



TÉRMINOS DE REFERENCIA SERVICIO DE SOLUCIÓN CORPORATIVA CLOUD COMPUTING (NUBE)

1. AREA USUARIA

Departamento de Informática.

2. FINALIDAD PÚBLICA

La ejecución de este servicio tiene como finalidad implementar una infraestructura flexible, segura, escalable y sostenible en el tiempo, el cual permitirá brindar un mejor servicio de los sistemas informáticos a nivel nacional, asegurando la disponibilidad de los mismos, en cumplimiento de los fines institucionales de SENCICO.

3. ACTIVIDAD DEL POI

Modernizar la Gestión Institucional de SENCICO

4. OBJETO DE LA CONVOCATORIA

Objetivo General

Se requiere seleccionar a una persona jurídica o natural para la contratación de un servicio de cloud computing (nube), el cual provisionará una plataforma de sistemas, flexible, segura, escalable, elástica y sostenible en el tiempo. El cual incluye la implementación de nuestros sistemas informáticos en la nube, capacitación en el uso adecuado y soporte por el periodo del servicio.

Objetivos Estratégicos

- Contratar a una empresa para que nos brinde el servicio cloud computing (nube), el cual permitirá tener nuestros sistemas en la nube.
- Brindar a nivel nacional una conexión más eficiente, segura y de rápido acceso a los sistemas del SENCICO, los cuales ya no se encontrarán en los servidores de la Sede Central.

5. SISTEMA DE CONTRATACIÓN

Mixto

6. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

El Servicio de Solución Corporativa Cloud Computing (Nube) estará compuesto por los siguientes servicios:

Prestación	Cantidad	Unidad de Medida	Descripción
Principal	1	Servicio	Servicio de implementación y migración
	1	Mixto	Servicio de solución corporativa Cloud Computing
Accesorio	1	Servicio	Soporte Técnico
	1	Servicio	Capacitación

I. Consideraciones Generales:

- a) El Contratista se encargará de la implementación, puesta en marcha, y todas las actividades necesarias, para la implementación del servicio solicitado, en coordinación con el Departamento de Informática, con el fin de contar con el Servicio Cloud Computing para todas las Sedes de Sencico a nivel nacional.
- b) El Contratista levantará información técnica dentro del alcance del presente TDR, para elaborar el Plan de Trabajo oportunamente, con el equipo de Informática del SENCICO.
- c) El CONTRATISTA deberá considerar el personal, equipos, licencias, herramientas y cualquier otro recurso necesario dentro del alcance del presente TDR, para llevar a cabo la correcta implementación del Servicio sin que genere un costo adicional para SENCICO.
- d) El CONTRATISTA dentro del plazo de implementación, deberá ejecutar un protocolo de pruebas, el cual no deberá contar con observaciones para dar la conformidad de la implementación y firmar el Acta de implementación del servicio.
- e) El CONTRATISTA es el responsable de la implementación en su totalidad, incluyendo la ejecución de los protocolos de pruebas.

- f) El Contratista deberá considerar lo necesario para que la implementación del servicio no afecte a los servicios y sistemas que se vienen ejecutando sobre la infraestructura Cloud Computing actual del SENCICO.
- g) SENCICO autorizará el ingreso a las instalaciones al personal del CONTRATISTA, de requerirlo, previa solicitud detallada, donde deberán presentar por correo electrónico lo siguiente:
 - Datos del personal
 - N° de DNI
 - Lista de materiales y/o equipos a ingresar de ser el caso
 - Fechas y horarios de ingreso
 - Actividades a realizar
 - Áreas y/o servicios afectados, en caso de corte de servicio
 - Declaración jurada del personal que trabajará presencialmente, que no cuenta con síntomas del Covid-19, así como no es personal de riesgo, de acuerdo a lo descrito en el PLAN PARA LA PREVENCIÓN Y CONTROL PARA EL COVID-19 EN EL SENCICO.
 - Prueba molecular o antigénica, con resultado negativo, con fecha de realización de la prueba como máximo de dos (2) días calendario antes de la fecha de ingreso a la Entidad, del personal que trabajará presencialmente, la misma que tendrá una vigencia de diez (10) días calendario.

La solicitud de ingreso, deberá remitirse con un tiempo mínimo de tres (3) días calendario, antes de la fecha del permiso solicitado. Con excepción de la prueba molecular o antigénica, que podrá remitirse por correo electrónico hasta 01 día calendario antes de la fecha del permiso solicitado.

- h) EL CONTRATISTA deberá contar con un sistema de gestión de ticket para la gestión del registro de las incidencias y requerimientos de todos los servicios.
- i) El CONTRATISTA en caso solicite el cambio del personal clave, este deberá ser ingresado por mesa de partes virtual, y no podrá cambiar el Personal clave hasta que la Entidad apruebe de manera formal mediante correo electrónico o Carta, la aceptación de dicho cambio; así mismo el CONTRATISTA deberá concretar una reunión para la transferencia de funciones, la cual debe ser como máximo a los 5 (cinco) días calendarios de remitida dicha aprobación al CONTRATISTA, donde SENCICO deberá participar.
- j) Se precisa que, en la actualidad, el SENCICO tiene implementados sus servicios en las nubes de Amazon Web Services, Microsoft Azure y On-Premise (infraestructura local).
- k) Se precisa que al mencionar el término “nubes” se refiere a multicloud, en el caso que el contratista decida integrar dos o más entornos de nube para cumplir lo solicitado en los TDR.
- l) La(s) nube(s) deberá(n) cumplir con los Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano de la PCM (Presidencia de Consejos de Ministros) establecidas a través de Secretaria de Gobierno Digital (SEGDI), el cual indica que se deberá presentar un certificado seguridad de la información ampliamente reconocido y basado en estándares internacionales, el mismo que tiene que ser emitido por una organización de auditoría independiente, como: Federal Risk and Authorization Management Program (FedRAMP) o similar. Los certificados de seguridad con el que tiene que acreditar la(s) nube(s) son los ISOs: ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, los cuales deberán presentarse para el perfeccionamiento del Contrato.
- m) EL CONTRATISTA deberá ser certificado o autorizado o partner o representante, en soluciones de las(s) nube(s) que oferte en el presente servicio. Se aceptará también "cartas estándar" de la(s) nube(s) en donde indique que EL CONTRATISTA es certificado o autorizado o partner o representante de la(s) nube(s) ofrecida(s); dicho documento deberá presentarse a la presentación de la oferta.
- n) EL CONTRATISTA deberá contar y/o activar con el soporte directo de la(s) nube(s), dicho documento deberá presentarse al perfeccionamiento del Contrato. Deberá acreditar con un Contrato que indique lo solicitado y/o suscripción al servicio de soporte advantage o prioritario o business y/o pago/suscripción de soporte y/o con una Carta emitida por la(s) nube(s) indicando lo solicitado, o documento similar que precise lo solicitado; dicho documento deberá presentarse al perfeccionamiento del Contrato.
- o) EL CONTRATISTA deberá integrar las nubes propuestas.

