

TÉRMINOS DE REFERENCIA

I. DENOMINACIÓN DE LA CONTRATACIÓN:

SERVICIO PARA LA IMPLEMENTACIÓN DE UN NUEVO SISTEMA DE INFORMACIÓN Y GESTIÓN DE ESTADÍSTICAS PERIÓDICAS – SIGEP

II. POI

Mejorar las soluciones tecnológicas para dar soporte a los servicios informáticos desplegados en la Institución.

III. ÁREA USUARIA

Dirección de Políticas Regulatorias y Competencia (DPRC)

IV. ÁREA TÉCNICA

Oficina Técnica de Información (OTI)

V. FINALIDAD PÚBLICA

Contratar el servicio de una consultoría para el desarrollo e implementación de la nueva versión del Sistema de Información y Gestión de Estadísticas Periódicas (SIGEP), considerando la entrada en vigencia de la Norma de Requerimientos de Información Periódica aprobada mediante Resolución de Consejo Directivo N° 043-2022-CD/OSIPTEL¹, esto con el objetivo de obtener información periódica exacta, completa y actualizada sobre la realidad y evolución del mercado de telecomunicaciones, para desarrollar adecuadamente las labores de monitoreo y supervisión del sector.

VI. ANTECEDENTES

El sector telecomunicaciones es un sector muy dinámico como consecuencia del desarrollo tecnológico, la diversificación en la oferta comercial, y los cambios en la dinámica competitiva. Bajo este contexto, es esencial que el OSIPTEL cuente con información periódica exacta, completa y actualizada sobre la realidad y evolución del mercado de telecomunicaciones, para desarrollar adecuadamente sus labores de monitoreo y supervisión del sector, efectuar análisis y estudios previos a la toma de decisiones regulatorias y normativas, así como evaluar los efectos de las medidas aplicadas en el sector.

En ese sentido, en el marco de las facultades previstas en los artículos 5, 6 y 13 de la Ley de Desarrollo de las Funciones y Facultades del OSIPTEL, Ley N° 27336, este Organismo emitió la Norma de Requerimientos de Información Periódica (NRIP), aprobada por Resolución de Consejo Directivo N° 121-2003-CD/OSIPTEL y modificada con resoluciones N° 024-2009-CD/OSIPTEL, N° 050-2012-CD/OSIPTEL y N° 096-2015-CD/OSIPTEL, y cuya nueva versión ha sido aprobada mediante Resolución de Consejo Directivo N° 043-2022-CD/OSIPTEL.

Cabe precisar que el 11 de julio de 2012, el OSIPTEL firmó el contrato N° 014-2012/OSIPTEL, para la contratación de la “Consultoría para la implementación de un sistema de información que gestione las estadísticas periódicas reportadas por las empresas operadoras al OSIPTEL”, como resultado del proceso de Adjudicación

¹ <https://www.osiptel.gob.pe/n-043-2022-cd-osiptel/>



de Menor Cuantía N° 006-2012/OSIPTEL – IV Convocatoria, derivada de la Adjudicación Pública N° 007-2011/OSIPTEL. Como resultado de dicha consultoría, se desarrolló la versión vigente del SIGEP, la cual debe ser actualizada como consecuencia de la nueva versión de la NRIP.

VII. OBJETO DEL SERVICIO

Contratar el servicio de desarrollo e implementación de la nueva versión del SIGEP que permita la gestión de las estadísticas periódicas reportadas por las empresas operadoras al OSIPTTEL, en cumplimiento a lo establecido en la Norma de Requerimientos de Información Periódica aprobada mediante Resolución de Consejo Directivo N° 043-2022-CD/OSIPTTEL (en adelante, la nueva NRIP), siendo que a partir de febrero de 2023 las empresas operadoras del sector telecomunicaciones deben reportar información periódica conforme a los formatos establecidos en los Anexos I y II de la nueva NRIP.

VIII. DESCRIPCIÓN DE LA PRESTACIÓN PRINCIPAL

La implementación de un nuevo SIGEP, en el marco del presente proceso de contratación, contempla el desarrollo y ejecución del módulo de “Administración Central”.

El módulo de “Administración Central” del nuevo SIGEP debe contemplar la gestión de reportes, asignación y descarga de formatos, así como el procesamiento, almacenamiento, mantenimiento de la información de la base de datos del nuevo SIGEP, entre otras funcionalidades detalladas en los requerimientos funcionales.

A continuación, se detallan los requerimientos funcionales del módulo:

REQUERIMIENTOS FUNCIONALES

Nº	Requerimientos Funcionales
1	Asignación, carga y reportes de información empleando el nuevo SIGEP
1.1	Se debe contar con un perfil “Administrador”, el cual debe permitir: <ul style="list-style-type: none"> (i) Realizar la asignación de formatos a las empresas operadoras (ii) Descargar los formatos reportados por las empresas operadoras. (iii) Consultar el estado de reportes efectuados por las empresas operadoras. (iv) Agregar, modificar o eliminar formatos, e incorporar nuevos requerimientos de información. (v) Crear perfiles para uso del Sistema, y a los usuarios dentro de cada perfil.
1.2	Se debe contar con un perfil “Empresa”, el cual debe permitir al usuario designado por cada empresa: <ul style="list-style-type: none"> (i) Ingresar al SIGEP, mediante la autenticación del nombre de usuario y contraseña correspondiente. (ii) Consultar y descargar los formatos que tiene asignados la empresa para cada periodo de reporte. (iii) Cargar y reportar la información mediante la selección del periodo



