TÉRMINOS DE REFERENCIA

SERVICIO DE ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE INTRUSIÓN PARA LA INFRAESTRUCTURA TECNOLÓGICA DE SEDAPAR SA.

1. DENOMINACIÓN DE LA CONTRATACIÓN

SERVICIO DE ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE INTRUSIÓN PARA LA INFRAESTRUCTURA TECNOLÓGICA DE SEDAPAR SA.

2. FINALIDAD PÚBLICA

Mejorar los controles de ciberseguridad en Sedapar SA, buscando fomentar una cultura de seguridad en el uso de herramientas digitales, reducir riesgos asociados a incidentes cibernéticos y cumplir con los estándares y normativas aplicables.

3. OBJETIVO DE LA CONTRATACIÓN

El presente proceso tiene por objetivo la contratación de un servicio especializado de Análisis de Vulnerabilidades y pruebas de intrusión para la Infraestructura tecnológica de Sedapar SA, el cual permitirá evaluar el nivel de seguridad en el sistema de defensa perimetral, redes, sistemas operativos, aplicaciones web publicadas, sistemas de información y equipos de comunicación.

4. ACTIVIDAD DEL POI

A04 - Análisis de vulnerabilidades y pruebas de intrusión de la plataforma tecnológica

5. CÓDIGO CATÁLOGO ÚNICO DE BIENES, SERVICIOS Y OBRAS(CUBSO)

8111220800255161, “SERVICIO DE ANALISIS DE VULNERABILIDAD DE ACTIVOS Y APLICACIONES WEB”

6. MODALIDAD DE PAGO

El contrato se rige por la modalidad de SUMA ALZADA, de conformidad con el artículo 130 del Reglamento.

7. PLAZO DE PRESTACIÓN DEL SERVICIO

El servicio materia de la presente convocatoria se prestan en el plazo de **45 DÍAS CALENDARIO**, en concordancia con lo establecido en la estrategia de contratación y el artículo 105 del Reglamento.

8. SISTEMA DE ENTREGA

NO APLICA

9. LUGAR DE ENTREGA

Se entregará en digital a través de mesa de partes virtual Sedapar SA accediendo a: https://sgd.sedapar.com.pe, dirigido al Jefe del Departamento de Tecnologías de Información y Comunicaciones.

10. LUGAR DE PRESTACIÓN DEL SERVICIO

El servicio se realizará en la Sede Central de SEDAPAR S.A., ubicado en Av. Virgen del Pilar 1701, de la ciudad de Arequipa.

El Proveedor deberá considerar todo el material necesario y equipamiento para el cumplimiento de sus tareas.

11. FORMA DE PAGO

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.

La entidad contratante paga las contraprestaciones pactadas a favor del contratista dentro de los diez días hábiles siguientes de otorgada la conformidad por parte del área usuaria, y es prorrogable, previa justificación de la demora, por cinco días hábiles.

En el caso que se haya suscrito contrato con un consorcio, el pago se realiza, a quien corresponda, de acuerdo con lo que se indique en el contrato de consorcio.

La recepción y la conformidad es responsabilidad del área usuaria (Dpto. Tecnologías de Información y Comunicaciones), quien se encargará de supervisar y dar la conformidad al cumplimiento del contrato, términos de referencia y demás obligaciones contractuales. El Dpto. TIC emitirá un informe de cumplimiento.

Para el pago, el Proveedor debe haber cumplido con remitir los entregables correspondientes de acuerdo a lo señalado en el numeral 15. Entregables.

PAGO EN TRES ARMADAS

Pagos	Porcentaje	N° Entregable
Primer Pago	10%	Entregable 01, que será entregado a los 07 días de iniciado el proyecto.
Segundo Pago	30%	Entregable 02, que será entregado a los 25 días de iniciado el proyecto
Tercer Pago	60%	Entregable 03, que será entregado a los 45 días de iniciado el proyecto.