- p) EL CONTRATISTA brindará entornos como servicio (IaaS / PaaS / SaaS) desde múltiples Centros de Datos para soportar software, bases de datos y las diversas aplicaciones que se encuentran en el alcance, incluyendo componentes de almacenamiento y red. Contemplará una arquitectura transparente para el SENCICO, y deberá implementar todas las condiciones necesarias para otorgar los servicios solicitados.
- q) EL CONTRATISTA deberá contemplar una estrategia de segmentación de red, con el fin de elevar los niveles de restricción y seguridad separando los ambientes de nube(s) implementados de acuerdo a su función.
- r) EL CONTRATISTA deberá considerar lo necesario para que la implementación del servicio se realice fuera del horario de oficina administrativa y fuera de horario de las clases del área educativa, con el fin de no afectar los servicios actuales del SENCICO, exceptuando aquellas actividades que no afecten los servicios actuales en coordinación con SENCICO. En lo posible se optará por una implementación de manera remota. Se detallan los horarios sugeridos de implementación:
 - Fuera de horario – oficina administrativa: lunes a viernes de 6:00 p.m. a 7:00 a.m., y sábados y domingos las 24 horas.
 - Fuera de horario – área educativa: lunes a domingo de 11:00 p.m. a 7:00 a.m.
- s) EL CONTRATISTA debe brindar accesos a todos los ambientes en nube donde se almacenen datos, fuentes de programas, librerías, componentes desarrollados por SENCICO, para hacer posible la migración de los servicios prestados a otros proveedores de servicios en plataforma “Cloud Computing” o para otro entorno definido por SENCICO.
- t) EL CONTRATISTA debe disponer de los medios adecuados (software, herramientas, etc.) y personal especializado en cada una de las tecnologías y servicios que proponga, para que proporcionen el soporte técnico en la migración de los servicios prestados a otros proveedores de plataformas “Cloud Computing” o para otro entorno definido por SENCICO a la finalización del contrato.
- u) La propiedad e información generada por SENCICO en el ambiente provisto por EL CONTRATISTA, en cualquier momento y durante la vigencia, terminación o expiración del Contrato, será exclusivamente de SENCICO.
- v) EL CONTRATISTA y la(s) nube(s) deberá garantizar la confidencialidad y secreto de la información facilitada por el SENCICO, a cualquier persona que por su relación con EL CONTRATISTA deba tener acceso a dicha información. Esto se debe suscribir en un documento de ACUERDO DE CONFIDENCIALIDAD, entre SENCICO y el CONTRATISTA, como parte del Plan de Trabajo.
- w) EL CONTRATISTA deberá asegurar que la(s) nube(s) propuesta(s) soporten el protocolo IPv6.

II. PRESTACIÓN PRINCIPAL

A. Servicio de Implementación y Migración

EL CONTRATISTA deberá contemplar lo siguiente, para realizar la implementación y migración de datos desde las actuales nubes del SENCICO ubicadas en AWS Amazon Web Services, Microsoft Azure y On-Premise:

- a) Durante el último mes del servicio, etapa de transición, EL CONTRATISTA deberá realizar reuniones de trabajo propias de la transferencia e inicio del servicio, respuestas a consultas basadas en el servicio contratado, así como considerar la disponibilidad, datos, información, accesos, formatos, facilidades, recursos, etc. con el fin de que se realice la migración y transición de todos los servicios requeridos por SENCICO hacia la plataforma de nube(s) ofertada(s) por el CONTRATISTA.
- b) La plataforma “Cloud Computing”, así como cada uno de sus componentes, software, eventos, sistemas operativos y configuraciones, debe estar sincronizada con un servicio de NTP (“Network Time Protocol”) donde la precisión del reloj y representación de información/eventos/gráficos deberá figurar en GMT -5 (zona horaria correspondiente a Perú). Se precisa que, el servicio NTP podrá ser un servicio nativo de nube o un recurso de cómputo dedicado.
- c) EL CONTRATISTA deberá migrar, instalar e implementar los servidores, servicios, base de datos, conexiones, arquitectura de red y sistemas del SENCICO hacia la plataforma cloud ofertada, para lo cual EL CONTRATISTA deberá proponer una arquitectura de acuerdo a lo solicitado a los Términos de Referencia del presente proceso.
- d) EL CONTRATISTA deberá realizar la configuración de todas las redes virtuales

necesarias para habilitar el servicio en la plataforma cloud computing, previa validación del Departamento de Informática de SENCICO.

- e) EL CONTRATISTA entregará un inventario de accesos a todas las consolas de administración de servidores, bases de datos y servicios a la finalización de la implementación. La información deberá ser remitida al Asesor de Sistemas e Informática de SENCICO. EL CONTRATISTA es responsable de la cuenta de administración asignada para la gestión y soporte de la solución.
- f) EL CONTRATISTA es responsable de la cuenta de administración asignada para la gestión y soporte de la solución.
- g) Se precisa que SENCICO brindara al Contratista, en la etapa de la migración, el acceso de nivel administrador a todos los servidores y bases de datos, acceso de solo lectura a las consolas de gestión de entornos de nube e inventario de servidores y aplicaciones. El Contratista deberá realizar el relevamiento de información para complementar los datos que considere necesarios.
- h) Sencico facilitará la coordinación para que se pueda realizar la migración de suscripciones.

B. Habilitación de ambientes cloud

- a) EL CONTRATISTA deberá asegurar y garantizar, que el Servicio de Cloud Computing que oferte, cuente de forma inicial con todas las capacidades especificadas en las Características actuales de los servicios del SENCICO descritos en la Tabla N° 01.

Tabla N° 01 - Características actuales de los servicios del SENCICO

Nro	ID	Zona	Entorno	Tipo	Sistema Operativo	**Servicio	Nube	Clasificación	vCPU	vRAM
1	SERVIDOR 1	Produccion	Bases de Datos	PaaS	RDS	Oracle SE2 19c	AWS	BD Tipo 1	4	32
2	SERVIDOR 2	Produccion	Bases de Datos	IaaS	Windows Server 2016	MS-SQL Standard 2016	AWS	BD Tipo 3	16	64
3	SERVIDOR 3	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_01	AWS	Web Tipo 1	1	2
4	SERVIDOR 4	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_02	AWS	Web Tipo 1	1	2
5	SERVIDOR 5	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_03	AWS	Web Tipo 1	1	2
6	SERVIDOR 6	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_04	AWS	Web Tipo 1	1	2
7	SERVIDOR 7	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_05	AWS	Web Tipo 1	1	2
8	SERVIDOR 8	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_06	AWS	Web Tipo 1	1	2
9	SERVIDOR 9	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_07	AWS	Web Tipo 1	1	2
10	SERVIDOR 10	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_08	AWS	Web Tipo 1	1	2
11	SERVIDOR 11	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_09	AWS	Web Tipo 1	1	2
12	SERVIDOR 12	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_10	AWS	Web Tipo 1	1	2
13	SERVIDOR 13	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_11	AWS	Web Tipo 1	1	2
14	SERVIDOR 14	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_12	AWS	Web Tipo 1	1	2
15	SERVIDOR 15	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_13	AWS	Web Tipo 1	1	2
16	SERVIDOR 16	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_14	AWS	Web Tipo 1	1	2
17	SERVIDOR 17	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_15	AWS	Web Tipo 1	1	2
18	SERVIDOR 18	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_16	AWS	Web Tipo 1	1	2
19	SERVIDOR 19	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_17	AWS	Web Tipo 1	1	2
20	SERVIDOR 20	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_18	AWS	Web Tipo 1	1	2
21	SERVIDOR 21	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_19	AWS	Web Tipo 1	1	2
22	SERVIDOR 22	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_20	AWS	Web Tipo 1	1	2
23	SERVIDOR 23	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_21	AWS	Web Tipo 1	1	2
24	SERVIDOR 24	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_22	AWS	Web Tipo 1	1	2
25	SERVIDOR 25	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_23	AWS	Web Tipo 1	1	2
26	SERVIDOR 26	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_24	AWS	Web Tipo 1	1	2
27	SERVIDOR 27	Produccion	Aplicaciones Web	PaaS	Windows Server 2019	App_25	AWS	Web Tipo 1	1	2



