TÉRMINOS DE REFERENCIA – 192026 [1]

1. Denominación de la contratación:

Servicio especializado de Ethical Hacking, que permita analizar e identificar vulnerabilidades en la infraestructura informáticas, así como, en los servicios digitales publicados.

2. Área usuaria que requiere el servicio:

Subjefatura de Tecnologías de la Información.

3. Finalidad Pública:

SERVIR, mediante la Oficina General de Administración y Finanzas y a través de Subjefatura de Tecnologías de la Información, requiere contratar el servicio especializado de seguridad informática que evalúe la seguridad de la plataforma tecnológica y de los servicios digitales de la Autoridad Nacional del Servicio Civil - SERVIR, todo ello con el objetivo general de identificar, documentar y corregir las vulnerabilidades que podrían generar riesgos contra la continuidad operativa de los servicios de tecnologías que se brindan la Autoridad Nacional del Servicio Civil – SERVIR.

La implementación del servicio se enmarca en el cumplimiento a la implementación de categoría de controles N° 8.7 Protección contra programas maliciosos, 8.8 Gestión de Vulnerabilidades Técnicas y 8.20 Seguridad de Redes de la Norma Técnica Peruana NTP ISO/IEC 27001:2022

4. Antecedentes:

De acuerdo al artículo 33 del Decreto Legislativo 1412, establece que la Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno.

Asimismo, de acuerdo al artículo 105 del Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Legislativo que aprueba la Ley de Gobierno Digital, establece que las entidades públicas planifican y realizan pruebas para evaluar vulnerabilidades a los siguientes activos: aplicativos informáticos, sistemas, infraestructura, datos y redes, que soportan los servicios digitales, procesos misionales o relevantes de la entidad.

[1] Ley N° 32069 – Ley General de Contrataciones Públicas, Artículo 5 Principios Rectores de la Contratación, literal C) **Valor por dinero:** las entidades contratantes maximizan el valor de lo que obtienen en cada contratación, en términos de eficiencia, eficacia y economía, lo cual implica que se contrate a quien asegure el cumplimiento de la finalidad pública de la contratación, considerando la calidad, la sostenibilidad de la oferta y la evaluación de los costos y plazos, entre otros aspectos vinculados a la naturaleza de lo que se contrate, y que no procure únicamente el menor precio.

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

En ese sentido, la Autoridad Nacional del Servicio Civil, surge la necesidad de contar con un servicio especializado de Ethical Hacking, que permita analizar e identificar vulnerabilidades en la infraestructura informáticas, así como, en los servicios digitales publicados.

5. Objetivo de la contratación:

5.1 Objetivo General:

Contar con un servicio especializado para evaluar la seguridad de la plataforma tecnológica y de los servicios digitales de la Autoridad Nacional del Servicio Civil - SERVIR en el marco del fortalecimiento de su Sistema de Gestión de Seguridad de la Información – SGSI.

5.2 Objetivos Específicos:

- Proveer una visión del nivel de seguridad informática de la red de SERVIR desde internet y determinar si los controles implementados ante amenazas externas son los adecuados.
- Identificar los factores de vulnerabilidad específicos como caminos de acceso para penetrar en los sistemas de SERVIR.
- Verificar que las medidas de seguridad implementadas por SERVIR son las adecuadas y si son capaces de evitar una posible intrusión.
- Obtener recomendaciones generales y específicas que permitan a SERVIR, implementar los mecanismos de protección acorde con las mejores prácticas de ciberseguridad.

6. Actividad del POI:

4.4.5 Implementación de proyectos de desarrollo digital seguros y confiables en SERVIR

7. Alcance y Descripción del Servicio:

El servicio incluye realizar una exploración interna y externa de la infraestructura tecnológica y de los servicios digitales de manera controlada, a través de técnicas de escaneo e intrusión para realizar el respectivo análisis de vulnerabilidades y obtener un panorama detallado de la misma. Además, deberá evidenciarse el grado de exposición o intrusión de estos recursos tecnológicos ante un eventual ataque informático y por ende hacer las recomendaciones adecuadas del caso.