Pago: Equivalente al 10%(Primer Pago), el 30%(Segundo Pago) y 60%(Tercer Pago) del monto total, dentro de los siete (07) días calendario posterior a la conformidad de la prestación por la entrega de cada entregable del servicio.

Para proceder con el pago se deberá presentar los siguientes documentos:

- Informe de Conformidad emitido por el Dpto. de Tecnologías de Información y comunicaciones.
- Comprobante de pago.

No se entregarán adelantos.

12. ADELANTOS

NO APLICA

13. TÉRMINOS DE REFERENCIA

DESCRIPCION DEL SERVICIO

ACTIVIDADES

El presente proyecto tiene la finalidad de evaluar el nivel de seguridad en las aplicaciones webs publicadas, activos internos de la red y aplicaciones móviles.

OBJETIVO GENERAL

Contratación de un servicio especializado de Análisis de Vulnerabilidades y pruebas de intrusión para la Infraestructura tecnológica de Sedapar SA, el cual permitirá evaluar el nivel de seguridad en el sistema de defensa perimetral, redes, sistemas operativos, aplicaciones web publicadas, sistemas de información y equipos de comunicación.

OBJETIVOS ESPECÍFICOS

- Identificar vulnerabilidades técnicas en la infraestructura tecnológica de SEDAPAR mediante herramientas de escaneo especializadas y pruebas de penetración controladas.
- Evaluar el nivel de exposición a ciberamenazas, simulando ataques reales (ethical hacking) bajo metodologías reconocidas (OWASP, NIST, OSSTMM, PTES).
- Fortalecer la seguridad de la infraestructura tecnológica mediante la detección temprana de fallas de configuración, accesos indebidos y riesgos de explotación.
- Proveer recomendaciones técnicas y estratégicas que permitan a SEDAPAR priorizar medidas de remediación y mitigación de riesgos de ciberseguridad.
- Contribuir a la cultura de seguridad de la información, concientizando sobre vulnerabilidades y riesgos, en cumplimiento de normativas y buenas prácticas internacionales en materia de ciberseguridad.

Las actividades de la **Fase IV Análisis de vulnerabilidades** estará constituida por los dispositivos de la red interna de SEDAPAR indicados en el **Anexo N°01**, con el fin de

lograr la identificación, clasificación de vulnerabilidades y/o debilidades presentes en los diferentes equipos, servidores, servicios y sistemas.

Las actividades de la **Fase V Pruebas Test de Intrusión,** se realizará sobre las direcciones web publicadas y a las aplicaciones móviles de SEDAPAR indicados en el **Anexo N°01.**

El Proveedor deberá utilizar las siguientes metodologías:

a) OSSTMM (Open-Source Security Testing Methodology Manual)

b) PTES (Penetration Testing Execution Standard)

c) OWASP Risk Rating Methodology

El Dpto. de Tecnologías de Información y Comunicaciones de SEDAPAR facilitará la información que sea necesaria para cada etapa de ejecución del servicio.

FASES DEL SERVICIO

La ejecución deberá desarrollarse siguiendo las siguientes fases:

I. Planeación y definición de mecanismos de seguimiento y control.
II. Identificación de los objetivos.
III. Levantamiento de Información (footprint, scanning y enumeración)
IV. Análisis de Vulnerabilidades.
V. Pruebas de Intrusión.
VI. Análisis de Resultados.

Fase I: Planeación y definición de mecanismos de seguimiento y control

El Proveedor y SEDAPAR SA acordarán las fechas de inicio y fin de cada una de las actividades contenidas en el plan de trabajo(contenidas dentro de los 45 días calendarios del servicio) y además establecerán los criterios de seguimiento y control de los resultados esperados.

Fase II: Identificación de los objetivos

El Proveedor debe realizar como primera etapa la identificación de los objetivos en base a la información suministrada por SEDAPAR SA.

