones	<ul style="list-style-type: none"><li>• PMP vigente.</li></ul>
Experiencia (mínima)	<ul style="list-style-type: none"><li>• Tres (03) años en proyectos de tecnologías de información en instituciones públicas y/o privadas desempeñando roles de gerente o líder de proyecto.</li></ul>



<b>Especialista SGSI</b>	
Formación académica	<ul style="list-style-type: none"> <li>• Título Profesional en Ingeniería de Sistemas, Informática, Industrial, o profesiones afines.</li> <li>• Especialización o post-grado en temas relacionados a seguridad de la información.</li> </ul>
Certificaciones	<ul style="list-style-type: none"> <li>• CISM (Certified Information Security Management).</li> <li>• ISO/IEC 27001 Lead Implementer.</li> </ul> <p>Se valorarán, adicionalmente, las siguientes certificaciones:</p> <ul style="list-style-type: none"> <li>• ISO/IEC 27001 Auditor Lead.</li> <li>• ISO/IEC 27005 Gestión de Riesgos de Seguridad de Información.</li> </ul>
Experiencia (mínima)	<ul style="list-style-type: none"> <li>• Cuatro (04) años en servicios de consultoría relacionados con gestión de seguridad de la información.</li> </ul>

<b>Especialista "Ethical Hacking"</b>	
Formación académica	<ul style="list-style-type: none"> <li>• Título Profesional en Ingeniería de Sistemas, Informática, Ciencias de la Computación, o afines.</li> </ul>
Certificaciones	<ul style="list-style-type: none"> <li>• Certificación en "ethical hacking" o "penetration testing" (EC-Council, Mile2, Offensive Security, u otra).</li> </ul> <p>Se valorarán, adicionalmente, las siguientes certificaciones:</p> <ul style="list-style-type: none"> <li>• Secure Web Application Engineer (por ejemplo, Mile2, u otra).</li> <li>• Secure Developer (por ejemplo, WhiteHat u otra).</li> </ul>
Experiencia (mínima)	<ul style="list-style-type: none"> <li>• Cuatro (04) años en servicios de "ethical haking".</li> </ul>

## MECANISMOS DE COORDINACIÓN

Como parte de la organización del proyecto, deberá existir un Comité Directivo, el cual se constituye en la instancia máxima para la toma de decisiones y para el seguimiento de la marcha del proyecto, se reunirá según la frecuencia a definir en el Plan de Gestión y estará conformado por:

- Por la SUNAT:
  - Director de Proyecto (Intendente Nacional de Sistemas)
  - Jefe de Proyecto



- Otros integrantes que defina SUNAT.
- Por la firma consultora:
  - Director de Proyecto
  - Jefe de Proyecto
  - Otros integrantes que defina la firma.

## **LUGAR, PLAZO Y HORARIO DE LA EJECUCIÓN DE LA PRESTACIÓN**

### **Lugar**

La prestación se realizará en las instalaciones de la INSI.

Toda documentación requerida para la suscripción del contrato y relacionada a la firma consultora o su personal, y los entregables referidos a la prestación, se deberán entregar a la Sede Central de la SUNAT sito en Av. Garcilaso de la Vega 1472 – Lima Cercado, dirigido a la Unidad Ejecutora Mejoramiento del Sistema de Información de la SUNAT - UEMSI.

De haber algún cambio de lugar de entrega este será comunicado a la firma consultora a los cinco (05) días calendario de ocurrido el hecho.

### **Plazo de ejecución**

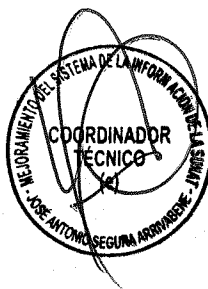
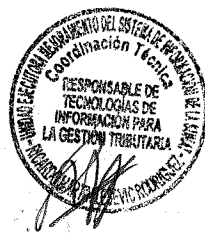
El plazo de la consultoría es de 120 días calendario, que incluyen los plazos de revisión y conformidad de los entregables, contados a partir del día siguiente a la suscripción del contrato por ambas partes.

### **Horario**

Las actividades que, por su naturaleza, deban ser realizadas en los locales de la SUNAT, se ejecutarán dentro del horario habitual de trabajo el cual es de lunes a viernes de 08:30 am a 05:30 pm huso horario de Perú (UTC-05:00); en caso la firma consultora requiera realizar alguna actividad fuera de dicho horario deberá solicitarlo de forma anticipada como mínimo dos (2) días calendario vía correo electrónico al Jefe del Proyecto de la SUNAT para su aprobación.