Por otro lado, deberá realizarse la búsqueda de información confidencial accesible en Internet que puedan comprometer con la confidencialidad e integridad de la infraestructura tecnológica y de los servicios digitales de la Entidad. Adicionalmente, incluye realizar pruebas de ingeniería social a los servidores civiles de la Entidad.

7.1 Actividades:

7.1.1. Ethical Hacking de infraestructura interna

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

Este análisis se centra en el contexto interno de la organización. El contratista deberá evaluar los puntos clave de la red interna de Minera Veta Dorada, así como la información que fluye a través de sus diferentes niveles y áreas lógicas.

El alcance de las pruebas de infraestructura interna será de 20 direcciones IP.

El análisis deberá estar basado en metodologías de OSSTMM y PTES. Además, debe ser realizado con herramientas actualizadas para auditoria de vulnerabilidades (Herramientas comerciales). Este análisis se realizará desde cualquier lugar de Internet; con direcciones IP Públicas fijas o variables. Para la ejecución de estos trabajos el proveedor deberá considerar como mínimo las siguientes tareas:

a) Recopilar la mayor cantidad de información susceptible de ser utilizada para romper cualquiera de las protecciones que pueda disponer Veta Dorada, para el acceso seguro a los servicios.
b) Escaneo de puertos, identificación de servicios y sistemas operativos.
c) Determinar, utilizando herramientas comerciales disponibles además de herramientas exclusivas y técnicas manuales, sobre las deficiencias de seguridad que existen en los sistemas incluidos dentro del servicio.
d) Analizar vulnerabilidades en las aplicaciones y componentes que pudieran poner al descubierto la seguridad del servicio.

7.1.2. Ethical Hacking de infraestructura externa

Este tipo de análisis se refiere al contexto desde donde se realizará la evaluación. Por tanto, en el análisis externo, el Contratista deberá evaluar todos aquellos puntos relacionados con los servicios de publicación externa de la red de la Autoridad Nacional del Servicio – CIVIL; entre los cuales se encuentran: Servicios de publicación con acceso Web, equipos de red tales como Firewall Perimetrales, IDS e IPS perimetrales.

El alcance de las pruebas de infraestructura externa será de hasta 34 direcciones IP.

Asimismo, el análisis deberá estar basado en OSSTMM y PTES. Además, debe ser realizado con herramientas actualizadas para auditoria de vulnerabilidades, dichas herramientas libres y comerciales deberán contar con las licencias adecuadas para este tipo de servicio. Este análisis se realizará desde cualquier lugar de Internet; con direcciones IP Públicas fijas o variables.
Para la ejecución de estos trabajos el proveedor deberá considerar como mínimo las siguientes tareas:

a) Recopilación de la mayor cantidad de información susceptible a ser utilizada para vulnerar cualquiera de los controles de seguridad de las que pudiera disponer SERVIR.
b) Escaneo y análisis de la red con el objetivo de obtener información sobre de la misma.
c) Escaneo de puertos, identificación de servicios y sistemas operativos.

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

d) Determinar, utilizando herramientas comerciales disponibles además de herramientas exclusivas y técnicas manuales, las deficiencias de seguridad que existen en los sistemas incluidos dentro del servicio.
e) Ejecutar intentos de obtención de cuentas de usuarios (login y password) del sistema a través de herramientas automáticas y técnicas manuales utilizadas por los hackers, revisión de contraseñas predeterminadas del sistema y ataques de diccionario.
f) Analizar vulnerabilidades en la infraestructura pública y componentes que pudieran poner en riesgo la seguridad de los servicios.

7.1.3. Ethical Hacking de Aplicaciones web

Este tipo de análisis se refiere al contexto desde donde se realizará la evaluación. Por tanto, en el análisis de aplicaciones web, el Contratista deberá evaluar todos aquellos puntos relacionados con los Sistemas Web de la Autoridad Nacional del Servicio Civil – SERVIR

El alcance de las pruebas de aplicaciones web se realizará a ocho (8) Sistemas que la Autoridad Nacional del Servicio Civil.