Fase III: Levantamiento de Información (footprint, scanning y enumeración)

SEDAPAR SA, para las aplicaciones webs publicadas en internet facilitará únicamente el FQDN de acceso público indicadas en el Anexo N°01, el Proveedor realizará sus actividades desde una red externa a la institución, tal como un intruso lo podría realizar, así como el nombre de las aplicaciones móviles disponible para descargar en las

tiendas digitales de aplicaciones. Para los activos internos de la red, SEDAPAR brindará la lista de direcciones IPs internas y las facilidades de acceso para que el Proveedor realice sus actividades dentro de la red de SEDAPAR SA; estas actividades podrán realizarse de manera presencial y/o virtual. Ver Anexo 01.

Fase IV: Análisis de las vulnerabilidades

El Análisis de Vulnerabilidades comprende pruebas automatizadas para descubrir potenciales vulnerabilidades en los equipos de la red interna de SEDAPAR, aplicaciones webs publicadas y aplicaciones móviles. Dependiendo de la información de la fase anterior, el Proveedor realizará las pruebas de vulnerabilidad. El análisis de vulnerabilidades como mínimo debe incluir las siguientes actividades:

a) Recopilar la mayor cantidad de información susceptible de ser utilizada por un posible atacante.

b) Escaneo de puertos, identificación de servicios y sistemas operativos.

c) Determinar, utilizando herramientas, las deficiencias de seguridad que existen en los sistemas incluidos dentro del servicio.

d) Para las aplicaciones web publicadas en el ANEXO N°01, se debe contemplar como mínimo los siguientes tipos de ataques:

- Desbordamiento de Búffer
- Comunicaciones inseguras
- Manejo inadecuado de errores
- Lenguaje de comandos entre distintos sitios (XSS)
- Control de Acceso Inapropiado (por ejemplo, no seguras, sin restricción de acceso a URL y exposición completa de directorios
- Falsificación de solicitudes entre distintos sitios (CSRF)

Para la ejecución de las actividades de la presente fase, a solicitud y en coordinación con la empresa proveedora, SEDAPAR podrá proporcionar recursos virtuales y/o servidores necesarios, así como las facilidades de comunicación dentro de su red institucional y la conectividad hacia los activos detallados en el Anexo N°01. Sobre dicha infraestructura provista por la Entidad, el Proveedor realizará las actividades del servicio haciendo uso de sus propias herramientas, plataformas y soluciones de software especializadas

Las actividades podrán ser realizadas de manera virtual, para lo cual SEDAPAR brindará las facilidades de conectividad que requiera el Proveedor, incluyendo la comunicación dentro de la red institucional y el acceso remoto a los activos necesarios para la correcta ejecución del servicio.

El Proveedor deberá proporcionar a la Entidad toda la información técnica necesaria (como direcciones IP, rangos de red, puertos y protocolos utilizados por las

herramientas de escaneo) con la finalidad de que SEDAPAR realice las configuraciones y exclusiones correspondientes en sus equipos y soluciones de seguridad implementadas.

En caso sea necesario, Sedapar brindará un espacio físico para equipamiento y/o herramientas del Proveedor.

Estas acciones deberán garantizar que las tareas de escaneo de vulnerabilidades y pruebas de seguridad puedan ejecutarse de manera completa y sin interferencias.

Fase V: Pruebas Test de intrusión a las Aplicaciones Web publicadas y aplicaciones móviles.

En base al resultado de la **Fase IV Análisis de Vulnerabilidades**, el test de intrusión (Pruebas dinámicas – DAST entre otras) será realizado a las aplicaciones web públicas y aplicaciones móviles descritas en el ANEXO N°01, generando resultados, las cuales deben incluir la entrega de un informe técnico detallado que contenga como mínimo los siguientes elementos:

- ➢ Descripción de las pruebas realizadas.
- ➢ Listado de deficiencias de seguridad evidenciados mediante el análisis DAST.
- ➢ Recomendaciones para su mitigación

El informe a presentar formará parte del informe final del servicio.