28	SERVIDOR 28	Produccion	Directorio Activo	IaaS	Windows Server 2016	Active Directory	AWS	Tipo 5	4	8
29	SERVIDOR 29	Produccion	Directorio Activo	IaaS	Windows Server 2016	Active Directory	AWS	Tipo 5	4	8
30	SERVIDOR 30	Produccion	Complementarios	IaaS	Windows Server 2016	SIAF	Azure	Tipo 6	4	16
31	SERVIDOR 31	Produccion	Complementarios	IaaS	Windows Server 2016	SIAF	Azure	Tipo 3	2	8
32	SERVIDOR 32	Produccion	Complementarios	IaaS	Linux CentOS 7	Sistema Moodle	AWS	Tipo 8	8	32
33	SERVIDOR 33	Produccion	Complementarios	IaaS	Windows Server 2016	Sistema web	AWS	Tipo 3	2	8
34	SERVIDOR 34	Produccion	Complementarios	IaaS	Linux CentOS 7	Glassfish	AWS	Tipo 4	2	8
35	SERVIDOR 35	Produccion	Complementarios	IaaS	Windows Server 2016	Sistema web	AWS	Tipo 5	4	8
36	SERVIDOR 36	Produccion	Complementarios	IaaS	Windows Server 2016	Sistema web	AWS	Tipo 5	4	8
37	SERVIDOR 37	Produccion	Complementarios	IaaS	Windows Server 2016	Sistema web	AWS	Tipo 5	4	8
38	SERVIDOR 38	Produccion	Complementarios	IaaS	Windows Server 2016	FTP	AWS	Tipo 1	2	4
39	SERVIDOR 39	Produccion	Complementarios	IaaS	Windows Server 2016	File Server	AWS	Tipo 5	4	8
40	SERVIDOR 40	Produccion	Complementarios	IaaS	Windows Server 2016	File Server	AWS	Tipo 5	4	8
41	SERVIDOR 41	Produccion	Complementarios	IaaS	Windows Server 2016	File Server	AWS	Tipo 1	2	4
42	SERVIDOR 42	Produccion	Complementarios	IaaS	Windows Server 2016	Sistema documental	AWS	Tipo 6	4	16
43	SERVIDOR 43	Produccion	Complementarios	IaaS	Windows Server 2016	Sistema web	AWS	Tipo 1	2	4
44	SERVIDOR 44	Produccion	Complementarios	IaaS	Linux Ubuntu 16 LTS	Sistema web	AWS	Tipo 2	2	4
45	SERVIDOR 45	Produccion	Complementarios	IaaS	Windows Server 2016	Sistema web	AWS	Tipo 3	2	8
46	SERVIDOR 46	Produccion	Complementarios	IaaS	Windows Server 2016	Sistema web	AWS	Tipo 3	2	8
47	SERVIDOR 47	Produccion	Complementarios	IaaS	Windows Server 2016	Sistema web	AWS	Tipo 5	4	8
48	SERVIDOR 48	Produccion	Complementarios	IaaS	Windows Server 2016	Sistema Helpdesk	AWS	Tipo 5	4	8
49	SERVIDOR 49	Produccion	Complementarios	IaaS	Windows Server 2016	Sistema antivirus	AWS	Tipo 6	4	16
50	SERVIDOR 50	Produccion	Complementarios	IaaS	Amazon Linux	Sistema web	AWS	Tipo 7	8	16
51	SERVIDOR 51	Produccion	Complementarios	IaaS	Linux CentOS 7	Sistema web	AWS	Tipo 4	2	8
52	SERVIDOR 52	Desarrollo	Bases de Datos	PaaS	RDS	Oracle SE2 19c	AWS	BD Tipo 2	4	16
53	SERVIDOR 53	Desarrollo	Bases de Datos	IaaS	Windows Server 2016	MS-SQL Standard 2016	AWS	BD Tipo 4	4	8
54	SERVIDOR 54	Calidad/TST	Bases de Datos	PaaS	RDS	Oracle SE2 19c	AWS	BD Tipo 2	4	16

**Se precisa que, La tipificación descrita en la columna “Clasificación” de la Tabla Nro. 01 corresponde a un ordenamiento de servidores en base a su similitud de capacidades (CPU, RAM).*

** Se precisa que SENCICO cuenta con aplicaciones web de tipo .Net, .Net Core 3, PHP 7.2, NodeJS 10.19, Glassfish, Java 8.2, .Net Framework 3.5.*

** Las aplicaciones web se encuentran compiladas y empaquetadas en formato .zip. El Contratista deberá realizar la preparación de despliegue en los entornos que proponga de acuerdo a la sección “Sección C. Servicio de Aplicaciones web, punto a)”.*

*** Lo descrito corresponde a una información general. El detalle técnico de cada servicio será entregado al postor ganador.*

C. Servicios de Aplicaciones Web

EL CONTRATISTA deberá considerar lo siguiente durante la implementación de los servidores asociados a los servicios de aplicaciones web:

- EL CONTRATISTA deberá implementar los entornos para aplicaciones web, proveyendo plataformas administradas de tipo PaaS (Platform-as-a-Services) o de tipo contenedores, y de uso específico para aplicaciones web productivas.
- EL CONTRATISTA deberá provisionar los entornos necesarios para aislar cada una de las siguientes aplicaciones web:

Nro	Servidor	Servicio	Plataforma	Tipo
1	SERVIDOR 3	APP_01	Windows	Net Core / .Net
2	SERVIDOR 4	APP_02	Windows	Net Core / .Net
3	SERVIDOR 5	APP_03	Windows	Net Core / .Net

4	SERVIDOR 6	APP_04	Windows	Net Core / .Net
5	SERVIDOR 7	APP_05	Windows	Net Core / .Net
6	SERVIDOR 8	APP_06	Windows	Net Core / .Net
7	SERVIDOR 9	APP_07	Windows	Net Core / .Net
8	SERVIDOR 10	APP_08	Windows	Net Core / .Net
9	SERVIDOR 11	APP_09	Windows	Net Core / .Net
10	SERVIDOR 12	APP_10	Windows	Net Core / .Net
11	SERVIDOR 13	APP_11	Windows	Net Core / .Net
12	SERVIDOR 14	APP_12	Windows	Net Core / .Net
13	SERVIDOR 15	APP_13	Windows	Net Core / .Net
14	SERVIDOR 16	APP_14	Windows	Net Core / .Net
15	SERVIDOR 17	APP_15	Windows	Net Core / .Net
16	SERVIDOR 18	APP_16	Windows	Net Core / .Net
17	SERVIDOR 19	APP_17	Windows	Net Core / .Net
18	SERVIDOR 20	APP_18	Windows	Net Core / .Net
19	SERVIDOR 21	APP_19	Windows	Net Core / .Net
20	SERVIDOR 22	APP_20	Windows	Net Core / .Net
21	SERVIDOR 23	APP_21	Windows	Net Core / .Net
22	SERVIDOR 24	APP_22	Windows	Net Core / .Net
23	SERVIDOR 25	APP_23	Windows	Net Core / .Net
24	SERVIDOR 26	APP_24	Windows	Net Core / .Net
25	SERVIDOR 27	APP_25	Windows	Net Core / .Net

**Se precisa que, SENCICO cuenta con aplicaciones web de tipo .Net, .Net Core 3, PHP 7.2, NodeJS 10.19, Glassfish, Java 8.2, .Net Framework 3.5.*

** Las aplicaciones web se encuentran compiladas y empaquetadas en formato .zip. El Contratista deberá realizar la preparación de despliegue en los entornos que proponga de acuerdo a la sección “Sección C. Servicio de Aplicaciones web, punto a)”.*

- c) EL CONTRATISTA deberá provisionar de forma adicional a lo descrito en el punto anterior, los entornos necesarios para implementar cada una de las siguientes nuevas aplicaciones web, con capacidades de 1 vCPU, 2GB RAM y 100Gb de almacenamiento:

Nro	Servidor	Servicio	Plataforma	Tipo
1	SERVIDOR NUEVO 1	APP_26	Windows	Net Core / .Net
2	SERVIDOR NUEVO 2	APP_27	Windows	Net Core / .Net
3	SERVIDOR NUEVO 3	APP_28	Windows	Net Core / .Net
4	SERVIDOR NUEVO 4	APP_29	Windows	Net Core / .Net
5	SERVIDOR NUEVO 5	APP_30	Windows	Net Core / .Net
6	SERVIDOR NUEVO 6	APP_31	Windows	Net Core / .Net
7	SERVIDOR NUEVO 7	APP_32	Windows	Net Core / .Net
8	SERVIDOR NUEVO 8	APP_33	Windows	Net Core / .Net
9	SERVIDOR NUEVO 9	APP_34	Windows	Net Core / .Net
10	SERVIDOR NUEVO 10	APP_35	Windows o Linux	PHP

Se precisa que lo descrito en la tabla predecesora, denominados como “SERVIDORES NUEVOS” corresponden a servicios adicionales a lo descrito en la Tabla Nro 1.