Asimismo, el análisis deberá estar basado en OSSTMM, PTES y OWASP Testing Guide. Además, debe ser realizado con herramientas actualizadas para Auditoria de Vulnerabilidades (Herramientas libres y comerciales).

Este análisis se realizará desde cualquier lugar de Internet; con direcciones IP Públicas fijas o variables, desde una perspectiva de atacante externo con credenciales para ingresar a los sistemas.

Para la ejecución de estos trabajos el Contratista deberá considerar como mínimo la siguiente metodología dividida en dos fases:

- **Modo pasivo:**
  En esta fase se intenta comprender la lógica de la aplicación mediante la interacción con la misma y la utilización de herramientas para recopilación de información. Al final de esta fase se debería comprender cuales son todos los puntos de acceso de la aplicación y los posibles vectores de ataque.

- **Modo activo:**
  En esta fase se ejecutan los test definidos en la guía de pruebas de OWASP con el objetivo de detectar fallos de seguridad concretos. categorías de prueba.

7.1.4. Pruebas de OSINT (Open Source Intelligence)

Se debe de realizar la evaluación sobre la recopilación y análisis de información pública accesible en Internet, con el fin de extraer conclusiones útiles para investigaciones, monitoreo, campañas de ingeniería social y evaluación del nivel de exposición de su organización, tales como:

- Infraestructura tecnológica expuesta

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

- Información institucional expuesta
- Recursos informáticos de la entidad en la Dark Web

7.1.5. Pruebas de Ingeniería Social

Se debe realizar ataques de obtención de información utilizando técnicas de ingeniería social sobre el personal de la entidad, en un rango de 150 personas, simulándose situaciones reales (situaciones del ámbito de la entidad), que permitan identificar brechas de seguridad en el eslabón normalmente considerando más débil de la cadena de seguridad información, las personas.

Las pruebas a la infraestructura tecnológica y de los servicios digitales se realizarán desde las siguientes perspectivas: CAJA NEGRA y CAJA GRIS. Para la realización de las pruebas en CAJA GRIS se brindarán credenciales de acceso al sistema de información, con uno (01) o dos (02) perfiles de acceso.

7.2 Requisitos para la contratación:

Perfil del proveedor:

- Persona Natural o jurídica.
- RUC activo y habido
- Contar con Registro Nacional de Proveedores (RNP) vigente (De corresponder).
- No estar imposibilitado para contratar con el Estado.
- De conformidad con la Ley N° 28970, Ley que crea el Registro de Deudores Alimentarios Morosos y modificatorias, en caso estar inscrito en el REDAM se requiere que previo a la suscripción del contrato (contrato u orden de servicio), el deudor acredite el cambio de su condición a través de la cancelación respectiva o autorice el descuento, del monto de la pensión mensual fijada en el proceso de alimentos, lo cual será coordinado con la Subjefatura de Abastecimiento (cuando corresponda).

Experiencia en la especialidad:

El proveedor debe acreditar experiencia en servicios de Ethical Hacking o Análisis de Vulnerabilidades o Red Team auditorías o ciberseguridad por un monto acumulado mínimo de S/ 100,000.00 (Cien mil con 00/100 soles) durante los últimos 3 años, vinculado a servicios de análisis de vulnerabilidades y/o Ethical Hacking y/o Red Team y/o servicio de consultoría de ciberseguridad en el sector público o privado.

Acreditación:
Se acreditará con copia simple de (i) contratos u órdenes de servicio, con su respectiva conformidad; o (ii) constancia de prestación; o (iii) comprobantes de pago cuya cancelación se acredite con: constancia de depósito o nota de abono o reporte de estado de cuenta o cualquier otro documento emitido por entidad del sistema financiero que acredite el abono; o (iv) cualquier otra documentación que, de manera fehaciente, demuestre la experiencia solicitada

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

Perfil del personal Clave:

Para la prestación del servicio, el Contratista deberá contar como mínimo dos (02) personas con los siguientes perfiles:

Un (1) jefe de Proyectos en Seguridad Informática:

Formación Académica:
Profesional bachiller o titulado en Ingeniería de Sistemas; o Ingeniería informática; o Ingeniería electrónica; o Ingeniería de computación y sistemas; o Ingeniería en Telecomunicaciones; o Ingeniería empresarial y de sistemas.