Nº	Requerimientos Funcionales
	<p>de reporte, y del tipo de proceso (Proceso Normal, Proceso de rectificación a solicitud del OSIPTEL, y Proceso de rectificación a solicitud de la Empresa).</p> <p>(iv) Verificar el estado de sus reportes de información (estado “Observado”, “Validado” y “Registrado”).</p> <p>(v) Descargar los reportes de información que han alcanzado el estado de “Registrado” en el nuevo SIGEP.</p>
1.3	<p>Se debe contar con un perfil “Usuario Interno”, el cual debe permitir:</p> <p>(i) Ingresar al SIGEP, mediante la autenticación del nombre de usuario y contraseña correspondiente.</p> <p>(ii) Descargar los formatos reportados por las empresas operadoras, considerando únicamente a aquellos que previamente el Administrador del SIGEP haya determinado.</p> <p>(iii) Consultar el estado de reportes efectuados por las empresas operadoras.</p>
1.4	<p>Se debe contar con un mecanismo ágil de asignación de formatos por cada empresa operadora, a partir de los servicios que brinda al mercado.</p> <p>Una vez realizada la referida asignación, ésta debe aplicarse automáticamente para todos los periodos de reporte considerando la periodicidad de entrega de cada formato. Asimismo, el mecanismo de asignación debe permitir modificar en cualquier momento la referida asignación.</p> <p>Para la asignación de formatos, se debe considerar variables como las siguientes: empresa, periodo de reporte, fechas de inicio y vencimiento, tipo de proceso (Proceso Normal, Proceso de rectificación a solicitud del OSIPTEL, y Proceso de rectificación a solicitud de la Empresa), código del formato, etc.</p>
1.5	<p>El SIGEP debe permitir crear los usuarios del perfil “Empresa”, solo a aquellas empresas que se encuentren registradas en la “Base de datos Única de Empresas” del Osipitel. Se debe considerar que, la “Base de datos Única de Empresas” puede cambiar en el tiempo y el sistema debe permitir gestionar este cambio.</p>
1.6	<p>El sistema debe contar con una opción que permita al Administrador del SIGEP establecer los tipos de archivos que se pueden cargar en dicho sistema. En primer lugar, debe permitir cargar los tipos de archivo establecidos en los formatos de reporte señalados en el Anexo II de la nueva NRIP: Excel (.xls, .xlsx), GIS (shp), Google Earth (kml, kmz), Documentos (pdf, docx, doc), zip, rar, pptx. En segundo lugar, debe permitir cargar otros tipos de archivo que el Administrador del SIGEP establezca, como por ejemplo formatos con extensión de base de datos (dta, csv, sql, txt, json, etc.).</p>
1.7	<p>Se debe contar un mecanismo que efectúe la “validación de forma” de los formatos reportados por las empresas operadoras, a fin de considerar las razones señaladas en la sección 4.1.1 del Anexo IV de la NRIP y asegurar que se respete la estructura del formato, sus valores permisibles (los cuales</p>



Nº	Requerimientos Funcionales
	<p>son detallados a nivel de cada formato en el Anexo II de la nueva NRIP), etc.</p> <p>En caso de que existan formatos de reporte cuya información no haya superado el proceso de validación de forma, el sistema debe permitir a la empresa corregir y cargar nuevamente los formatos, previa anulación de los formatos observados, de conformidad a lo establecido en la sección 4.1.1 del Anexo IV de la nueva NRIP.</p>
1.8	Adicionalmente, el proceso de “validación de forma”, debe considerar el “Directorio Institucional de Centros Poblados” (DICCOP) del OSIPTEL, a fin de realizar la validación respecto a los campos de los reportes de información que refieren a desagregación geográfica (provincia, distrito, centro poblado). Así también, se debe considerar que el DICCOP puede cambiar en el tiempo y el sistema debe permitir gestionar este cambio.
1.9	Se debe contar con un mecanismo automático de constancia de entrega de reportes de información (mediante correo electrónico remitido al usuario designado por la empresa y al Administrador del SIGEP), cuando la empresa haya cumplido con reportar dicha información a través del nuevo SIGEP.
1.10	Se debe contar con un mecanismo que permita a las empresas efectuar la rectificación de sus formatos reportados, considerando que dicha rectificación puede ser requerida por el OSIPTEL (Proceso de rectificación a solicitud del OSIPTEL), o solicitada por la empresa (Proceso de rectificación a solicitud de la Empresa). Asimismo, toda rectificación debe ser previamente autorizada por el Administrador del SIGEP.
1.11	Se debe contar con un mecanismo que permita al Administrador del SIGEP descargar los formatos reportados por las empresas operadoras, ordenados en carpetas y subcarpetas (a nivel del periodo de reporte, empresa operadora, fecha de reporte, tipo de proceso, formato reportado, etc.), según se coordine con la Dirección de Políticas Regulatorias y Competencia (DPRC).
1.12	<p>Se debe contar con un mecanismo que permita al Administrador del SIGEP realizar la consulta del estado de reportes efectuados por las empresas operadoras, con el fin de determinar a nivel de cada empresa el porcentaje y número de formatos reportados respecto a la cantidad de formatos que tiene asignados.</p> <p>Asimismo, el sistema debe permitir generar un reporte que muestre el detalle de la información reportada y no reportada por la empresa operadora. La estructura del reporte en mención será proporcionada por el OSIPTEL.</p>
1.13	El sistema debe ser lo suficientemente flexible de modo que permita al Administrador del SIGEP la modificación y eliminación de formatos, así como la incorporación de nuevos requerimientos de información.
1.14	El sistema debe permitir la incorporación de nuevos módulos de reporte de información, que permita a las empresas remitir cualquier tipo de información al OSIPTEL, adicionales a lo requerido en el marco de la NRIP.
2	Generación y gestión de base de datos del nuevo SIGEP



Nº	Requerimientos Funcionales
2.1	<p>La información reportada por las empresas operadoras debe ser almacenada en base de datos.</p> <p>La base de datos del nuevo SIGEP debe contar con un diseño óptimo, y debe ser desarrollada con las mejores prácticas de diseño de Base de Datos.</p> <p>Asimismo, la base de datos del nuevo SIGEP debe permitir su adaptabilidad para que sea explotada con cualquier software de explotación de base de datos.</p>
2.2	<p>El sistema debe contar con un mecanismo flexible de procesamiento, almacenamiento y mantenimiento de la base de datos del nuevo SIGEP.</p> <p>Para tal efecto, se debe incorporar un entorno de trabajo que permita realizar fácilmente la explotación y uso de la base de datos, el cual por lo menos debe considerar lo siguiente:</p> <ol style="list-style-type: none"> Opciones para crear y/o modificar el procesamiento de los formatos de entrega de información (así por ejemplo, procesos ETL: <i>Extraction-Transform-Load</i>) y los elementos de la explotación de la información. Que los formatos bajo los cuales las empresas operadoras reportarán periódicamente pueden variar de acuerdo a cambios en los requerimientos de información.
2.3	<p>El sistema debe contar con un módulo de gestión de información histórica, de modo que permita al OSIPTEL realizar copias de respaldo y/o restauración (carga de archivos) de data histórica reportada por las empresas operadoras a través del nuevo SIGEP.</p>