Referida a la Evaluación de Seguridad de Aplicaciones

Según Anexo N°01 – Relación de Aplicaciones

- La ejecución del servicio no debe causar daño alguno en el funcionamiento de los sistemas o en el desempeño de la red de datos de la Entidad. Así mismo bajo ninguna circunstancia y momento se generará algún tipo de cambio sobre los sistemas y/o información a las que se logre acceso (salvo que sean generados por los registros de acceso y actividades del sistema).
- Las aplicaciones web publicadas (externas) serán evaluadas con las URL entregadas (Caja gris o Greybox).
- Las vulnerabilidades detectadas deben de disponer de trazabilidad a fin de que la Entidad disponga de las evidencias respectivas.
- Las vulnerabilidades comprobadas deberán ser calificadas aplicando el sistema “Common Vulnerability Score System” (CVSS) tanto a nivel cuantitativo como cualitativo.
- Pruebas de penetración para Aplicaciones Web y Aplicaciones móviles. Esta se deberá realizar una vez, y se deberá hacer entrega de un reporte terminado el servicio. Los reportes serán técnicos como ejecutivos.

- Se deben incluir las siguientes pruebas para las aplicaciones webs publicadas:

  - ➢ Errores de inyección SQL
  - ➢ Errores de comandos OS, LDAP y XPATH

➢ Desbordamiento de buffer
➢ Comunicaciones inseguras
➢ Manejo inadecuado de errores
➢ Errores del tipo XSS
➢ Evaluar Cross Site Scripting basados en DOM (Document Object Model)
➢ Control de acceso inapropiado (por ejemplo, no seguras, sin restricción de acceso a URL y exposición completa de directorios
➢ Falsificación de solicitudes entre distintos sitios (CSRF)
➢ Evaluar cifrados débiles de SSL/TSL, protección protecciones insuficientes en el transporte
➢ Evaluar información sensible enviada por canales no encriptados.
➢ Evaluar la ejecución de JavaScript
➢ Evaluar redirecciones de URL en el Lado Cliente
➢ Evaluar inyecciones de HTML
➢ Evaluar inyecciones de CSS
➢ Evaluar la manipulación de recursos del Lado Cliente
➢ Evaluar "Cross Origin Resource Sharing"
➢ Evaluar "Cross Site Flashing"
➢ Evaluar "Clickjacking"
➢ Evaluar WebSockets
➢ Evaluar "Web Messaging" (Cross Document Messaging)
➢ Evaluar almacenamiento local
➢ Evaluar inyecciones de LDAP
➢ Evaluar inyecciones en datos generados por una herramienta ORM (Object Relational Mapping)
➢ Evaluar inyecciones de XML
➢ Evaluar inyecciones de SSI
➢ Evaluar inyecciones de XPath
➢ Evaluar inyecciones IMAP/SMTP
➢ Evaluar inyecciones de código
➢ Evaluar inyecciones de comandos
➢ Evaluar desbordamiento de buffer
➢ Evaluar vulnerabilidades incubadas
➢ Evaluar la división y/o encubrimiento de tráfico HTTP
➢ Análisis de códigos de error
➢ Análisis de trazados de pila
➢ Evaluar Cross Site Scripting Almacenado
➢ Evaluar la manipulación de verbos HTTP
➢ Evaluar la "contaminación" de parámetros HTTP
➢ Evaluar el recorrido de directorios/inclusión de archivos
➢ Evaluar la evasión del esquema de autorización
➢ Evaluar el escalamiento de privilegios
➢ Evaluar las referencias inseguras a objetos de forma directa

➢Revisar archivos con Metadata en búsqueda de divulgación de información

➢ Enumerar las aplicaciones en el servidor web

➢ Revisar los comentarios y Metadata de las páginas web buscando divulgación de información

➢ Identificar los puntos de entrada de las aplicaciones

➢ Mapear las rutas de ejecución a través de las aplicaciones

➢ Evaluar los métodos HTTP

➢ Evaluar la seguridad estricta en el transporte vía HTTP

Referidas a las Pruebas de Intrusión

El servicio consiste en conducir un ataque real de manera controlada en sistemas conectados a Internet designados por la SEDAPAR SA, así como otros activos para identificar riesgos críticos del negocio, analizar y documentar el ataque, dar prioridad y destacar los riesgos a la seguridad identificada y las acciones correctivas.