Acreditación:
Copia simple del grado académico de bachiller o titulo

Experiencia laboral General:
Mínimo (06) años de experiencia en Seguridad Informática.

Experiencia laboral especifica[2]:
Haber participado en cinco (05) servicios iguales o similares al objeto de la contratación en el sector Público o Privado como mínimo.

Acreditación:
Se acreditará con copia simple de (i) contratos u órdenes de servicio, con su respectiva conformidad; o (ii) constancia de prestación o certificado de trabajo o constancia de trabajo; o (iii) comprobantes de pago cuya cancelación se acredite con: constancia de depósito o nota de abono o reporte de estado de cuenta o cualquier otro documento emitido por entidad del sistema financiero que acredite el abono; o (iv) cualquier otra documentación que, de manera fehaciente, demuestre la experiencia solicitada

Certificaciones Internacionales:
Poseer la certificación por lo menos tres (03) de las siguientes certificaciones profesionales adicionales:

- Project Management Professional (PMP)
- ECCouncil Certified Project Management (CPM)

[2] Estos documentos deben señalar los nombres y apellidos del personal clave; el cargo desempeñado indicando el día, mes y año de inicio y culminación; el nombre de la entidad u organización que emite el documento; la fecha de emisión y nombres y apellidos de quien suscribe el documento.

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo de la misma solo se considera una vez el periodo traslapado.

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

- EC Council Certified Ethical Hacker. (CEH)
- EC Council Certified Ethical Hacker Practical. (CEH-P)
- EC Council Certified Ethical Hacker Master. (CEH-M)
- EC Council Certified Security Analyst. (ECSA)
- EC Council Licensed Penetration Tester. (LPT)
- OSSTMM Professional Security Analyst. (OPSA)
- OSSTMM Professional Security Tester. (OPST)
- Mile2 Certified Penetration Testing Engineer (CPTE)
- Certified Ethical Hacking Professional Certification (CEHPC)
- Certified Secure Web Application Engineer (CSWAE)
- Certified Professional Ethical Hacker (CPEH).
- EC Council Certified Security Specialist.

Acreditación:
Las certificaciones internacionales se acreditarán con copia simple de la certificación.

Un (1) Consultor Líder Técnico en Seguridad

Formación Académica:
Profesional bachiller o titulado en Ingeniería de sistemas; o Ingeniería informática; o Ingeniería electrónica; o Ingeniería de computación y sistemas; Ingeniería en seguridad informática; o Ingeniería en Telecomunicaciones; o Ingeniería empresarial y de sistemas.

Acreditación:
Copia simple del grado académico de bachiller o titulo

Certificaciones Internacionales:
Poseer por lo menos dos (02) de las siguientes certificaciones profesionales:

- CISSP (Certified Information Systems Security Professional)
- EC Council Certified Ethical Hacker Master. (CEH-M)
- Certified Ethical Hacking Professional Certification (CEHPC)
- EC Council Certified Ethical Hacker. (CEH)
- EC-Council Certified Security Specialist (ECSS)
- EC Council Licensed Penetration Tester. (LPT)
- OSSTMM Professional Security Analyst. (OPSA)
- OSSTMM Professional Security Tester. (OPST)
- Offensive Security Certified Expert (OSCE)
- GIAC Certified Intrusion Analyst (GCIA)
- Certified Professional Ethical Hacker (CPEH)

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

- EC Council Certified Ethical Hacker Practical (CEH PRACTICAL)
- Certified Penetration Testing Professional (CPENT).
- eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX)

Acreditación:
Las certificaciones internacionales se acreditarán con copia simple de la certificación.

Experiencia laboral General:
Experiencia profesional como mínimo (03) años de experiencia en Seguridad Informática o Ethical Hacking o Análisis de Vulnerabilidades o Pentesting,

Experiencia laboral especifica[3]:
Haber participado en (03) servicios iguales o similares al objeto de la contratación en el sector Público o Privado como mínimo.