REQUERIMIENTOS NO FUNCIONALES

Nº	Requerimientos
1	<p>Confiabilidad</p> <ul style="list-style-type: none"> Incorporar mecanismos que garanticen la integridad de los datos reportados por las empresas operadoras; es decir, que la información reportada por las empresas sea almacenada sin alteraciones en el nuevo SIGEP. Optimizar los tiempos de respuesta en la ejecución de las consultas. Controlar adecuadamente los errores producidos y todos los potenciales errores que podrían generarse.
2	<p>Seguridad</p> <p>2.1. ANÁLISIS Y DISEÑO</p> <p>2.1.1. AUTENTICACIÓN</p> <ol style="list-style-type: none"> El software desarrollado para OSIPTEL debe de autenticarse a través de protocolos que garanticen que las credenciales son transmitidas de forma segura. La autenticación de usuarios internos (OSIPTEL) debe hacer uso de las credenciales del LDAP de la institución, y para el caso de usuarios externos se debe diseñar un esquema seguro de Base de Datos según esquema establecido por OSIPTEL.





		<p>c) Se debe contar con URL (enlaces) independientes para los accesos de usuarios internos del OSIPTEL y de usuarios externos o de las empresas operadoras.</p> <p>d) Se debe implementar mecanismos que eviten ataques automatizados de fuerza bruta como captchas y prohibir múltiples inicios de sesión desde una misma cuenta.</p> <p>e) El software desarrollado debe permitir que los usuarios externos realicen el cambio y/o restablecimiento de su contraseña cumpliendo con los lineamientos de la Política² de Seguridad de la Información del OSIPTEL (ítem 6.8.1 – Identificación y Contraseñas)</p> <p>f) El perfil “Empresa” debe poder realizar la suspensión de cuentas. El sistema debe asegurar que mientras dure la suspensión de una cuenta, la empresa operadora no pueda cargar, reportar ni registrar reportes de información periódica utilizando dicha cuenta.</p> <p>2.1.2. GESTION DE USUARIOS Y PERFILES</p> <p>a) Se debe documentar el análisis de los perfiles, el cual debe responder a los actores dentro del flujo del proceso soportado por el software; los perfiles deben ser diseñados de forma que apoyen a la adecuada segregación de funciones en el proceso.</p> <p>b) Todo software desarrollado para OSIPTEL y que cuente con usuarios externos deberá contar con un módulo de Gestión de Usuarios y Perfiles que como mínimo cumpla:</p> <ul style="list-style-type: none"> - Permitirá registrar usuarios externos, empresas operadoras. - Permitirá la asociación del usuario externo a una o varias empresas y el usuario-empresa a uno o varios perfiles. - Segregar el acceso de acuerdo al perfil y empresa operadora al que pertenezca. - Permitir realizar la activación u desactivación (suspensión) del usuario - Permitir realizar la asignación y retiro del perfil. <p>c) Implementar características técnicas que eviten el acceso no autorizado, usar bloqueo de cuentas después de intentos fallidos de acceso, captchas, fortaleza de contraseñas, entre otras buenas prácticas.</p> <p>d) Documentar la Matriz de perfiles y opciones donde se registran los módulos, opciones y sub opciones del software y los perfiles existentes en este; lográndose identificar la asociación de perfil con opción permitida. La matriz incluye un nivel de acción que corresponde</p>
--	--	---



a si el perfil tiene acceso a lectura o modificación en dicha opción.

2.1.3. RIESGOS

- Clasificar los datos procesados, almacenados o transmitidos por el software identificando su confidencialidad o sensibilidad de acuerdo a las normas de seguridad de la información o leyes, normas aplicables a OSIPTEL
- Identificar las acciones que pueden amenazar la confidencialidad, integridad o disponibilidad de la información e implementar las acciones que las mitiguen; comunicarlas al OSIPTEL para llevar el seguimiento de estas.
- Diseñar mecanismos que brinden protección contra la falsificación, alteración, repudio, revelación de información y ataques a la elevación de privilegios.

2.1.4. AUDITORÍA

El sistema desarrollado para OSIPTEL debe contar con un módulo de Auditoría donde se puedan visualizar los siguientes registros:

- Registros (logs) que permitan la trazabilidad sobre registro, cambios, actualización o desactivación de usuarios.
- Registros (logs) que permitan la trazabilidad sobre las acciones donde se procese (registre, actualice, elimine, desactivación) información confidencial y/o datos personales.
- Registros (logs) que permitan la trazabilidad sobre acciones requeridas por el propietario o dueño del proceso involucrado.

2.2. CODIFICACIÓN E IMPLEMENTACIÓN

2.2.1. CODIFICACIÓN SEGURA

El software desarrollado para OSIPTEL debe de cumplir con buenas prácticas de programación, mínimamente con las siguientes, sin necesidad de ser las únicas:

- Validación de datos de entrada, para evitar que un atacante envíe datos inválidos con la intención de que el software realice algo distinto para lo que ha sido diseñado y/o programado. Tener en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas.
- Gestión de Sesiones, evitando que los ID's de sesión sean expuestos, actualizando los ID's de sesiones luego de un login exitoso, invalidando los ID's de sesiones durante el proceso de cierre de sesión o después de un periodo de inactividad.
- Manejo de logs, evitando que los logs almacenen información confidencial de los usuarios (contraseñas, conexión a la BD, etc.), o sensible de la aplicación.



- d) Manejo de errores, evitando que los mensajes de error revelen información que pueda servir a un atacante para impactar de forma negativa sobre la aplicación incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, debe implementarse mensajes de error genéricos.
- e) Manejo de archivos, evitando que se transfiera al servidor archivos sin previa autenticación y restringiendo su tipo (pdf, doc, xls) estrictamente a lo requerido.
- f) Estandarización y reutilización de funciones de seguridad.
- g) Remover todas las funcionalidades y archivos que no sean necesarios para el software y/o sistema de información, previo a la puesta en producción.
- h) No se debe incluir información sensible en el manejo de tokens, debido a que estos pueden ser descifrados. Se debe implementar los mecanismos adecuados para validar la firma y metadatos ingresados para asegurar la validez y veracidad del token.
- i) No se debe usar Framework y librerías con vulnerabilidades conocidas a la puesta en producción.
- j) No debe haber ninguna lógica de negocio sensible, claves secretas u otra información propietaria en el código del lado del cliente.