## **PRESENTACIÓN DE ENTREGABLES E HITOS DE PAGO**

En el siguiente cuadro se detallan los hitos de pago (expresados en porcentaje del monto total del contrato) y plazos máximos que tiene la firma consultora para remitir a la SUNAT cada uno de los entregables, contados a partir del día siguiente de la firma del contrato. En el Plan de Gestión se establecerá el mecanismo de revisión y aprobación de entregables. La SUNAT tendrá un plazo máximo para revisar y para otorgar la respectiva conformidad de 10 días calendario, computados desde la recepción del respectivo entregable.





	Entregable	Plazo de Presentación	Pagos
E1	Plan de Gestión	A los diez (10) días calendario de la firma del contrato.	-
E2	Inventario de activos de información críticos	A los cuarenta y cinco (45) días calendario de la firma del contrato.	15%
E3	Informe de diagnóstico de brechas en controles de seguridad	A los setenta y cinco (75) días calendario de la firma del contrato.	30%
E4	Informe de diagnóstico de vulnerabilidades (ethical hacking)	A los ciento cinco (105) días calendario de la firma del contrato.	30%
E5	Plan de acción para remediación de brechas y vulnerabilidades	A los ciento veinte (120) días calendario de la firma del contrato.	25%

Adicionalmente, y previo al último pago a cargo de la SUNAT, se requerirá la no objeción del BID al último entregable de la firma consultora.

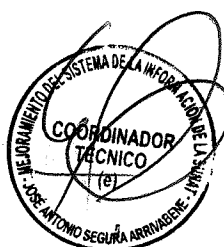
## CONFORMIDADES

El Coordinador Técnico de la Unidad Ejecutora Mejoramiento de los Sistemas de Información de la SUNAT otorgará la conformidad de los entregables presentados por la firma consultora, con la opinión favorable de las áreas de la Intendencia Nacional de Sistemas de Información que se definan en el Plan de Gestión.

## CLAUSULAS ESPECIALES

### Otras obligaciones de LA FIRMA CONSULTORA.

- Todo personal de LA FIRMA CONSULTORA que labore en el proyecto deberá firmar un compromiso de confidencialidad de la información del proyecto y de los datos de LA SUNAT, los cuales se encuentran bajo reserva tributaria y la violación a dicha confidencialidad implica acciones penales.
- LA FIRMA CONSULTORA se compromete, a que el personal clave se encontrará físicamente en el Perú y ubicados de manera presencial en las instalaciones de la SUNAT.
- LA FIRMA CONSULTORA deberá asumir los daños causados a personas y/o propiedades de LA SUNAT, durante la prestación, para lo cual deberá tomar todas las precauciones necesarias y recaudos legales actuales y exigibles, a fin de evitar accidentes personales y/o daños a las propiedades.
- LA FIRMA CONSULTORA es especialista en los trabajos de este rubro, y habiendo revisado la totalidad de esta documentación, no podrá alegar ignorancia en caso de errores, y/o especificaciones, teniendo la obligación de formular las aclaraciones necesarias antes de efectuar trabajos o gastos relacionados por los mismos, no reconociéndose adicionales.



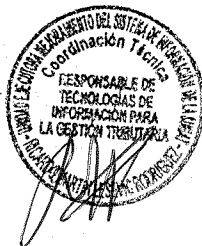
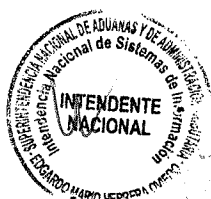
- e) **LA FIRMA CONSULTORA** se compromete a cumplir y observar lo establecido en la Ley de Seguridad y Salud en el Trabajo (aprobado mediante Ley N° 29783) y en su Reglamento (aprobado mediante Decreto Supremo N° 005-2012-TR); durante la ejecución de las prestaciones de servicios a su cargo; obligándose a implementar, dotar, proveer y/o suministrar a cada uno de sus trabajadores los implementos de seguridad que corresponda de acuerdo al grado y/o nivel de riesgo que pueda evidenciarse en el desarrollo de las actividades propias de la presente contratación dentro de las instalaciones de **LA SUNAT**; así como garantizar la contratación de los respectivos seguros de acuerdo a la normatividad vigente.
- f) Del mismo modo, **LA FIRMA CONSULTORA** se compromete a cumplir y respetar cada una de las medidas de seguridad previstas en el Reglamento Interno de Seguridad y Salud en el Trabajo de **LA SUNAT**, el que será puesto en conocimiento de sus trabajadores al inicio de la prestación de servicios; para cuyo efecto **LA SUNAT**, a la suscripción del contrato, cumplirá con hacer entrega de una copia legible del mismo.
- g) Los errores que se reporten a **LA FIRMA CONSULTORA** hasta doce (12) meses después de la aceptación del servicio (Acta final de aprobación implantación del aplicativo), deberán ser corregidos sin costo alguno para **LA SUNAT**.
- h) **LA FIRMA CONSULTORA** será responsables sobre la custodia y conservación del hardware, software, licencias, manuales o cualquier Información propiedad de **LA SUNAT** que le fuera encomendada.
- i) **LA FIRMA CONSULTORA** deberá cumplir con los requerimientos de documentación técnica de la entidad, de igual manera bajo los parámetros de entrega de seguridad informados por **LA SUNAT** y acorde con las políticas internas.
- j) Los entregables generados en el marco del servicio serán en idioma español.
- k) **LA FIRMA CONSULTORA** deberá proporcionar a la firma del contrato:
- Documentos que acrediten la tenencia o alquiler de una oficina en el Perú, ubicado en la Ciudad de Lima (dirección, distrito, código postal) en donde **LA SUNAT** podrá notificar cualquier comunicación que estime pertinente.
  - Declaración Jurada indicando los números de Teléfonos, Fax, Correos electrónicos, etc. necesario para que **LA SUNAT** pueda realizar el reporte de errores o problemas de los entregables del presente contrato.