Acreditación:
Se acreditará con copia simple de (i) contratos u órdenes de servicio, con su respectiva conformidad; o (ii) constancia de prestación o certificado de trabajo o constancia de trabajo; o (iii) comprobantes de pago cuya cancelación se acredite con: constancia de depósito o nota de abono o reporte de estado de cuenta o cualquier otro documento emitido por entidad del sistema financiero que acredite el abono; o (iv) cualquier otra documentación que, de manera fehaciente, demuestre la experiencia solicitada

7.3 Lugar y plazo de prestación del servicio:

Lugar:

La prestación del servicio se realizará de manera remota en forma virtual y/o presencial (sede Arequipa N° 934 – Cercado de Lima).

Plazo:

La ejecución se realizará en un plazo de hasta sesenta (60) días calendarios, contabilizados a partir del día siguiente de la recepción de la orden de servicio.

7.4 Entregables (Resultados esperados):

Entregable N° 01: Informe de ejecución del servicio

El Contratista deberá presentar lo siguiente:

[3] Estos documentos deben señalar los nombres y apellidos del personal clave; el cargo desempeñado indicando el día, mes y año de inicio y culminación; el nombre de la entidad u organización que emite el documento; la fecha de emisión y nombres y apellidos de quien suscribe el documento.

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo de la misma solo se considera una vez el periodo traslapado.

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

- Informe ejecutivo y técnico que muestre el resultado de las pruebas de hacking a la infraestructura interna y externa.

- El Informe técnico debe estar detallado, el cual deberá mostrar el resultado de la ejecución del servicio, el cual deberá considerar al menos los siguientes aspectos:

  - ❖ Definición de prioridades y ponderación de cada riesgo identificado.
  - ❖ Descripción de las pruebas realizadas.
  - ❖ Metodología empleada.
  - ❖ Elementos evaluados.
  - ❖ Resultados obtenidos.
  - ❖ Herramientas utilizadas.
  - ❖ Listado de vulnerabilidades encontradas en los elementos de la plataforma tecnológica.
  - ❖ Descripción de las vulnerabilidades identificadas.
  - ❖ Evidencias.
  - ❖ Nivel de criticidad (Alto, Medio, Bajo).
  - ❖ Recomendaciones.
  - ❖ Conclusiones.

En un plazo de hasta treinta (30) días calendarios contados a partir día siguiente de la recepción de la orden de servicio.

Entregable N° 02: Informe con el resultado de pruebas de Ethical Hacking de las Aplicaciones web
El Contratista deberá presentar lo siguiente:

- Informe ejecutivo que muestre el resultado de las pruebas de Ethical hacking a las aplicaciones web.

- El Informe técnico debe estar detallado, el cual deberá mostrar el resultado de la ejecución del servicio, el cual deberá considerar al menos los siguientes aspectos:

  - ❖ Definición de prioridades y ponderación de cada riesgo identificado.
  - ❖ Descripción de las pruebas realizadas.
  - ❖ Metodología empleada.
  - ❖ Elementos evaluados.
  - ❖ Resultados obtenidos.
  - ❖ Herramientas utilizadas.
  - ❖ Listado de vulnerabilidades encontradas en los elementos de la plataforma tecnológica.
  - ❖ Descripción de las vulnerabilidades identificadas.
  - ❖ Evidencias.
  - ❖ Nivel de criticidad (Alto, Medio, Bajo).
  - ❖ Recomendaciones.
  - ❖ Conclusiones.

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

En un plazo de hasta veinte (20) días calendarios, contabilizado a partir del día siguiente de la presentación del primer entregable o desde el día siguiente de cumplido el plazo para la presentación del primer entregable, lo que ocurra primero.

Entregable N° 03: Informe con el resultado de las pruebas de OSINT y el de Ingeniería Social
El Contratista deberá presentar lo siguiente:

- Informe que contenga resulta de la evaluación de las pruebas de OSINT, así como, las pruebas de ingeniería social de las últimas 150 personas elegidas por la entidad.

En un plazo de hasta diez (10) días calendarios, contabilizado a partir del día siguiente de la presentación del segundo entregable o desde el día siguiente de cumplido el plazo para la presentación del segundo entregable, lo que ocurra primero.