- d) EL CONTRATISTA deberá implementar balanceadores webs de tipo aplicaciones, para cada una de las aplicaciones web desplegadas; por lo que se deberá proveer balanceador de carga por cada aplicación.
El Contratista deberá dimensionar el tamaño de los balanceadores de acuerdo a su relevamiento de información, tomando en cuenta las capacidades de las “Aplicaciones web” descritas en la sección B. Habilitación de Ambientes Cloud, punto a), Tabla Nro. 1” y considerando lo indicado en la Sección C. Servicio de Aplicaciones Web, punto g)” que indica “EL CONTRATISTA deberá configurar las plataformas para que escalen en forma horizontal y/o vertical, de manera automatizadas basada en patrones de comportamiento (uso de CPU, uso de RAM) definiendo límites mínimos y máximos de crecimiento.”
- e) EL CONTRATISTA deberá provisionar certificados de seguridad SSL para cada una de las aplicaciones web desplegadas en las plataformas, de acuerdo a lo tipificado en la sección “Seguridad – Certificados SSL”. El Contratista deberá generar certificados nuevos.
- f) EL CONTRATISTA deberá configurar cada plataforma para que pueda conectarse a los servicios de bases de datos Oracle, Microsoft SQL y MySQL, y a los servicios de Active Directory.
- g) EL CONTRATISTA deberá configurar las plataformas para que escalen en forma horizontal y/o vertical, de manera automatizadas basada en patrones de

comportamiento (uso de CPU, uso de RAM) definiendo límites mínimos y máximos de crecimiento.

- h) EL CONTRATISTA deberá utilizar versiones de sistema operativo que no cuenten con “EOL” (End of Life) o “EOS” (End of Support) declarado por los fabricantes y/o por la(s) nube(s) durante el plazo de contratación. En caso de que exista una declaración oficial con fechas programadas dentro del plazo del contrato, EL CONTRATISTA deberá realizar el proceso de migración y actualización de los sistemas operativos a las versiones soportadas por los fabricantes, en coordinación con SENCICO. SENCICO no proveerá ningún licenciamiento.

D. Servicios de Bases de Datos

EL CONTRATISTA deberá considerar lo siguiente durante la implementación de los servidores asociados a los servicios de bases de datos:

- a) EL CONTRATISTA deberá proveer servicios administrados y/o plataformas administradas para los entornos de bases de datos Oracle, Microsoft SQL y MariaDB/MySQL, incluyendo la gestión del sistema operativo, motor de base de datos, acciones de monitoreo, mantenimiento y optimización de plataforma, con el fin de asegurar la disponibilidad y no degradación del servicio.

Se precisa que se permite la implementación mediante IaaS (Infrastructure-as-a-Services), PaaS (Platform-as-a-Services), DBaaS (Databases as a Services) o con tecnologías similares disponibles en la(s) nube(s) propuesta(s).

El Contratista deberá proponer la infraestructura más adecuada que cumpla con todos los puntos indicados en la presente sección, considerando que lo requerido es un “servicio” y/o “plataforma”.

- b) EL CONTRATISTA deberá implementar plataformas de uso específico para bases de datos, de alto rendimiento, que soporten el nivel de operaciones de las bases de datos del SENCICO.
- c) EL CONTRATISTA deberá proveer el licenciamiento necesario para cada una de las soluciones de base de datos, de acuerdo a su levantamiento de información.
- d) EL CONTRATISTA deberá contar con personal especialista, para implementar y gestionar los entornos de base de datos de acuerdo a las buenas prácticas de cada fabricante.
- e) EL CONTRATISTA deberá provisionar los siguientes entornos:

Nro	Servidor	Servicio	Versión mínima
1	SERVIDOR 1	Oracle	Oracle SE2 19c
2	SERVIDOR 2	Microsoft SQL	MS-SQL 2016
3	SERVIDOR NUEVO	MariaDB	MariaDB 10.4

Se precisa que los ítems “SERVIDOR 1” y “SERVIDOR 2” se corresponden con la Tabla Nro 1, en donde indica que actualmente se encuentran en AWS y se describen las capacidades requeridas.

Se precisa que el ítem “SERVIDOR NUEVO” corresponde a un servicio adicional a lo descrito en la Tabla Nro 1, por lo que actualmente no existe. Así mismo, se precisa que las características requeridas para este servidor son: 2 vCPU, 8Gb RAM, disco 36Gb

Se precisa que, las versiones superiores a la mínima solicitadas que han sido validadas son las siguientes:

- MS-SQL: 2016 y 2019
- Oracle: 19c
- MariaDB: 10.4

- f) EL CONTRATISTA deberá implementar conexiones de “Linked-Server” entre las bases de datos Microsoft SQL y Oracle.
- g) EL CONTRATISTA deberá configurar las plataformas para que escalen en forma automatizada basada en patrones de comportamiento (uso de CPU, uso de RAM) definiendo límites mínimos y máximos de crecimiento.
- h) EL CONTRATISTA deberá verificar que las versiones de los motores de bases de datos implementados no cuenten con “EOL” (End of Life) o “EOS” (End of Support) declarado por los fabricantes y/o por la(s) nube(s) durante el plazo de contratación. En caso de que exista una declaración oficial con fechas programadas dentro del plazo del contrato, EL CONTRATISTA deberá realizar

el proceso de migración y actualización de los motores a las versiones soportadas por la(s) nube(s) en coordinación con SENCICO.

E. Servicios de Directorio Activo

EL CONTRATISTA deberá considerar lo siguiente durante la implementación de los servidores asociados a los servicios de directorio activo (autenticación):

- a) El SENCICO cuenta con servicios de directorio activo implementados en las nubes actuales, bajo el siguiente esquema:

Nro	Servidor	Servicio	Objetos
1	SERVIDOR 28	AD Administrativo	1,000
2	SERVIDOR 29	AD Académico/Educativo	10,000

* La tabla descrita en este punto se corresponde con la Tabla Nro 1, en donde indica que se encuentran en AWS (columna "Nube" de la Tabla Nro 1).

* La tabla descrita en este punto se corresponde con la Tabla Nro 1, en donde se encuentra la descripción de capacidades de CPU y RAM. Así mismo, las capacidades de almacenamiento se describen en la "sección G. Almacenamiento, punto b)".

Se precisa que el dominio administrativo es distinto al dominio educativo, que el bosque administrativo es distinto al bosque educativo y que si existe relación de confianza entre ambos dominios.

- b) EL CONTRATISTA deberá implementar los servidores necesarios e integrarlos a los dominios correspondientes.
- c) EL CONTRATISTA deberá garantizar una correcta integración / replicación de datos en los servidores implementados para los servicios de directorio activo.
- d) Se precisa que el SENCICO cuenta con una sincronización de cuentas hacia el servicio de "Microsoft Office 365" mediante el software "Microsoft AD Connect", implementados en los directorios activos administrativo y académico/educativo de la nube actual. EL CONTRATISTA deberá implementar esta sincronización en los nuevos servidores desplegados.

En la Tabla Nro. 1, columna "Nube" se indica la locación actual de los servidores de Directorio Activo de nube, encontrándose en AWS.

Se aclara que, los roles principales de Directorio Activo deberán estar en nube.

Se precisa que SENCICO tiene y mantendrá réplicas de los directorios activos en on-premise en modo GC (Global Catalog).

El equipo de arquitectos cloud del Contratista deberá proponer el escenario más adecuado para el rol de "AD Connect". Este rol podrá convivir en los mismos servidores AD o en servidores dedicados.

- e) EL CONTRATISTA deberá garantizar la no afectación de acceso a los usuarios durante la implementación del servicio y sincronización del aplicativo "Microsoft AD Connect".

F. Servicios Conexos

EL CONTRATISTA deberá considerar lo siguiente durante la implementación de servidores asociados a los siguientes servicios:

- a) EL CONTRATISTA deberá proveer e implementar un servicio de tipo "web services" con conexión nativa hacia el almacenamiento de nube. Este servicio será utilizado por los "servicios de aplicaciones web" para el almacenamiento de archivos.

Nro	Servidor	Servicio	Plataforma
1	SERVIDOR NUEVO	API Web Storage	Windows

Se precisa que este ítem, denominado como "SERVIDOR NUEVO" corresponde a un servicio adicional a lo descrito en la Tabla Nro 1. Este servicio podrá ser provisto mediante IaaS (Infrastructure-as-a-Services), PaaS (Platform-as-a-Services) o contenedores.

El Contratista deberá determinar las capacidades más adecuadas, considerando que el punto en mención requiere la implementación como "servicio" y se permite el despliegue en modo IaaS, PaaS o contenedores.