#### Otras obligaciones de LA SUNAT

- a) **LA SUNAT** entregará la información necesaria que **LA FIRMA CONSULTORA** requiera para cumplir satisfactoriamente el presente contrato, previa evaluación de **LA SUNAT** considerando los acuerdos de confidencialidad, reserva y de las normas vigentes.

#### Confidencialidad.

- a) **LA FIRMA CONSULTORA** se obliga a no difundir, aplicar ni comunicar a terceros información, base de datos, procesos, documentos ni cualquier otro aspecto relacionado a **LA SUNAT** a la que tenga acceso durante la ejecución del servicio y después de la finalización del mismo, excepto previo consentimiento por escrito de **LA SUNAT**.
- b) **LA FIRMA CONSULTORA** se obliga a adoptar las medidas necesarias para asegurar la confidencialidad de sus empleados y terceros.



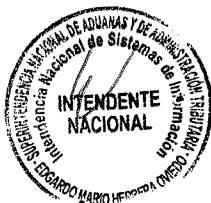
- c) En caso que **LA FIRMA CONSULTORA** incumpla con lo señalado en los párrafos anteriores, **LA SUNAT** a su sola discreción podrá resolver el contrato y además adoptar las acciones legales que corresponda.
- d) **LA FIRMA CONSULTORA** se compromete a no usar el nombre de **LA SUNAT** ni hacer referencia al servicio, en cualquier promoción, publicidad o anuncio, sin previa autorización de **LA SUNAT**.
- e) Los documentos, archivos y en general cualquier información o conocimientos generados durante el servicio, serán de propiedad única y exclusiva de **LA SUNAT**, quedando prohibido el uso por parte de **LA FIRMA CONSULTORA**, salvo autorización expresa de **LA SUNAT**.

#### Retiro del personal asignado al proyecto

- a) **LA SUNAT** se reserva el derecho de solicitar a **LA FIRMA CONSULTORA** que cualquier miembro de su personal, o cualquier subcontratista o personal de éste, sea retirado y reemplazado por una alternativa de acuerdo a los perfiles mínimos considerados por **LA SUNAT**, a condición de que este derecho sólo fuere ejercido cuando **LA SUNAT** razonablemente considere que la cantidad o calidad del trabajo del empleado o subcontratista en cuestión resultan inaceptables. Se debe solicitar formalmente el cambio del personal con la justificación correspondiente, **LA FIRMA CONSULTORA** tendrá un plazo máximo de diez (10) días calendario para presentar al reemplazo El/La reemplazante deberá ser aprobado por **LA SUNAT** en un plazo de dos (2) a diez (10) días calendario y reunir similares habilidades, competencia y experiencia que el/la reemplazado/a, en el momento del reemplazo.
- b) **LA FIRMA CONSULTORA** se compromete, en tanto esté a su alcance, a no reasignar ni remover ningún miembro de su personal asignado. Si debiera producirse un reemplazo por razones de fuerza mayor:
  - i. **LA FIRMA CONSULTORA** comunicará la salida del personal con un plazo máximo de veinticuatro (24) horas de ocurrido el evento.
  - ii. El/La reemplazante deberá ser aprobado por **LA SUNAT** en un plazo de dos (2) a diez (10) días calendario y reunir similares habilidades, competencia y experiencia que el/la reemplazado/a, en el momento del reemplazo.