2.2.2. COMPONENTES DEL SOFTWARE

- a) Se debe tener un registro (inventario) de todos los componentes que son usados en el software (software base, librerías, frameworks u otros), incluyendo la versión.
- b) Los componentes usados no deben de tener vulnerabilidades conocidas a la puesta en producción.

2.2.3. SEGURIDAD EN LAS COMUNICACIONES

- a) Cuando el Software procese información cuya clasificación no es pública debe usarse mecanismos de cifrado que protejan los datos en tránsito (TLS, etc.). Se debe utilizar algoritmos y protocolos estándares y fuertes para el cifrado.
- b) No se debe almacenar en caches datos sensibles como los datos personales.
- c) Las cadenas de conexión a la base de datos no deben de estar incluidas en el código de la aplicación. Las cadenas de conexión a la base de datos deben de estar en un archivo de configuración separado en un sistema confiable y debe ser encriptado.
- d) No se debe almacenar en cache ni cookies u otros metadatos, información sensible como los datos personales y, en caso sea necesario, se deben aplicar controles de cifrado pertinentes para proteger su confidencialidad.

		<p>2.2.4. PRUEBAS DE SEGURIDAD El software desarrollado para OSIPTEL, así como la infraestructura y componentes que lo soportan, debe de pasar por las siguientes pruebas de seguridad y contar con los registros de estas:</p> <ul style="list-style-type: none"> a) Realizar pruebas de control de acceso, gestión de usuarios y auditoría en las pruebas unitarias y de integración. b) Revisión de código fuente, que incluyan la deuda técnica en relación a la cantidad de bugs, vulnerabilidades, códigos duplicados, cobertura y hotspots. c) Análisis de Vulnerabilidades (OWASP TOP 10 vigente, entre otros) <p>2.2.5. REMEDIACIÓN DE VULNERABILIDADES</p> <ul style="list-style-type: none"> a) En caso se hayan encontrado vulnerabilidades u observaciones en las pruebas de seguridad deberán ser resueltas antes del pase a producción. b) Las vulnerabilidades u observaciones deben de ser informadas al Oficial de Seguridad de la Información de forma que se lleve el registro y se realice su seguimiento de acuerdo a los procedimientos aprobados.
3	Usabilidad	<ul style="list-style-type: none"> • Incluir interfaces gráficas sencillas, amigables, intuitivas, consistentes y de fácil uso para los usuarios. El OSIPTEL se reserva el derecho de establecer una guía/estándar visual para los sitios desarrollados y, en ese caso, dicha guía/estándar deberá ser respetada por el contratista. • Considerar factores de presentación en el formato de las pantallas a través de hoja de estilos *.css, temas, plantillas, resolución de pantalla (pixel), scripts, manejando los estándares de diseño que se emplean en el OSIPTEL. • Compatible con las versiones recientes (al menos las últimas cuatro versiones) de navegadores de Internet: Google Chrome, Mozilla FireFox y Microsoft Edge o Internet Explorer.
4	Escalabilidad	<p>Viabilidad para incluir módulos adicionales que se integren al sistema a desarrollar.</p> <p>Implementación de módulos de registros de datos generales y/o parámetros empleados para la integración de los datos en el sistema y mejor manejo de los mismos por el usuario.</p>
5	Disponibilidad	<p>Se requiere que los servicios estén completamente operativos las 24 horas del día, 7 días a la semana. El contratista deberá proponer mecanismos alternos (contingencia) para asegurar la continuidad de estos servicios.</p>
6	Administrable	<p>Gestión de roles y usuarios.</p> <ul style="list-style-type: none"> • Configuración de parámetros.



		<ul style="list-style-type: none"> • Mecanismos de auditoría, seguimiento y trazabilidad de la información y las transacciones realizadas en el sistema. • Tratamiento del log de eventos, para contemplar el registro de caídas del servicio, manejo de errores y excepciones.
--	--	---

CAPACITACION

1. Se deberá capacitar a los responsables de la administración tanto a nivel técnico como funcional, así como a los representantes de las empresas operadoras.

Esta capacitación se realizará dentro del plazo de ejecución de la prestación principal, y antes de la puesta en producción del sistema.

2. El contratista debe brindar capacitación de dieciséis (16) horas en total, según el siguiente detalle:
 - a. Una (01) sesión de cuatro (04) horas sobre aspectos técnicos a un mínimo de tres (03) funcionarios de la Oficina de Tecnologías de Información (en adelante OTI).
 - b. Una (01) sesión de cuatro (04) horas sobre aspectos funcionales a un mínimo de seis (06) funcionarios de la DPRC.
 - c. Cuatro (04) sesiones de dos (02) horas, las cuales podrán ser desarrolladas el mismo día, sobre aspectos funcionales para el perfil EMPRESA a un mínimo de veinte (20) representantes de las empresas.
3. La provisión de equipos, materiales u otros recursos utilizados para la capacitación, estarán a cargo del contratista.
4. La capacitación se realizará dentro del horario de 9:00 a 18:00 horas, de lunes a viernes, las mismas que podrían ser virtuales y/o presenciales, esta última en las oficinas de la sede Parque Norte 1180 o en la sede Calle la Prosa 136, ambas ubicadas en el distrito de San Borja. La fecha de inicio de la capacitación será previamente coordinada entre la DPRC, OTI y el contratista mediante correo electrónico.
5. Al finalizar la capacitación el contratista deberá presentar un informe, conteniendo como mínimo los temas desarrollados, la lista de asistencia, el material de la capacitación, las conclusiones y recomendaciones; la misma que deberá ser presentada dentro de los cinco (05) días calendario de culminada la capacitación a través de mesa de partes virtual o física.