- b) EL CONTRATISTA deberá proveer e implementar un servicio de transmisión SFTP (Secure FTP), provisionando la infraestructura y el certificado de seguridad SSL público necesarios.

Nro	Servidor	Servicio	Plataforma
1	SERVIDOR 38	SFTP	Servicio

Se precisa que este servicio podrá ser provisto mediante IaaS (Infrastructure-as-a-Services), PaaS (Platform-as-a-Services) o como un servicio nativo de nube. El Contratista deberá determinar las capacidades más adecuadas, considerando que el punto en mención requiere la implementación como “servicio” y se permite el despliegue en modo IaaS, PaaS o contenedores.

Las capacidades de almacenamiento se encuentran tipificadas en la sección “G. Almacenamiento, punto b)”.

- c) EL CONTRATISTA deberá proveer e implementar un servicio de retransmisión SMTP autenticado para el envío de email’s de todos los sistemas internos. EL CONTRATISTA deberá realizar las configuraciones necesarias para que los mensajes no sean catalogados como spam.

Nro	Servidor	Servicio	Mensajes promedio por Mes	promedio por mensaje
1	SERVIDOR NUEVO	SMTP	12,000	50 Kb

Se precisa que este servicio podrá ser provisto mediante un servicio nativo de nube, o como IaaS (Infrastructure-as-a-Services), o como PaaS (Platform-as-a-Services). Así mismo, se deberá contar con un log detallado de los mensajes enviados, entregados, rechazados, rebotados, reclamaciones.

El Contratista deberá determinar las capacidades más adecuadas, considerando que el punto en mención requiere la implementación como “servicio” y se permite el despliegue en modo IaaS o PaaS o contenedores.

Se aclara que, el punto en mención tipifica que el servicio será utilizado por “todos los sistemas internos”. Se precisa que éstos serán los sistemas de nube(s) y/o de on-premise.

Actualmente se utiliza el servicio SMTP de Office 365.

G. Almacenamiento

- a) EL SENCICO requiere una provisión de almacenamiento a demanda desde el inicio del servicio, provisto de acuerdo al uso del mismo.
- b) EL CONTRATISTA deberá implementar de forma inicial el almacenamiento actual utilizado por SENCICO:

Nro	Servidor	Zona	Storage (GB)
1	SERVIDOR 1	Produccion	1500
2	SERVIDOR 2	Produccion	580
3	SERVIDOR 3	Produccion	100
4	SERVIDOR 4	Produccion	100
5	SERVIDOR 5	Produccion	100
6	SERVIDOR 6	Produccion	100
7	SERVIDOR 7	Produccion	100
8	SERVIDOR 8	Produccion	100
9	SERVIDOR 9	Produccion	100
10	SERVIDOR 10	Produccion	100
11	SERVIDOR 11	Produccion	100
12	SERVIDOR 12	Produccion	100
13	SERVIDOR 13	Produccion	100
14	SERVIDOR 14	Produccion	100
15	SERVIDOR 15	Produccion	100
16	SERVIDOR 16	Produccion	100
17	SERVIDOR 17	Produccion	100
18	SERVIDOR 18	Produccion	100
19	SERVIDOR 19	Produccion	100
20	SERVIDOR 20	Produccion	100
21	SERVIDOR 21	Produccion	100
22	SERVIDOR 22	Produccion	100
23	SERVIDOR 23	Produccion	100
24	SERVIDOR 24	Produccion	100
25	SERVIDOR 25	Produccion	100
26	SERVIDOR 26	Produccion	100

27	SERVIDOR 27	Produccion	100
28	SERVIDOR 28	Produccion	80
29	SERVIDOR 29	Produccion	80
30	SERVIDOR 30	Produccion	639
31	SERVIDOR 31	Produccion	127
32	SERVIDOR 32	Produccion	2500
33	SERVIDOR 33	Produccion	140
34	SERVIDOR 34	Produccion	200
35	SERVIDOR 35	Produccion	200
36	SERVIDOR 36	Produccion	200
37	SERVIDOR 37	Produccion	100
38	SERVIDOR 38	Produccion	150
39	SERVIDOR 39	Produccion	1270
40	SERVIDOR 40	Produccion	650
41	SERVIDOR 41	Produccion	90
42	SERVIDOR 42	Produccion	1650
43	SERVIDOR 43	Produccion	150
44	SERVIDOR 44	Produccion	40
45	SERVIDOR 45	Produccion	245
46	SERVIDOR 46	Produccion	400
47	SERVIDOR 47	Produccion	491
48	SERVIDOR 48	Produccion	250
49	SERVIDOR 49	Produccion	150
50	SERVIDOR 50	Producción	500
51	SERVIDOR 51	Producción	500
52	SERVIDOR 52	Desarrollo	2040
53	SERVIDOR 53	Desarrollo	450
54	SERVIDOR 54	Calidad/TST	1500
TOTAL			19,372

- c) EL CONTRATISTA deberá adicionar a la tabla anterior, el almacenamiento requerido para los SERVIDORES NUEVOS especificados en el presente TDR.
- d) EL CONTRATISTA deberá verificar y configurar las particiones/discos de todos los servidores descritos en la Tabla Nro 1, de tal forma que se permita su crecimiento de forma autónoma sin interrupción de servicios.

H. Servicio DNS público

- a) Se precisa que el SENCICO cuenta con dos (02) dominios públicos en internet, mediante el cual gestiona los registros DNS de los sistemas públicos de la entidad.
- b) EL CONTRATISTA deberá implementar y gestionar un servicio de DNS público para albergar los dominios DNS del SENCICO:

Nro	Ámbito	Dominio
1	Administrativo	sencico.gob.pe
2	Académico/Educativo	sencico.edu.pe

I. Servicios de Red

- a) EL CONTRATISTA deberá definir e implementar las reglas de ruteo y comunicación entre las redes de la(s) plataforma(s) de nube(s), previa validación del Departamento de Informática del SENCICO.
- b) EL CONTRATISTA deberá garantizar una latencia razonable e interconexión adecuada para que el uso de los servicios, aplicaciones, sistemas y bases de datos del SENCICO se desarrollen de manera correcta y eficiente.
- c) EL CONTRATISTA deberá incluir servicios de conexión VPN segura, que permita establecer sesiones seguras y privadas con túneles de IP security (IPSEC) y seguridad de la capa de transporte (TLS), con certificado SSL/TLS v3, cuya llave deberá ser generada dentro de la plataforma de nube.
- d) **Conectividad dentro de la nube**
El contratista deberá garantizar una latencia promedio de 1ms (1 milisegundo) en todas las conexiones de red internas dentro de la nube.
- e) **Conectividad entre nubes**
En el caso que el contratista contemple la implementación de múltiples nubes, deberá proveer lo siguiente:
- Interconectar las nubes entre sí mediante conexión VPN-Site-to-Site o similar, con el fin de establecer una red privada segura.
 - Garantizar una latencia máxima de 10ms (10 milisegundos) en la comunicación entre nubes.
- f) **Conectividad con SENCICO**

El contratista deberá interconectar la nube y/o nubes hacia la red privada del SENCICO mediante VPN-Site-to-Site o similar, a través de los enlaces a internet del SENCICO. Se precisa que el SENCICO cuenta con equipos de seguridad Next-Generation/SD-WAN en cada sede a nivel nacional.

g) Conectividad a Internet

- EL CONTRATISTA deberá incluir las IP Públicas necesarias de acuerdo al número de servicios publicados hacia internet en la(s) nube(s) que proponga.
- EL CONTRATISTA deberá garantizar el acceso a internet de los servidores y servicios implementados en la nube, estableciendo mecanismos de filtrado y restricción, de acuerdo a las políticas de seguridad que determine el SENCICO.
- Se precisa que inicialmente se publicarán 45 servicios web hacia internet.