El alcance de estas pruebas se realizará en 08 direcciones webs publicadas y 01 aplicación móvil dirigida a Android y iOS.

El servicio deberá incluir:

- Intentar obtener acceso directo a datos confidenciales y a privilegios de acceso de administrador o elevados en sistemas vulnerables.
- Intentar escalar accesos a otros equipos de la red interna.
- Demostrar debilidades específicas o sistemáticas en la seguridad si están presentes.

Los métodos utilizados para demostrar dichas debilidades deben incluir:

- Explotación de credenciales de inicio de sesión usando recursos públicos.
- Hacking de contraseña con fuerza bruta directamente contra aplicaciones.
- Explotación de vulnerabilidades de “buffer overflow” y “formatstring”
- SessionHijacking (si es posible).
- Vulnerabilidades de aplicación Web incluyendo “SQL Injection”, “XPATH injection”, validación de entrada inadecuada y errores de lógica de aplicación.

Fase VI: Análisis de Resultados

Dentro de esta fase el especialista de las pruebas y el Jefe del proyecto realizarán una exposición presencial de los resultados obtenidos para determinar el nivel de exposición, lo cual se plasmará en un informe ejecutivo el cual formará parte del informe Final del Servicio.

DE LA METODOLOGÍA DEL SERVICIO

Metodología para el Hackeo Ético

Durante la realización del Ethical Hacking el equipo deberá emplear las metodologías basados en estándares como los desarrollados por Common Criteria (Common Criteria for Information Technology Security Evaluation, Supplemment: Vulnerability Analisys and Penetration Testing), PTES (Penetration Testing Execution Standard) así como la Open Source Security Testing Methodology Manual (OSSTMM).

Asimismo, se podrá admitir otras pruebas complementarias o metodologías a sugerencia del postor, previa evaluación y aprobación del supervisor de pruebas de SEDAPAR Sede Central.

LABORES DEL PROVEEDOR

a. El Proveedor deberá presentar un plan de trabajo a los cinco (5) días calendarios contados a partir del día siguiente de suscrito el contrato, dicho plan permitirá describir las tareas y actividades a realizarse para la prestación del servicio , sujeto a revisión por parte de Sedapar SA, el cual tendrá dos (02) días calendario para aprobarlo; de presentarse alguna observación deberá ser subsanada por el contratista en un plazo no mayor de dos (02) días calendario; este plazo no será computable respecto al plazo total.

b. El Proveedor se compromete a no violar la confidencialidad, seguridad y propiedad de los archivos, programas y sistemas de aplicación que existan al interior de la entidad.

c. Sedapar SA brindará todas las facilidades para realizar la planificación y el despliegue de la solución.

14. REQUISITOS MÍNIMOS DEL PROVEEDOR

El Postor deberá ser una empresa natural o jurídica, debidamente constituida, estar inscrita y habilitada en el Registro Nacional de Proveedores de Estado.

El Postor debe acreditar un monto facturado acumulado equivalente a mínimo 03 veces el monto del producto a ofertar, por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (08) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran bienes similares a los siguientes:

Servicios de implementación de normas de seguridad de información y/o ciberseguridad y/o privacidad y/o continuidad de negocios y/o Auditoría de sistemas de información y/o recuperación de desastres, o consultorías de seguridad de información en general.

PERSONAL DEL PROVEEDOR

Se requiere un equipo de trabajo que está compuesto por los siguientes roles (la misma persona no desempeña más de un rol):

Formación Académica:

01 Jefe de Proyecto

Un (01) Profesional titulado en Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería de Telecomunicaciones; deberá estar colegiado y habilitado al momento de la presentación de la propuesta.