Los entregables, podrán ser presentados a través de los siguientes canales:

MESA DE PARTES DIGITAL: Los entregables, pueden ser presentados digitalmente por la mesa de partes N° Digital – MPD de SERVIR a través del link https://www.servir.gob.pe/modulo-de-orientacion-y-mesa-de-partes-digital-servir/, la cual está habilitada las veinticuatro (24) horas del día de los siete (7) días de la semana y no tiene restricción de horarios para la presentación de documento.

MESA DE PARTES PRESENCIAL: Los entregables pueden ser presentados en la Mesa de Partes Presencial ubicada en el Psje. Francisco de Zela N° 150, Jesús María en los siguientes horarios: lunes a viernes de 08:30 horas a 16:30 horas (horario corrido).

Los entregables se presentarán con una carta dirigida al área usuaria, debiendo consignar el número de la orden de compra, adjuntando los documentos digitalizados en PDF o en físico, los cuales deben cumplir con los requisitos mínimos como:

- Documento principal dirigido al área usuaria.
- Firma (manuscrita, escaneada o digitalizada).
- Nombre y apellido de la persona que firma.
- Correo electrónico.
- Teléfono.
- Dirección.

7.5 Otras obligaciones del contratista:

El contratista es el responsable directo y absoluto de las actividades que realizará, ya sea directamente o a través de su personal, debiendo responder por el servicio brindado. Indicar, de ser necesario, otras obligaciones que serán asumidas por el contratista, que tengan incidencia directa en la ejecución del servicio.

7.6 Confidencialidad:

A la suscripción del contrato del servicio o a la recepción de la orden de servicio el CONTRATISTA queda obligado a no difundir, aplicar ni a comunicar a terceros la información fruto de la prestación del servicio, del análisis, implementación o cualquier otro aspecto relacionado a SERVIR. Esta obligación se mantendrá incluso después de la conclusión del contrato.

En tal sentido, el contratista deberá dar cumplimiento a todas las políticas y estándares definidos por la Entidad, en materia de seguridad de la información. Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido el servicio. Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, documentos y demás documentos e información compilados o recibidos por el contratista.

7.7 Propiedad Intelectual:

La Entidad tendrá todos los derechos de propiedad intelectual, incluidos sin limitación, las patentes, derechos de autor, nombres comerciales y marcas registradas respecto a los productos o documentos y otros materiales que guarden una relación directa con la ejecución del servicio o que se hubieren creado o producido como consecuencia o en el curso de la ejecución del servicio.

A solicitud de la Entidad, el contratista tomará todas las medidas necesarias, y en general, asistirá a la Entidad para obtener esos derechos.

8. Medidas de control durante la ejecución contractual:

- **Área que coordinara con el contratista:** La Subjefatura de Tecnologías de la Información.
- **Área responsable de la medida de control:** La Subjefatura de Tecnologías de la Información.
- **Área que brindará la conformidad:** La Subjefatura de Tecnologías de la Información.

9. Modalidad de pago:

La modalidad será a suma alzada.

10. Forma de pago:

El pago se realizará previa conformidad del servicio a cargo de la Sub Jefatura de Tecnologías de la Información de la OGAF, y se realizará en tres (3) armadas, distribuidas de la siguiente manera:

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

Entregable	Porcentaje del monto contractual
Primer Entregable	40 %
Segundo Entregable	30 %
Tercer Entregable	30 %

Posteriormente, y a requerimiento de la Subjefatura de Abastecimiento, el contratista deberá emitir y remitir el comprobante de pago en forma electrónica (factura, boleta de venta o recibo por honorarios, según corresponda) al correo electrónico institucional designado para tal fin.

11. Penalidad por mora:

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{Plazo}}$$

Donde F tiene los siguientes valores:

Para bienes y servicios: F = 0.40

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato, componente o ítem que debió ejecutarse o, en caso de que estos involucren entregables cuantificables en monto y plazo, al monto y plazo del entregable que fuera materia de retraso.

12. Otras penalidades:

NO APLICA.