J. Seguridad

Protección de Datos

- a) Toda la solución requerida deberá contar con mecanismos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.
- b) La solución proporcionada por EL CONTRATISTA deberá de manejar alguno de los siguientes protocolos de cifrado: AES o TDES o RSA o ECC para la protección de la transmisión de datos de todo el(los) entorno(s) cloud computing implementado(s)
- c) Los servicios de nube(s) deben soportar la seguridad de datos de acuerdo con lo siguiente:
 - Datos en tránsito: con capacidad de cifrado con llave externa proporcionada por la(s) nube(s).
 - Datos en reposo: con capacidad de cifrado de datos proveído por la plataforma y capacidad de cifrado de la(s) unidades de almacenamiento con llave externa proporcionada por la(s) nube(s).
- d) EL CONTRATISTA deberá habilitar medidas de seguridad a nivel de red que minimicen el impacto y/o alcance de ciberataques a los servicios.

Protección Perimetral / Anti-DDOS

- a) EL CONTRATISTA deberá de proporcionar un servicio de Protección Perimetral de internet, considerando como mínimo las funcionalidades de: Next Generation Firewall, IPS, Antivirus, DLP, Control de aplicaciones, Sandboxing, antiDDoS y VPN (SSL & IPSEC). Opcionalmente podrá proveer mecanismos de evaluación en la adopción de mejores prácticas del fabricante de la solución propuesta. Se precisa que, lo solicitado es que la soporte IPv6 para todo el entorno, de acuerdo al Decreto Supremo N°081-2017-PCM (Transición al protocolo IPv6 para las entidades de la Administración Pública), para su posterior implementación.
- b) EL CONTRATISTA deberá implementar la protección perimetral en alta disponibilidad, mediante la implementación en múltiples zonas de disponibilidad, de tal forma que cumplan con la disponibilidad requerida en la sección “Disponibilidad del Servicio” del presente TDR.
- c) El servicio deberá estar operativo durante todo el plazo del contrato, y cubrir un incremento anual del 10% en el número de servidores/servicios cubiertos por el servicio.
- d) El servicio debe permitir que SENCICO restrinja el acceso a determinados recursos basados en protocolos, URL's y direcciones IP, tanto para los servidores como plataformas y servicios.
- e) EL CONTRATISTA deberá considerar la publicación de servicios para su acceso desde internet.
- f) EL CONTRATISTA deberá proveer, a través de las tecnologías de la(s) nube(s), un servicio de mitigación de ataques DDoS desde internet.
- g) Para el caso de entornos multi-cloud/multi-nube, EL CONTRATISTA deberá proveer el mismo nivel de protección perimetral, restricción de accesos y Anti-DDOS en cada nube propuesta, ya sea con la misma solución de protección o una equivalente.

Protección de Aplicaciones Web / WAF

- a) EL CONTRATISTA deberá implementar una solución de “WAF – Firewall de aplicaciones web” para proteger todos los sitios web, aplicaciones y API's del

SENCICO expuestos hacia internet, en todas la(s) nube(s) implementada(s). Se precisa que la cantidad de dominio que se protegerán las aplicaciones es 01 TLD: sencico.gob.pe. El tráfico promedio total al mes de los dominios que serán protegidos es 9Tb/mes.

- b) El servicio deberá estar operativo durante todo el plazo del contrato, y cubrir un incremento anual del 10% en el número de aplicaciones web cubiertas por el servicio.
- c) EL CONTRATISTA deberá brindar un control sobre el tráfico recibido HTTP / HTTPS, deberá crear reglas de seguridad diferenciadas por tipo de aplicación.
- d) El servicio WAF deberá bloquear como mínimo los patrones de ataque comunes, de inyección SQL, Cross-Site Scripting (XSS), entre otras vulnerabilidades descritas por OWASP.
- e) El servicio WAF deberá proveer reglas de seguridad pre-establecidas de acuerdo a las tecnologías web que utilice el SENCICO. SENCICO tiene las siguientes tecnologías WEB: PHP, .Net Core, .Net Framework, Java, NodeJS.

Protección de Bases de Datos

- a) EL CONTRATISTA deberá implementar un servicio de protección contra ataques a las Bases de datos del SENCICO mediante una plataforma dedicada.
- b) El servicio de protección deberá alcanzar a todas las bases de datos descritas en la sección “D. Servicios de Bases de Datos”.
- c) El servicio deberá estar operativo durante todo el plazo del contrato, y cubrir un incremento anual del 10% en el número de bases de datos cubiertos por el servicio. Se precisa que, este requerimiento está en la lista de precios unitarios, por lo que la Entidad pagará lo consumido mensual, según corresponda.
- d) Se precisa que la protección deberá comprender una plataforma que permita analizar la sensibilidad de los datos, enmascarar datos confidenciales, implementar y monitorear controles de seguridad, evaluar la seguridad del usuario, monitorear la actividad del usuario y abordar los requisitos de cumplimiento de seguridad de datos.
- e) EL CONTRATISTA deberá implementar la protección de base de datos en alta disponibilidad, mediante la implementación en múltiples zonas de disponibilidad, de tal forma que cumplan con la disponibilidad requerida en la sección “Disponibilidad del Servicio” del presente TDR.

Certificados SSL

- a) EL CONTRATISTA deberá implementar un servicio que permita provisionar, administrar y desplegar certificados de seguridad SSL/TLS públicos y privados válidos en internet.
- b) Los certificados emitidos deberán asignarse a todos los servicios implementados en nube(s) que lo requieran, y deberá permitir ser exportados para su implementación en servicios de tipo IaaS (IIS, Apache, Glassfish) en el(los) entorno(s) de nube(s).
- c) Los certificados emitidos deberán cumplir con las siguientes características mínimas, y podrán ser emitidos como servicios nativos de nube o mediante plataformas externas:
 - Estándar X.509 v3.
 - Algoritmo de cifrado mínimo: SHA-2 (Secure Hash Algorithm 2)
 - Longitud de la clave: de 2048, 3072 o 4096 bits
 - Nivel de Cifrado de 128 como mínimo hasta 256 bits de encriptación.
 - Soporte de OCSP (online certificate Status protocol) y CRL (Certificate Revocation List).
 - Soporte IDN (Internacional Domain names).
 - Remisiones gratuitas ilimitadas todo el tiempo contratado.
 - Compatibilidad con el 99.9% de navegadores (MS Edge, Safari, IE, Mozilla, Chrome, Opera, etc).
 - Certificado emitido por Root certificate Authority – CA (certification authority).
- d) EL CONTRATISTA deberá implementar certificados SSL de forma inicial a los siguientes servidores/servicios:

Nro	ID
1	SERVIDOR 3
2	SERVIDOR 4
3	SERVIDOR 5
4	SERVIDOR 6

5	SERVIDOR 7
6	SERVIDOR 8
7	SERVIDOR 9
8	SERVIDOR 10
9	SERVIDOR 11
10	SERVIDOR 12
11	SERVIDOR 13
12	SERVIDOR 14
13	SERVIDOR 15
14	SERVIDOR 16
15	SERVIDOR 17
16	SERVIDOR 18
17	SERVIDOR 19
18	SERVIDOR 20
19	SERVIDOR 21
20	SERVIDOR 22
21	SERVIDOR 23
22	SERVIDOR 24
23	SERVIDOR 25
24	SERVIDOR 26
25	SERVIDOR 27
26	SERVIDOR 32
27	SERVIDOR 33
28	SERVIDOR 34
29	SERVIDOR 35
30	SERVIDOR 36
31	SERVIDOR 37
32	SERVIDOR 38
33	SERVIDOR 42
34	SERVIDOR 43
35	SERVIDOR 44
36	SERVIDOR 45
37	SERVIDOR 48
38	SERVIDOR 50
39	SERVIDOR 51

- e) EL CONTRATISTA deberá implementar adicionalmente, certificados SSL a los 10 servidores/servicios nuevos descritos en la sección “II.C. Servicios de Aplicaciones web, punto c)” y a todo servicio que implemente y se encuentre expuesto hacia internet.