01 Especialista Ethical Hacking

Bachiller o Título Profesional en las especialidades de: Computación y/o Computación y Sistemas y/o Sistemas y/o Informática y/o Electrónica y/o Telecomunicaciones

Capacitaciones:

01 Jefe de Proyecto

Certificado de estudios en: Gestión de Proyectos y/o certificación PMP vigente

(Project Management Professional).

Especialista Ethical Hacking

Que cuente con al menos cuatro(04) de las siguientes certificaciones:

Offensive Securtity Certified Professional (OSCP)
Certified Ethical Hacking Master (EC-Council CEH Master)
Certified Read Team Professional (CRTP)
Computer Hacking Forensic Investigator EC-Council (CHFI)
Certified Professional Penetration Tester (eCPPT)
Certifiel AI/ML Pentester
Certified Incident Responder (eCIR)
Web Application Penetation Extremme (eWPTX)

Acreditación:

Se acreditará con copia simple de certificados.

Experiencia:

01 Jefe de Proyecto

Experiencia mínima de dos (02) años en Gestión de Proyectos de Tecnologías de la Información.

01 Especialista Ethical Hacking

Experiencia mínima de tres (03) años en implementaciones y/o consultorías y/o en puestos relacionados con seguridad de la información y/o ciberseguridad y/o ethical hacking y/o Pentest y/o seguridad informática

Acreditación:

Se acreditará con copia simple de certificados de trabajo.

NOTA IMPORTANTE:

Los documentos que acrediten en idioma distinto al castellano deberán adjuntar la traducción de acuerdo con el reglamento de la ley de contrataciones del estado.

15. ENTREGABLES

Primer Entregable:

Plan de trabajo a presentarse dentro de **los 07 (Siete) días calendarios** de iniciado el servicio.

El Proveedor deberá presentar obligatoriamente su plan de trabajo, conteniendo como mínimo lo siguiente: objetivo, metas, cronograma detallado de actividades, datos del personal clave que realizará las actividades, el cual debe ser entregado dentro de los siete (07) días calendarios siguientes a la fecha de firma del contrato.

Dentro de los 04 días calendarios posteriores a la presentación del plan de trabajo, se deberá realizar la primera reunión de inicio de actividades:

- Se determinarán las necesidades de información para el desarrollo de las actividades del servicio.
- Al inicio de la prestación se le proporcionará al Proveedor, la relación de los activos a evaluar, sin embargo, la Entidad previo a la evaluación podrá solicitar el cambio sin superar la cantidad de activos indicados.

Segundo Entregable:

A presentarse a los 25(veinte y cinco) días calendarios de iniciado el servicio:

a. Informe Parcial:

Debe contener lo siguiente:

- Informes y Resultados de la Fase I, Fase II y Fase III.

Tercer Entregable:

A presentarse a los 45(cuarenta y cinco) días calendarios de iniciado el servicio:

b. Informe Final:

Deberá contener lo siguiente:

- Resultados de la Fase IV, Fase V y Fase VI.
- Justificación de cada una de las actividades contenidas en los términos de referencia.
- Recomendaciones para la mejora de la seguridad sobre las debilidades o falencias encontradas durante la evaluación de seguridad realizada.
- Recomendaciones respecto de la configuración de la infraestructura física y/o lógica del presente análisis respecto de incidentes de seguridad.

16. PENALIDADES

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, de conformidad con el artículo 120 del Reglamento.

17. FORMA DE PAGO

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.

La entidad contratante paga las contraprestaciones pactadas a favor del contratista dentro de los diez días hábiles siguientes de otorgada la conformidad por parte del área usuaria, y es prorrogable, previa justificación de la demora, por cinco días hábiles.

En el caso que se haya suscrito contrato con un consorcio, el pago se realiza, a quien corresponda, de acuerdo con lo que se indique en el contrato de consorcio.

La recepción y la conformidad es responsabilidad del área usuaria (Dpto. Tecnologías de Información y Comunicaciones), quien se encargará de supervisar y dar la conformidad al cumplimiento del contrato, términos de referencia y demás obligaciones contractuales. El Dpto. TIC emitirá un informe de cumplimiento.