#### Propiedad intelectual

- a) **LA FIRMA CONSULTORA** deberá indemnizar y eximir de cualquier responsabilidad a **LA SUNAT**, a sus empleados y funcionarios, por cualquier litigio, acción legal o procedimiento administrativo, reclamación, demanda, pérdida, daño, costo y gasto cualquiera sea su naturaleza, incluidos los honorarios y gastos de representación legal, en los cuales pueda incurrir **LA SUNAT** como resultado de cualquier trasgresión o supuesta trasgresión de cualquier patente, uso de modelo, diseño registrado, marca registrada, derechos de autor o cualquier otro derecho de propiedad intelectual que estuviese registrado o de alguna otra forma existente a la fecha del contrato debido a la instalación de los bienes por parte de **LA FIRMA CONSULTORA** o el uso de los mismos por parte de **LA SUNAT**.
- b) Dicha indemnización no procederá si los bienes o cualquiera de sus partes fuesen utilizados para fines no previstos en el contrato o para fines que no pudiesen razonablemente inferirse de dicho contrato.



- c) Si se entablara una demanda o reclamación contra **LA SUNAT** como resultado de cualquiera de las situaciones indicadas, **LA SUNAT** notificará con prontitud a **LA FIRMA CONSULTORA**, y éste podrá, a su propio costo y a nombre de **LA SUNAT**, proceder con tales acciones legales o reclamaciones y llevar a cabo cualquier negociación pertinente para la resolución de tales demandas o reclamaciones.
- d) Si **LA FIRMA CONSULTORA** no cumpliera con la obligación de informar a **LA SUNAT** dentro del plazo de ley contado a partir de la fecha del recibo de tal notificación, de su intención de proceder con cualquier acción legal o reclamación, **LA SUNAT** tendrá derecho a emprender dichas acciones o reclamaciones a nombre propio.
- e) **LA SUNAT** se compromete a brindarle a **LA FIRMA CONSULTORA**, cuando éste así lo solicite, cualquier asistencia que estuviese a su alcance para que **LA FIRMA CONSULTORA** pueda contestar las citadas acciones legales o reclamaciones. **LA SUNAT** será reembolsado por **LA FIRMA CONSULTORA** por todos los gastos razonables en que hubiera incurrido.

### Virus

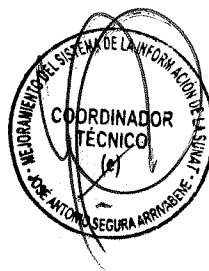
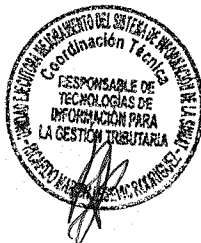
- a) Es posible que exista software que puede corromper no sólo el software objeto del Contrato, sino también otro software empleado en el mismo Procesador o en otros procesadores conectados a él, incluyendo software de base. Esta corrupción de software puede permanecer latente y no necesariamente será hallada durante el período de pruebas de aceptación. Dicha corrupción se denominará "virus" a los fines de esta cláusula.
- b) **LA FIRMA CONSULTORA** manifiesta que ha usado procedimientos aceptados en la industria durante la construcción del Software para minimizar la posibilidad de que se haya introducido o codificado virus en el Software.
- c) **LA FIRMA CONSULTORA** acuerda que, en caso de ser hallado un virus causado por los productos entregados por éste en virtud de la presente o por hechos efectuados por sus empleados, asistirá a **LA SUNAT** para reducir el efecto del virus, y particularmente si el virus causara pérdida de eficiencia operativa o pérdida de datos, asistir a **LA SUNAT** para mitigar dichas pérdidas y restaurar la eficiencia operativa original de **LA SUNAT**.

### RESPONSABILIDAD POR VICIOS OCULTOS

**LA FIRMA CONSULTORA** es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofrecido por un plazo de doce (12) meses contados a partir de la conformidad otorgada por **LA SUNAT**. La conformidad otorgada por **LA SUNAT** a considerar para el cómputo de los 12 meses, será la que se refiera al último entregable del servicio.

### DECLARACIÓN DE VIABILIDAD

Esta contratación está enmarcada en el proyecto de inversión pública "Mejoramiento de la efectividad del control tributario y aduanero del universo de administrados a nivel nacional", el nivel de estudio con el que se obtuvo la viabilidad fue el perfil con fecha de viabilidad 14 de marzo del 2014. El código SNIP asignado es 282107.



## OTRAS CONDICIONES

De requerirlo, el proveedor podrá solicitar un adelanto del 30% del monto del contrato contra la presentación de una carta fianza.



## ANEXO A: Formato de Acreditación del Personal Clave

ANEXO A	
Formato de Acreditación	
<b>Perfil</b>	
<b>Nombre del consultor</b>	
<b>Nombre del proyecto</b>	
<b>Esfuerzo del proyecto (en hombre - mes)</b>	
<b>Herramientas utilizadas</b>	
<b>Explique brevemente el proyecto, desde el punto de vista de su perfil</b>	
<b>Aportes y responsabilidades en el proyecto</b>	