Antivirus/Antiransomware

- a) EL CONTRATISTA deberá implementar un servicio de protección antivirus/antiransomware y antiexploits en todos los servidores de tipo IaaS (Infrastructure-as-a-Services).
- b) El servicio deberá identificar automáticamente las actividades sospechosas mediante mecanismos de machine learning o similares.
- c) El servicio deberá permitir la búsqueda de amenazas potenciales, así como la identificación de amenazas desconocidas.
- d) EL CONTRATISTA deberá implementar acciones para interrumpir y contener amenazas a los servicios implementados.
- e) El servicio deberá ser gestionado de forma centralizada desde una consola web basada en nube, y deberá otorgarse acceso de sólo lectura al personal del Departamento de Informática del SENCICO.
- f) Actualmente SENCICO cuenta con soluciones de Sophos.
- g) La solución de software deberá ser específicamente para sistemas operativos de tipo servidor (Windows / Linux). En cuanto a las versiones de los sistemas operativos, se solicita que deberá ser para todos los servidores de tipo IaaS, correspondiendo al Contratista validar con la versión final de sistema operativo que implementará en cada servidor de nube.
- h) Así mismo, la protección antivirus/antiransomware y antiexploits deberá implementarse en todos los servicios de escritorio remoto virtual (Windows Desktop).

Evaluación continua de Vulnerabilidades

- a) EL CONTRATISTA deberá implementar un servicio de evaluación automática y continua de vulnerabilidades en todos los servicios implementados en nube(s), tanto públicos como privados.

- b) El servicio deberá ejecutar análisis de forma mensual para todos los servicios y aplicaciones del ambiente Producción, Calidad y Desarrollo.
- c) El servicio deberá estar operativo durante todo el plazo del contrato, y cubrir un incremento anual del 10% en el número de aplicaciones cubiertos por el servicio.
- d) En análisis de vulnerabilidades deberá incluir el código fuente de las aplicaciones desarrolladas por el SENCICO. Se aclara que, lo que se solicita es detectar y corregir configuraciones inseguras en las plantillas de Infraestructura as Code (IaC) durante las fases previas a la implementación, estas plantillas podrán ser validadas con respecto a las mejores prácticas de implementación y los parámetros de seguridad integrados antes de implementarlas en el entorno de nube.
- e) El servicio deberá buscar exposiciones, vulnerabilidades y desviaciones en relación a las prácticas de seguridad recomendadas por OWASP.
- f) El servicio deberá analizar las configuraciones de red, de permisos y de puertos abiertos de los servicios implementados en nube(s).
- g) EL CONTRATISTA deberá gestionar e implementar de forma continua las “actualizaciones de seguridad” de SO’s (sistemas operativos) publicados por los fabricantes, con alcance a todos los servidores y servicios implementados. Las actualizaciones deberán ser autorizadas y coordinadas con el Departamento de Informática del SENCICO.

K. Postura de Seguridad

- a) EL CONTRATISTA deberá implementar un servicio de seguridad para los activos implementados en la(s) nube(s), de tal forma que brinde gestión y una postura de seguridad, que permitirá detectar errores de configuración, modelar y hacer cumplir activamente los estándares de seguridad de la nube (CIS, GDPR, HIPAA, ISO-27001, NIST-800, PCI-DSS, SOC 2 & Cloud Security Alliance, o similares), proteger contra ataques y amenazas internas, así como, brindar inteligencia de seguridad para la detección de vulnerabilidades en la(s) nube(s).
Se aclara que la sección en mención hace referencia a una solución de software con la infraestructura que requiera para soportar dicha solución.
- b) EL CONTRATISTA deberá gestionar el servicio durante todo el plazo del contrato, manteniendo en operación el mismo, realizando el monitoreo permanente de los eventos generados por el mismo, y tomando acciones de remediación ante eventos de seguridad que impacten lo implementado en la(s) nube(s), en coordinación con SENCICO.
- c) El servicio deberá estar operativo durante todo el plazo del contrato, y cubrir un incremento anual del 10% en el número de servidores/servicios cubiertos por el servicio. Se precisa que, en el caso que este requerimiento este en la lista de precios unitarios (Tabla N°02), la Entidad pagará lo consumido mensual, según corresponda. Y si en caso el servidor/servicio se encuentre en la lista de precios fijos (Tabla N°03), se pagará a través de una Adenda contractual.
- d) El servicio deberá tener la capacidad de analizar el código fuente e identificar las vulnerabilidades, desde un ambiente de azure devops. Se aclara que, lo que se solicita es escanear plantillas de IaC, imágenes de contenedor y funciones serverless en la fase de compilación o lanzamiento del pipeline de Azure DevOps.
El punto en mención hace referencia al código fuente de las aplicaciones del SENCICO. El Contratista deberá emitir recomendaciones sobre este ámbito, siendo responsabilidad del SENCICO la remediación de código fuente de las aplicaciones.
- e) El servicio deberá tener la capacidad de visualizar (DASHBOARD) y evaluar la postura de seguridad de la nube, detectar errores de configuración, modelar y hacer cumplir activamente las políticas de los estándares de seguridad de la nube, proteger contra ataques y amenazas internas, a su vez poseer inteligencia de seguridad para la detección de intrusiones en la nube y cumplir con los requisitos normativos y las mejores prácticas.
- f) El servicio deberá poder integrarse al Cloud Service Provider en dos modos: lectura (monitoreo) y prevención/escritura (bloqueo y/o toma de acción aplicando cambios en la infraestructura cloud).
- g) El servicio deberá admitir que las notificaciones de evaluación se envíen por correo electrónico.
- h) El servicio deberá proporcionar capacidades de evaluación tanto para los recursos implementados en la nube, como para las posibles implementaciones según lo definido por las plantillas de IaC (Infraestructura as a Code: Terraform, CFT).

- i) El servicio deberá proporcionar API REST que permitan el acceso programático para crear / ver reglas y conjuntos de reglas, y también crear políticas de cumplimiento continuo.
Se precisa que lo solicitado se refiere a la disponibilidad de API's preconfiguradas propias de cada plataforma de nube.
- j) El servicio deberá proporcionar capacidades para administrar los Network Security Groups de la(s) nube(s) de manera centralizada.
- k) El servicio deberá ser capaz de ofrecer una vista gráfica de los Grupos de Seguridad (Network Security Groups) del entorno de nube(s) que muestre los activos en la(s) nube(s) y cómo están interconectados; estas vistas deberán estar organizadas para mostrar el nivel de exposición al mundo exterior como: zona Externa, zona DMZ, zona interna) y así poder identificar si los activos que están mal configurados en la red o están demasiado expuestos.
- l) El servicio deberá proporcionar la verificación y corrección de cumplimiento normativo de las mejores prácticas como: "GDPR, CIS, PCI DSS, HIPAA, NIST SP 800-190, o similares", para los servicios de nube pública y cargas de trabajo nativas de nube (máquinas virtuales, contenedores, serverless).
- m) El servicio deberá proporcionar evaluaciones de riesgo frente a marcos, modelos y estándares externos como ISO 27001:2013 y NIST.
- n) El servicio deberá evitar que se realicen cambios en los Network Security Groups y/o revertir los cambios realizados cuando está operando en modo prevención/escritura. Así mismo, el servicio deberá emitir alertas ante cambios realizados cuando esté operando en los modos: lectura y prevención/escritura.
- o) El servicio deberá proporcionar la visibilidad y recomendaciones sobre las mejores prácticas de Identity and Access Management.
- p) El servicio deberá escanear los Storages de almacenamiento en busca de configuraciones incorrectas que puedan hacer que los datos sean accesibles al público.
- q) El servicio deberá garantizar que los recursos en la nube que se ocupan de los datos en reposo estén etiquetados y cifrados según las buenas prácticas de la industria.
- r) El servicio deberá garantizar que los usuarios, grupos y roles de administración de la(s) nube(s) "no" contengan privilegios excesivamente permisivos, especialmente en roles de instancia.
- s) El servicio deberá poseer un control granular sobre usuarios, roles y acciones de usuarios de administración de la(s) nube(s), basándose en la gestión de acceso sobre el principio de privilegio mínimo, el cual entregará un acceso federado para una protección de seguridad mejorada de IAM. También será válido que la solución pueda monitorear el comportamiento de los usuarios, roles y acciones definidas en IAM
- t) El servicio deberá proveer una protección contra manipulaciones (tamper protection) de la actividad sospechosa de los usuarios de administración, con el fin de identificar cualquier actividad inusual de la red y de cualquier usuario utilizando métodos como user entity behavior analysis (UEBA) o similares
- u) El servicio deberá realizar un escaneo continuo para descubrir funciones y mostrar su postura a nivel de seguridad: cumplimiento y vulnerabilidades.
- v) El servicio deberá proporcionar detección y remediación de cargas de trabajo como: funciones y clúster de contenedores.
- w) El servicio deberá incluir análisis de código estático para funciones e imágenes de contenedor, capaces de detectar dependencias vulnerables, credenciales integradas, roles de ejecución abiertamente permisivos (para funciones).
- x) El servicio deberá admitir la integración del análisis de código estático en una canalización de CI/CD (incluidos AWS Codepipeline, Azure Devops, Jenkins, Gitlabs, CircleCI).
- y) El servicio deberá proporcionar una vista grafica de las fuentes de eventos que desencadenan la función y los servicios con los que interactúa una función, el cual ayudara a entender mejor el funcionamiento de la función.
- z) El servicio deberá incluir protecciones en tiempo de ejecución para funciones y poder detectar/bloquear inyecciones de código y comportamiento anómalo. Se aclara que, lo que se solicita es, cambios en la inmutabilidad del workload, detectando cambios en el sistema de archivos, actividad de red y actividad del proceso en ejecución.
- aa) El servicio deberá ser capaz de generar para cada función, una sugerencia de un rol específico en base a mínimos privilegios requeridos, y/o deberá verificar y reportar periódicamente los privilegios no utilizados en los roles implementados.