Para el pago, el Proveedor debe haber cumplido con remitir los entregables correspondientes de acuerdo a lo señalado en el numeral XII. Entregables.

PAGO EN TRES ARMADAS

Pagos	Porcentaje	N° Entregable
Primer Pago	10%	Entregable 01, que será entregado a los 07 días de iniciado el proyecto.
Segundo Pago	30%	Entregable 02, que será entregado a los 25 días de iniciado el proyecto
Tercer Pago	60%	Entregable 03, que será entregado a los 45 días de iniciado el proyecto.

Pago: Equivalente al 10%(Primer Pago), el 30%(Segundo Pago) y 60%(Tercer Pago) del monto total, dentro de los siete (07) días calendario posterior a la conformidad de la prestación por la entrega de cada entregable del servicio.

Para proceder con el pago se deberá presentar los siguientes documentos:

- Informe de Conformidad emitido por el Dpto. de Tecnologías de Información y comunicaciones.
- Comprobante de pago.

No se entregarán adelantos.

18. CONFORMIDAD DEL SERVICIO Y TRÁMITE DE PAGO

El Dpto. de Tecnologías de Información y Comunicaciones otorgará la conformidad una vez concluida el servicio, con previa presentación por parte del proveedor, de los entregables del punto 15), e informe del área técnica Tecnologías de Información y Comunicaciones. La conformidad no excederá los siete (07) días calendarios luego de recibir el informe final del Proveedor.

19. PROPIEDAD INTELECTUAL

La Entidad tendrá todos los derechos de propiedad intelectual, incluido 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 hubiere entregado o producido como consecuencia o en el curso de la ejecución del servicio.

20. CONFIDENCIALIDAD

- El Proveedor se compromete a mantener absoluta reserva, y no revelar a tercero alguno, toda información que le sea suministrada por este último, excepto cuando sea estrictamente necesario para el cumplimiento del Contrato (por ejemplo, cuando empleados lleven a cabo en adelante los trabajos de instalación y mantenimiento de los servicios).
- El Proveedor se compromete a no revelar ni permitir la revelación de cualquier detalle a terceros, no revelar que SEDAPAR es cliente del postor con relación con el servicio y a no usar el nombre de SEDAPAR en cualquier promoción, publicidad o anuncio, sin previa autorización del representante legal de SEDAPAR.
- No será de aplicación a la información confidencial los siguientes supuestos:
  - Que resulte accesible al público por otros medios distintos al contratista.
  - Que haya sido publicada con anterioridad a la fecha de la firma del contrato.
  - Que obre ya en poder de la parte receptora y no esté sujeta a cualquier otro impedimento o restricción puesto de manifiesto a la otra parte en el momento de la revelación o luego de ella,
  - Que sea recibida a través de terceros sin restricciones y sin que implique incumplimiento del Contrato.
  - Que sea independientemente desarrollada por la parte receptora, siempre que no se hubiese utilizado para ello la Información confidencial proporcionada por la otra parte.
  - Que deba ser revelada para dar cumplimiento de una orden de naturaleza judicial o administrativa, en cuyo caso la parte receptora deberá informar a la otra parte en forma inmediata a la sola recepción de la citada orden.

21. CLÁUSULA ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción de este contrato, EL CONTRATISTA 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 CONTRATISTA 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 CONTRATISTA 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 proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación[1] 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 CONTRATISTA 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.

[1] Artículo 9 de la Ley N°32069, Ley General de Contrataciones Públicas.

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 cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato[2]. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco[3]. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar[4].

22. SOLUCIÓN DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, cuando se haya pactado, y arbitraje.

Para el arbitraje, el postor ganador de la buena pro selecciona a una de las siguientes Instituciones Arbitrales para administrar el arbitraje:

1. Cámara de Comercio e Industria Arequipa
2. AD HOC Centro Especializado en solución de controversias
3. MARC Perú Asociación para la prevención y solución de conflictos.