IX. PLATAFORMA TECNOLÓGICA ACTUAL DEL OSIPTEL

Se deberá considerar que el desarrollo del SIGEP debe estar implementado de acuerdo a la siguiente estandarización:

- Lenguaje de programación C#
- Entorno de Desarrollo Integrado (IDE) Visual Studio 2019 o superior
- Arquitectura de desarrollo de aplicaciones Net Framework y/o Net Core
- Arquitectura de desarrollo de servicios REST con interface Api RESTFul



- Sistema Operativo Windows Server 2019
- Base de datos: Oracle 12

Por otro lado, se precisa que el OSIPTEL utiliza MS Exchange Online mediante Microsoft 365 (OutLook) como plataforma de envío de correos. La utilización de esta solución se encuentra estandarizada mediante Resolución de Administración y Finanzas N° 0034-2022-OAF/OSIPTEL, que estandariza el software institucional.

X. ENTREGABLES

Fase	Entregable	Plazo de Entrega
1	Primer entregable: Planificación del Proyecto <ul style="list-style-type: none"> Planificación general para el desarrollo e implementación de los nuevos reportes. Declaración jurada de cumplimiento de Política³ de Seguridad de la Información. Entregables de acuerdo a la MIG (⁴) del OSIPTEL <ul style="list-style-type: none"> Plan General del Proyecto (MIG-TI-2210) Plan de Gestión de Riesgos (MIG-TI-2210) Plan de Gestión de Cambios (MIG-TI-2221) 	Dentro de los diez (10) días calendario, computados desde el día siguiente de suscrito el contrato .
2	Segundo entregable: Desarrollo del Sistema <ul style="list-style-type: none"> Desarrollo del modelo de la solución. El análisis de los perfiles que deberá ser presentado dentro del documento "MIG-TI-2120 Definición Inicial de Requerimientos V1.0". Matriz de perfiles y opciones Informe de riesgos de seguridad de la información identificados y su plan de acción implementado, incluyendo la clasificación de datos. El desarrollo de las pruebas consideradas en el numeral 2.2.4 a) sobre control de acceso, gestión de usuarios y auditoría dentro del documento de Pruebas Unitarias y de Integración. Informe y/o reporte de revisión de código fuente⁵ que debe contener lo solicitado en el numeral 2.2.4 b). Documento de análisis de vulnerabilidades que debe contener lo solicitado en el numeral 2.2.4 c). 	Dentro de los doscientos cincuenta (250) días calendario, computados desde el día siguiente de la conformidad del primer entregable .

3

<https://cdn.www.gob.pe/uploads/document/file/2130756/Pol%C3%ADticas%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf>

⁴ La Metodología Integrada de Gestión – MIG del OSIPTEL, establece un marco metodológico para los procesos del ciclo de vida de desarrollo del software basado en los estándares de ISO/IEC TR 15504:2003, PMI, CMMi, RUP y Métrica 3, respetando y cumpliendo con los lineamientos de la NTP – ISO / IEC 12207. Los formatos MIG listados, serán entregados por el OSIPTEL al contratista, al inicio de la ejecución del servicio

⁵ Realizado con alguna herramienta de verificación como sonarqube, Codebeat, Klocwork o similares



	<ul style="list-style-type: none"> • Registro de los componentes que son usados en el software que debe contener lo solicitado en el numeral 2.2.2. • Entregables de acuerdo a la MIG del OSIPTEL • Prototipo del sistema de información (MIG-OI-3020) • Modelo de Software (MIG-OI-3011) • Diseño del Sistema de Información (MIG-OI-3021) • Software Producido (MIG-OI-3040), que incluye el código fuente. • Manual de Instalación y Configuración (MIG-OI-3032) • Capacitación a Usuarios. • Informe de Pruebas de Usuario y pruebas de estrés (MIG-TI-2323) • Pase a Producción (MIG-OI-3041) 	
3	<p>Tercer entregable: Puesta en Producción</p> <p>Entregables de acuerdo a la MIG del OSIPTEL</p> <ul style="list-style-type: none"> • Caso de Prueba de Usuario (MIG-SI-4310) • Informe de implantación (MIG-TI-2324) • Manual de Usuario (MIG-OI-3030) • Manual del Sistema (MIG-OI-3031) • Cierre del Proyecto (MIG-TI-2410) • Versión final del flujo de trabajo del Módulo, empleando como referencia el esquema señalado en el Anexo 1 del presente documento. 	Dentro de los diez (10) días calendario, computados desde el día siguiente de la conformidad del segundo entregable .
Total de días		270

Asimismo, todos los borradores, especificaciones, diseños, informes, programas y otros documentos preparados por el contratista en virtud del servicio pasarán a ser propiedad del contratante, quedando reservado para estos los derechos como propietarios de los mismos.

Se mantendrán las reuniones que se estimen oportunas entre el OSIPTEL y el contratista para realizar las precisiones y aclaraciones necesarias sobre el contenido de los productos entregados y realizar las sugerencias acerca de los mismos. El contratista estará encargado de elaborar las actas respectivas, para cada reunión sostenida.

Los entregables serán presentados en Mesa de Partes Virtual; <https://serviciosweb.osiptel.gob.pe/MesaPartesVirtual/> (desde las 00:00 horas hasta las 23:59 horas. Los documentos presentados en día hábil se consideran recibidos en ese día, y los documentos que se presenten en día no laborable se darán por recibidos el primer día hábil siguiente) o, en Mesa de Partes del OSIPTEL sito en Calle De La Prosa 136 – San Borja, dentro del horario de 08:45 horas a 16:45 horas

XI. PRESTACION ACCESORIA



Para el caso de la prestación accesoria, que comprende un total de dos (2) periodos continuos, el contratista deberá presentar un “**Informe de actividades**” por cada periodo de ciento ochenta (180) días calendario de soporte. Dicho informe debe contener el detalle de las actividades realizadas en el periodo correspondiente. La presentación del “Informe de actividades” es necesaria para la conformidad del servicio y, por ende, para el pago del mismo. Se debe tener en cuenta que la prestación accesoria comprende dos periodos.

SOPORTE TÉCNICO

El soporte técnico, debe permitir la optimización del servicio, atención de incidencias por defectos en el funcionamiento, remediación de vulnerabilidades técnicas o consultas generadas a partir del uso del nuevo SIGEP.