13. Anticorrupción y Antisoborno:

EL POSTOR declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.
Asimismo, EL POSTOR se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL POSTOR se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación 34 y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL POSTOR se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta condición, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato[4]. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente condición conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco[5]. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar[6].

14. Solución de Controversias:

Todas las controversias que surjan entre las partes sobre los contratos menores se resuelven mediante conciliación, la cual se regula conforme a lo dispuesto en el numeral 81.3 del artículo 81 de la Ley N° 32069 - Ley General de Contrataciones Públicas.

15. Resolución del contrato:

Cualquiera de las partes puede resolver total o parcialmente el contrato menor, según corresponda, en los siguientes casos:

a) Incumplimiento de obligaciones contractuales, legales o reglamentarias a su cargo, pese a haber sido requerido para ello.
b) Caso fortuito o fuerza mayor, que imposibilite la continuación del contrato menor.
c) Hecho sobreviniente al perfeccionamiento del contrato, que imposibilite la continuación del contrato.
d) Por la presentación de documentación falsa y/o inexacta durante la indagación de mercado, la selección del proveedor o la ejecución contractual.

[4] Literal d) del Numeral 68.1 del Artículo 68 de la Ley N°32069, Ley General de Contrataciones Públicas.

[5] Literal d) del artículo 274 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.

[6] Numeral 122.6 del artículo 122 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

e) Por incumplimiento de la Cláusula Anticorrupción.
f) Haya llegado a acumular el monto máximo de la penalidad por mora o el monto máximo para otras penalidades, en la ejecución de la prestación a su cargo.
g) Paralice o reduzca injustificadamente la ejecución de la prestación, pese a haber sido requerido para corregir tal situación.
h) Por acuerdo entre las partes, siempre que la Entidad o el Contratista justifiquen las causas que imposibilitan continuar con la ejecución del contrato, previo pronunciamiento del área usuaria.

La comunicación de resolución será con carta simple, notificada al correo electrónico consignado en la oferta, la cual se entenderá recibida con la sola comunicación, sin que sea necesario acuse de recibo; salvo que, entre en vigencia la PLADICOP, en cuyo caso, las notificaciones se realizarán por dicho medio, teniendo los mismos efectos que la notificación física.

16. Responsabilidad por Vicios Ocultos:

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado por un plazo de un (01) año, contado a partir de la conformidad otorgada por el área usuaria.

17. Normativa específica:

NO APLICA

18. Cláusula Antisoborno:

i. La Autoridad Nacional del Servicio Civil, ente rector del Sistema Administrativo de Gestión de Recursos Humanos del Estado, como tal, impulsa una carrera pública meritocrática que propicie una cultura de integridad basada en la ética, valores y principios de los servidores y las servidoras civiles y promueva la profesionalización y la buena gobernanza del servicio público de calidad y orientado a la ciudadanía. En ese sentido, tenemos como filosofía la "tolerancia cero" frente al soborno y a otros actos de corrupción que involucren a funcionarios, directivos, servidores, proveedores, usuarios y otras partes interesadas de nuestra entidad".
ii. El proveedor/contratista se obliga a no efectuar algún pago, ni ofrecer o transferir algo de valor, a un funcionario o servidor, o cualquier tercero relacionado con el servicio o bien aquí establecido de manera que pudiese violar la Política de Integridad y Antisoborno de SERVIR.
iii. En forma especial, el proveedor / contratista acepta que no se encuentra inmerso en algún proceso de carácter penal vinculado a presuntos ilícitos penales contra el Estado Peruano, con el perfeccionamiento del contrato o la orden de servicio o la orden de compra.
iv. Asimismo, el proveedor/contratista se compromete a denunciar de manera oportuna cualquier acto de soborno o acto de corrupción del que tuviera conocimiento, a través del canal de denuncias: https://denuncias.servicios.gob.pe/?gobpe_id=354, o mediante el correo: integridad@servir.gob.pe, o a través de otros canales oficiales establecidos para la ciudadanía.

19. Cláusula de Cumplimiento:

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370

Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

www.servir.gob.pe
Pasaje Francisco de Zela 150
Piso 10, Jesús María
Lima 11, Perú
T: 51-1-2063370