23. RESOLUCIÓN DE CONTRATO POR INCUMPLIMIENTO

Se aplicará el Artículo 122 del Sub Capitulo III Incumplimiento del contrato del Capitulo V Disposiciones generales de ejecución contractual para bienes y servicios del Reglamento de la Ley General de Contratación Públicas.

24. CLAUSULA MEDIO AMBIENTAL

La ejecución del servicio debe garantizar la sostenibilidad ambiental, evitar impactos ambientales negativos

El contratista podrá proponer un plan de mitigación del polvo, ruido y grasas durante el desarrollo de las actividades, asimismo, después de culminado el servicio, deberá dejar el lugar de trabajo limpio y libre de residuos, basura y grasas.

---

[2] Literal d) del Numeral 68.1 del Artículo 68 de la Ley N°32069, Ley General de Contrataciones Públicas.
[3] Literal d) del artículo 274 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas

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

25. GESTIÓN DE RIESGOS

Categoría	Riesgo
Operacional / Disponibilidad	Interrupción del servicio: Las pruebas (exploits, escaneos agresivos o pruebas de carga) podrían provocar caídas o degradación de sistemas en producción.
Confidencialidad / Privacidad	Exposición o fuga de datos sensibles: Durante las pruebas se podrían acceder, copiar o dejar expuestos datos personales o corporativos (por ejemplo, credenciales, registros).
Legal / Cumplimiento	Ejecución fuera de autorización: El equipo de pruebas podría explorar sistemas no autorizados o ir más allá del alcance acordado, generando consecuencias legales.
Seguridad / Operacional	Detección como actor malicioso por terceras defensas: Herramientas de monitoreo, SOC o terceros proveedores podrían confundir las pruebas con un ataque real, activando respuestas automáticas (bloqueos, escalado).
Reputacional	Daño a la reputación institucional: Si las pruebas causan incidentes visibles para clientes o empleados, o si se filtra información sobre vulnerabilidades antes de remediarlas, la imagen de la organización puede verse afectada.
Operacional / Seguridad interna	Pérdida o compromiso de credenciales de prueba: Credenciales, claves SSH o tokens utilizados por los pentesters pueden ser almacenados inseguramente y luego reutilizados por actores maliciosos.
Proyecto / Riesgo humano	Insuficiente preparación técnica o recursos del equipo: El equipo interno o el proveedor pueden carecer de experiencia, herramientas o tiempo, lo que reduce la calidad de los hallazgos y recomendaciones.

26. RESPONSABILIDAD POR VICIOS OCULTOS

La recepción conforme de la prestación por parte de SEDAPAR no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la ley N°32069, Ley general de contrataciones públicas y el artículo 144 de su reglamento.

El plazo máximo de responsabilidad del contratista es de un (01) año contado a partir de la conformidad otorgada por SEDAPAR.

ANEXO N° 01

Fase V: Pruebas de test de intrusión:

Relación de Aplicaciones webs publicadas:

- ov.sedapar.com.pe
- sgd.sedapar.com.pe
- ctx.sedapar.com.pe
- gis.sedapar.com.pe
- mail.sedapar.com.pe
- gis2.sedapar.com.pe
- visitas.sedapar.com.pe
- comercial.sedapar.com.pe

Relación de aplicaciones móviles

Item	Aplicación	Sistema Operativo
1	ov sedapar	Android
2	ov sedapar	iOS

Fase IV: Análisis de Vulnerabilidades:

Relación de host internos:

Item	IP
1	10.1.0.5
2	10.1.0.9
3	10.1.0.89
4	10.1.0.8
5	10.1.0.3
6	10.1.0.10
7	10.1.0.4
8	10.1.0.8
9	10.1.0.41
10	10.1.0.47
11	10.1.0.50
12	10.1.0.60
13	10.1.0.73
14	10.1.0.74
15	10.1.0.25
16	10.1.0.26
17	10.1.0.27

18	10.1.20.7
19	10.1.0.133
20	10.1.0.29