TIPO DE INCIDENCIA/ACTIVIDAD	TIEMPO DE RESPUESTA (*)	TIEMPO DE RESOLUCIÓN (*)
Críticas: Las que afectan gravemente el funcionamiento de la aplicación y al cliente.	4 horas	Inmediato Ofreciendo una solución lo antes posible (máximo 1 día calendario)
Grave: Las que afectan moderadamente el funcionamiento de la aplicación.	8 horas	1-2 días calendario
Leve: Las que afectan de manera aleatoria o levemente el funcionamiento de la aplicación.	2 días calendario	3-4 días calendario

(*) El tiempo de atención será a partir de la notificación realizada por la OTI y/o DPRC mediante correo electrónico y/o de forma escrita.

TIPO DE VULNERABILIDAD (CVSS V3.1 o posterior) ⁶	TIEMPO DE RESPUESTA ⁷	TIEMPO DE REMEDIACIÓN ⁸
Crítica	4 horas	Máximo 5 días calendarios
Alta	8 horas	Máximo 10 días calendario
Media o baja	2 días calendario	Máximo 20 días calendario

Nota:

Los gastos de transporte, mano de obra y materiales que se puedan originar con motivo de las reparaciones o reposiciones dentro de la prestación accesoria serán por cuenta del contratista.

Al término de cada periodo, dentro de los cinco (05) días calendario posteriores, el contratista deberá presentar el informe con el detalle de todos los incidentes de la prestación accesoria, a través de mesa de partes.

Los informes de cada periodo serán presentados en Mesa de Partes Virtual; <https://serviciosweb.osiptel.gob.pe/MesaPartesVirtual/> (desde las 00:00 horas

⁶ El CVSS es una métrica de vulnerabilidad estándar del sector. Puede obtener más información sobre el CVSS en FIRST.org.

⁷ El tiempo de atención será a partir de la notificación realizada por la OTI y/o la Oficial de Seguridad de la Información, mediante correo electrónico y/o de forma escrita.

⁸ Se considera remediación a la subsanación de la vulnerabilidad en el ambiente de producción



hasta las 23:59 horas. Los documentos presentados en día hábil se consideran recibidos en ese día, y los documentos que se presenten en día no laborable se darán por recibidos el primer día hábil siguiente) o, en Mesa de Partes del OSIPTEL sito en Calle De La Prosa 136 – San Borja, dentro del horario de 08:45 horas a 16:45 horas

XII. LUGAR Y PLAZO DE EJECUCIÓN

LUGAR DE LA PRESTACIÓN DEL SERVICIO

El servicio será realizado en las instalaciones del contratista y los pases a producción serán realizados de forma remota en el OSIPTEL en coordinación con el personal técnico de la OTI.

Cabe precisar que, el servicio también – en coordinaciones con el OSIPTEL – podrá ser realizado en las instalaciones de este Organismo (sito en Calle La Prosa 136 y/o Avenida del Parque Norte 1180 – San Borja).

PLAZOS DE EJECUCIÓN DEL SERVICIO

Prestación principal

El plazo de ejecución es de doscientos setenta (270) días calendario, el mismo que se computa desde el día siguiente del perfeccionamiento del contrato.

Prestación accesoria

El servicio de soporte técnico será de trescientos sesenta (360) días calendario, computado desde el día siguiente de suscrito un Acta. La prestación accesoria comprende dos periodos distribuidos en plazos de ciento ochenta (180) días; cada uno. El servicio será prestado por 24 horas x 365 días calendario. La fecha de inicio quedará sentada en un Acta suscrito entre la DPRC, en su calidad de área usuaria, la OTI, en su calidad de área técnica, y el Contratista.

XIII. CONFORMIDAD DEL SERVICIO

Prestación principal y accesoria

La conformidad será otorgada por la DPRC, en su calidad de área usuaria, con el visto bueno de la OTI, en su calidad de área técnica.

XIV. FORMA DE PAGO

Prestación principal

El pago se efectuará de acuerdo con el siguiente detalle:

1	Primer entregable: Planificación del Proyecto	30% del monto del contrato (*).
2	Segundo entregable: Desarrollo del Sistema	40% del monto del contrato (*).
3	Tercer entregable: Puesta en Producción	30% del monto del contrato (*).

(*): Monto de la prestación principal.

Prestación accesoria



Soporte técnico

Los pagos serán en dos (02) partes iguales, por cada periodo; luego de presentado el "Informe de actividades" y otorgada la conformidad sobre el mismo. El informe de actividades se presenta al día siguiente de culminado el plazo del periodo establecido y que conforma la prestación accesoria.

XV. PENALIDAD POR MORA

Las penalidades por mora se aplicarán conforme al artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

XVI. OTRAS PENALIDADES

N°	Supuestos de aplicación de penalidad	Forma de Cálculo de la penalidad	Procedimiento para verificar el supuesto
Por retrasos en la remediación de vulnerabilidades La clasificación de las vulnerabilidades sigue el sistema de puntaje CVSS V3.1 o posterior vigente. El CVSS es una métrica de vulnerabilidad estándar del sector. Puede obtener más información sobre el CVSS en FIRST.org. Se considera remediación a la subsanación de la vulnerabilidad en el ambiente de producción.			
1	Vulnerabilidad CRITICA no solucionada en plazo (máximo 05 días calendarios)	Por cada día calendario de retraso de la vulnerabilidad no remediada dentro del tiempo máximo = 5% de la UIT	Revisión/Validación/Conformidad de la Oficial de Seguridad de la Información ⁹
2	Vulnerabilidad ALTA no solucionada en plazo (máximo 10 días calendarios)	Por cada día calendario de retraso de la vulnerabilidad no remediada dentro del tiempo máximo = 5% de la UIT	
3	Vulnerabilidad MEDIA o BAJA no solucionada en plazo (máximo 20 días calendarios)	Por cada día calendario de retraso de la vulnerabilidad no remediada dentro del tiempo máximo = 5% de la UIT	

XVII. SISTEMA DE CONTRATACIÓN

Suma alzada

XVIII. VICIOS OCULTOS

El plazo máximo de responsabilidad del contratista es de DOS (2) años contado a partir de la conformidad otorgada por LA ENTIDAD.

XIX. PROPIEDAD INTELECTUAL (DERECHOS DE AUTOR)

El contratista cede en forma ilimitada, exclusiva y gratuita:

- Todos los derechos patrimoniales y formas de explotación reconocidos por el Decreto Legislativo N° 822, Ley sobre Derechos de Autor, relativos a los sistemas del OSIPTEL, objeto del presente contrato.
- Todos los derechos sobre la documentación y los entregables que realice y produzca a favor del OSIPTEL como consecuencia del proyecto que se le encargue.

Dichos derechos serán libremente ejercidos y explotados por el OSIPTEL, pudiendo éste realizar modificaciones o versiones sucesivas del software materia del presente

⁹ Mediante correo electrónico, informe de verificación, memorando u algún otro medio.

contrato y obtener por ello beneficios salvo en los casos en que se trate de propiedad intelectual del contratista incluir las licencias de software la cuales deberán estar a nombre del OSIPTEL y entregadas en el formato oficial del fabricante, para dar la conformidad de la entrega, la misma que será verificada por la OTI del OSIPTEL.

En tal sentido, el contratista está prohibida directa o indirectamente a través de terceros de: reproducir parcial o totalmente, comunicar al público, distribuir, transformar o aplicar cualquier otra forma distinta a las indicadas en los dos primeros puntos, utilizar los diseños, código fuente, y en general el sistema objeto del contrato, sin expresa y previa autorización del OSIPTEL.

Esta prohibición tiene vigencia ilimitada, aun cuando el proyecto materia del contrato haya culminado o el contrato haya sido resuelto.

El OSIPTEL tiene el derecho expedito de realizar las gestiones de inscripción correspondientes ante la Dirección de Derechos de Autor de INDECOPI.

El contratista no podrá hacer referencia sobre el OSIPTEL en publicidad o literatura sin la previa aprobación escrita de éste. Esta prohibición es a perpetuidad y se mantiene vigente aun cuando el contrato haya culminado o haya sido resuelto.

El desarrollo de software, el código fuente generado, y las aplicaciones elaboradas por el contratista serán de propiedad del OSIPTEL.

XX. ACUERDO DE CONFIDENCIALIDAD

Se prohíbe la divulgación, incluso después que haya terminado su relación contractual, exigiéndose mantener estricta confidencialidad respecto a toda información, documentos, contratos, propuestas, códigos fuentes y material del presente servicio que se confieran por escrito o se reciban verbalmente durante las tareas ejecutadas en el cumplimiento de su labor, en caso de surgir un evento que la información sea revelada por el contratista a terceros no partícipes de este acuerdo de confidencialidad, el contratista se compromete a indemnizar a (nombre de la compañía que divulga) por todos los perjuicios directos o indirectos que de la revelación se deriven, provengan de hechos dolosos o culposos.

XXI. SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Para el OSIPTEL la seguridad de la información y protección de los datos personales son aspectos importantes que debe garantizarse en todos sus procesos, con este objetivo el contratista (persona natural o jurídica, así como el personal destacado para la prestación del servicio) tiene las siguientes responsabilidades:

- Mantener la disponibilidad, integridad y confidencialidad de la información suministrada por el OSIPTEL y/o sus usuarios, durante la prestación de su servicio o cual sea el objeto de su contratación.
- Hacer uso adecuado de los datos personales de los usuarios del OSIPTEL que se hayan suministrado durante la prestación de su servicio o cual sea el objeto de su contratación, evitando la fuga de información.



- Cumplir con la Política¹⁰ de seguridad de la información del OSIPTEL la misma que declara conocer y cumplir a través de una declaración jurada simple.
- Implementar los controles de seguridad de la Información de la NTP-ISO/IEC 27001:2014 que le sean aplicables en la prestación de su servicio o cual sea el objeto de su contratación.
- En caso un incidente de seguridad se concrete, afectando la confidencialidad, integridad o disponibilidad de la información, el contratista o proveedor se compromete a indemnizar al OSIPTEL por todos los perjuicios directos o indirectos que se deriven, provengan de hechos dolosos o culposos.

El incumplimiento de las disposiciones establecidas en las políticas de seguridad de la información, procedimientos, manuales o cualquier otro documento derivado de estas, tendrá como resultado la aplicación de medidas correctivas y de mejora necesarias. En caso se encontrará responsabilidad en un colaborador y/o tercero, se dará inicio al procedimiento administrativo disciplinario correspondiente y/o a las acciones legales que la ley faculte.

XXII. OTRAS CONSIDERACIONES DEL SERVICIO

- La inclusión de enlaces, logotipos y/o referencias de marcas comerciales ajenas a la institución, deberán ser autorizados expresamente por el OSIPTEL.
- Está prohibida la subcontratación de cualquier actividad relacionada directamente con el servicio prestado al OSIPTEL.
- Es responsabilidad del contratista asignar los recursos suficientes para el servicio prestado al OSIPTEL, garantizando el cumplimiento de las actividades y plazos del servicio.
- No se otorgarán adelantos para la ejecución del servicio.

XXIII. REQUISITOS DE CALIFICACIÓN

FUNCIONES DEL PERSONAL CLAVE

Un (01) Coordinador del Proyecto

Estará encargado de la gestión y supervisión del proyecto por parte del contratista.

Un (01) Analista de Sistemas

Estará encargado del levantamiento de información y análisis funcional del sistema.

Dos (02) Analistas Programador

Estará encargado de las actividades operativas relacionadas con el diseño, construcción e implementación de las adecuaciones al sistema.

Un (01) Analista de Calidad

Encargado de validar la calidad del producto (sistema) durante las actividades correspondientes a las pruebas y capacitación.

A	CAPACIDAD TÉCNICA Y PROFESIONAL
A.1.1	FORMACIÓN ACADÉMICA



Requisito:**(01) Coordinador del Proyecto:**

Título profesional en Ingeniería de sistemas o Ingeniería Informática o Ciencias de la Computación o Ingeniería de Sistemas de Información o Ingeniería de Sistemas e Informática o Ingeniería de Software o Ingeniería Informática y de Sistemas o Ingeniería de Sistemas e Informática o Ingeniería de Tecnologías de la Información y Sistemas, Ingeniería Informática o Ingeniería de Computación o Ingeniería de Computación y Sistemas, Ingeniería de Telecomunicaciones o Ingeniería Electrónica o Ingeniería en Computación e informática

(01) Analista de Sistemas:

Bachiller en Ingeniería de Sistemas o ingeniería de Informática o Ciencias de la Computación o Ingeniería de Sistemas de Información o Ingeniería de Sistemas e Informática o Ingeniería de Software o Ingeniería Informática y de Sistemas o Ingeniería de Sistemas e Informática o Ingeniería de Tecnologías de la Información y Sistemas o Ingeniería Informática o Ingeniería de Computación o Ingeniería de Computación y Sistemas o Ingeniería de Telecomunicaciones o Ingeniería Electrónica o Ingeniería en Computación e informática.

(02) Analista Programador:

Bachiller en Ingeniería de Sistemas o Ingeniería de Informática o Ciencias de la Computación o Ingeniería de Sistemas de Información o Ingeniería de Sistemas e Informática o Ingeniería de Software o Ingeniería Informática y de Sistemas o Ingeniería de Sistemas e Informática o Ingeniería de Tecnologías de la Información y Sistemas o Ingeniería Informática o Ingeniería de Computación o Ingeniería de Computación y Sistemas o Ingeniería de Telecomunicaciones o Ingeniería Electrónica o Ingeniería en Computación e informática o técnico titulado en Computación o Informática o Sistemas

(01) Analista de Calidad:

Bachiller en Ingeniería de Sistemas o Ingeniería de Informática o Ciencias de la Computación o Ingeniería de Sistemas de Información o Ingeniería de Sistemas e Informática o Ingeniería de Software o Ingeniería Informática y de Sistemas o Ingeniería de Sistemas e Informática o Ingeniería de Tecnologías de la Información y Sistemas o Ingeniería Informática o Ingeniería de Computación o Ingeniería de Computación y Sistemas o Ingeniería de Telecomunicaciones o Ingeniería Electrónica o Ingeniería en Computación e informática.

Acreditación:

El BACHILLER O TÍTULO PROFESIONAL será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <https://enlinea.sunedu.gob.pe/> o, en caso de TÍTULO TÉCNICO, en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link : <http://www.titulosinstitutos.pe/>, según corresponda.

En caso el BACHILLER, TÍTULO PROFESIONAL O TÍTULO TÉCNICO no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.



A.1.2	CAPACITACIÓN
	<p><u>Requisito:</u></p> <p><u>(01) Coordinador del Proyecto:</u></p> <ul style="list-style-type: none"> • Especialización en Gestión de Proyectos (PMI), de por lo menos 40 horas lectivas. • Curso en metodologías ágiles, de por lo menos 20 horas lectivas. <p><u>(01) Analista de Sistemas:</u></p> <ul style="list-style-type: none"> • Curso en metodologías y/o técnicas y/o herramientas para el modelamiento y documentación de sistemas como RUP, UML de por lo menos 20 horas lectivas. <p><u>(02) Analista Programador:</u></p> <ul style="list-style-type: none"> • Curso de capacitación en desarrollo de sistemas con .Net, de por lo menos 20 horas lectivas. • Curso en desarrollo de base de datos, de por lo menos 20 horas lectivas. <p><u>(01) Analista de Calidad:</u></p> <ul style="list-style-type: none"> • Curso en metodologías y/o, técnicas y/o herramientas para el análisis de calidad, de por lo menos 40 horas lectivas. <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de CONSTANCIAS o CERTIFICADOS. Cabe precisar que es válido la presentación de constancias o certificados cuya sumatoria de horas permita alcanzar las horas totales exigidas en cada materia.</p>
A.2	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisito:</u></p> <p><u>(01) Coordinador del Proyecto:</u></p> <ul style="list-style-type: none"> • Experiencia no menor a tres (03) años en proyectos de sistemas de información institucionales y/o desarrollo de aplicaciones web. <p><u>(01) Analista de Sistemas:</u></p> <ul style="list-style-type: none"> • Experiencia no menor a tres (03) años en actividades de levantamiento de requerimientos funcionales o como analista de sistemas. <p><u>(02) Analista Programador:</u></p> <ul style="list-style-type: none"> • Experiencia no menor a dos (02) años en implementación de soluciones web, y, en proyectos en .Net 2015 C# o superior, y, en desarrollo con base de datos Oracle. • <p><u>(01) Analista de Calidad:</u></p> <ul style="list-style-type: none"> • Experiencia no menor a tres (03) años como analista de calidad.. •



	<p>Respecto al personal clave cuyo requisito mínimo es el Título Profesional en Ingeniería, la experiencia, debe cumplir con la exigencia del Colegio de Ingenieros que establece lo siguiente:</p> <p>En relación con lo expuesto, el artículo 1 de la Ley N° 28858 –Ley que complementa la Ley N° 16053, “Ley que autoriza a los Colegios de Arquitectos del Perú y al Colegio de Ingenieros del Perú para supervisar a los profesionales de Arquitectura e Ingeniería de la República”, todo profesional que ejerza las labores propias de ingeniería requiere poseer grado académico y título profesional o extranjero debidamente revalidado en el país, estar colegiado y encontrarse habilitado por el Colegio de Ingenieros del Perú</p> <p><u>Acreditación:</u> La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p>
B	<p>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</p> <p><u>Requisito:</u> El postor debe acreditar un monto facturado acumulado equivalente a S/. 350,000.00 (Trescientos cincuenta mil y 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) 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.</p> <p>Se consideran servicios similares a los siguientes: Diseño y/o mantenimiento y/o desarrollo de sistemas web para intranet y/o dispositivos móviles, y/o administradores de contenidos y/o desarrollo de software en general y/o aplicaciones web.</p> <p><u>Acreditación:</u> La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones.</p>



Anexo 1: Flujo de trabajo del SIGEP

[Ver archivo adjunto]

Anexo 2: Matriz de perfiles y opciones (modelo)

PERFILES	OPCIONES	USUARIOS
Administrador	Las señaladas en el requerimiento funcional 1.1	Usuario A1 Usuario A2 ...
Empresa	Las señaladas en el requerimiento funcional 1.2	Usuario E1 Usuario E2 ...
Usuario Interno	Las señaladas en el requerimiento funcional 1.3	Usuario I1 Usuario I2 ...