- bb) El servicio deberá ofrecer inteligencia avanzada de seguridad en la nube, y deberá realizar análisis de tráfico de red y brindar sugerencias de remediación o aplicar políticas de remediación automática, para una respuesta más rápida y eficiente a las amenazas de ciberseguridad más avanzadas de la Nube.
- cc) El servicio deberá proporcionar la correlación de eventos de los activos de la Nube e información de configuración con una base de inteligencia externa del mismo fabricante para detectar anomalías en la Nube.
- dd) El servicio deberá enriquecer los logs proporcionados por la Nube Pública el cual permitirá obtener una comprensión más rápida y clara de los eventos que ocurren en su nube, por ejemplo: identificar el tráfico de fuentes no deseadas o brechas en la configuración de seguridad de la red.
- ee) El servicio deberá visualizar gráficamente los flow logs de una manera intuitiva para comprender el flujo de tráfico en mi entorno e identificar el tráfico no deseado.
- ff) El servicio deberá alertar sobre cualquier actividad maliciosa potencial en el entorno de Nube que deba investigarse más a fondo y filtrar la información para resaltar el tráfico de interés.
- gg) El servicio deberá identificar el método de ataque sofisticado de escalación de privilegios de Máquinas Virtuales y/o contenedores.
- hh) El servicio deberá identificar el método común de exfiltración de datos, utilizando los nodos de salida de tráfico de tipo Tor (Anonymizer).
- ii) El servicio deberá identificar tamaños de paquetes NTP sospechosos dentro de la Nube, a su vez detectar actividad desde ubicaciones geográficas prohibidas, uso sospechoso de puertos o intentos anormales de inicio de sesión / autenticación.
- jj) El servicio debe contar con informes nativos relacionados a:
 - Reporte de inventarios
 - Alertas de alta severidad
 - Top de postura de seguridad
 - Top de inteligencia de amenazas
 - Reporte de Postura de Seguridad entregara un detalle del cumplimiento de acuerdo a los estándares soportados por la solución.

L. Servicio de Escritorios Remotos Virtuales

- a) EL CONTRATISTA deberá proveer el servicio en una modalidad de tipo PaaS (Platform-as-a-Services) o similar.
- b) EL CONTRATISTA deberá implementar un servicio de escritorios remotos virtuales basados en "Microsoft Windows 10 Professional" en modo multi-sesión o de asignación permanente, y en idioma Español Perú.
- c) EL CONTRATISTA deberá proveer licenciamiento de entornos virtuales para cuatrocientos cincuenta (450) usuarios.
- d) EL CONTRATISTA deberá integrar el servicio al directorio activo administrativo de la Entidad, para permitir el inicio de sesión con sus credenciales de red y/o con el entorno de Office 365 a través del tenant existente en Microsoft. Se precisa que la entidad cuenta con un tenant administrativo en Office 365 de tipo educativo.
- e) Los entornos virtuales deberán poder comunicarse con los distintos servidores/servicios implementados en nube(s), de acuerdo a las políticas de seguridad que determine el SENCICO.
- f) Los entornos virtuales deberán contar con software instalado y licenciamiento Microsoft Office 365 o Microsoft Office Standard, que incluya Excel, Word y PowerPoint en idioma Español Perú.
- g) El servicio deberá estar disponible bajo el siguiente esquema:

Horario	Detalle	Días	Capacidad
Principal	7am a 12m (medianoche)	Lunes a viernes	150 usuarios concurrentes
Extendido	12m (medianoche) a 7am	Lunes a viernes	20 usuarios concurrentes
Fin de Semana	24 horas	Sábados, Domingos y Feriados	20 usuarios concurrentes

- h) Cada entorno de usuario deberá contar con capacidades equivalentes a 2 cores y 4Gb de RAM.
- i) Los entornos desplegados no deberán exceder un umbral del 85% de uso de recursos de memoria RAM y/o de CPU, con el fin de garantizar un rendimiento óptimo de la sesión del usuario.
- j) EL CONTRATISTA deberá garantizar este rendimiento mediante la escalabilidad de recursos.

- k) EL CONTRATISTA deberá implementar la protección antivirus/antiransomware correspondiente a todos los entornos de usuario desplegados.
- l) EL CONTRATISTA deberá preparar los entornos en coordinación con el SENCICO, para incluir el software y configuraciones requeridas por la Entidad. EL CONTRATISTA deberá garantizar que todos los entornos sean idénticos en configuraciones y software instalado.
- m) El servicio deberá permitir el acceso mediante interfaces web o de cliente instalado en computadoras Windows, OS X y Linux, así como en dispositivos móviles de tipo Android e iOS.
- n) El servicio deberá permitir bloquear o restringir la navegación a internet por usuario y/o grupo de usuarios, en base a las políticas de seguridad del SENCICO.
- o) EL CONTRATISTA deberá garantizar la asignación virtual de las impresoras conectadas en la computadora de origen del usuario final.

M. Copias de Seguridad / Backup

- a) EL CONTRATISTA deberá proveer un servicio de backup (copias de seguridad) que incluya funcionalidades de: configurar políticas de copia de seguridad (frecuencia por hora), programación de los puntos de recuperación, configuración del periodo de conservación (diaria, semanal o mensual) y mecanismos que permitan su verificación (integridad de la información).
- b) EL CONTRATISTA deberá realizar verificaciones de la integridad de la información dos (2) veces al año para mínimo 6 instancias seleccionadas por SENCICO. Asimismo, EL CONTRATISTA deberá habilitar estos ambientes para relanzar el levantamiento de la instancia y verificar la integridad de los datos, con mecanismos que permitan garantizar que los archivos generados no presenten error en su restauración. Este proceso de verificación se considerará exitoso cuando el Contratista demuestre que el proceso de restauración de los backup ha sido satisfactorio. Se precisa que, el costo implicado de infraestructura (instancias) debe enmarcarse en los conceptos de la tabla de precios unitarios, y se pagara mensual según lo consumido.
- c) EL CONTRATISTA deberá configurar las políticas de respaldo de todos los servicios y servidores implementados en toda(s) la(s) nube(s) propuesta(s), considerando el espacio de almacenamiento suficiente para llevar a cabo los backup requeridos por SENCICO.
- d) La información deberá resguardarse en dos sitios distintos geográficamente. Es decir, el “backup principal” estará alojado en el Data Center del servicio Cloud y el “backup secundario” en un lugar geográficamente diferente.
- e) El servicio de backup deberá permitir realizar backups y restauración de datos en las siguientes formas:
 - Backup y Restauración de servidor y/o servicio completo, en el mismo destino o destino diferente.
 - Backup y Restauración a nivel de archivos de cada uno de los servidores y servicios desplegados en nube, en el mismo destino o destino diferente.
 - Backup y Restauración a nivel de base de datos de cada uno de los “servicios de bases de datos”, en el mismo destino o destino diferente.
- f) Los backups se deberá ejecutar de la siguiente manera, para lo cual el CONTRATISTA deberá considerar el espacio necesario:

Backup diario (para bases de datos)	Backup incremental de lunes a domingo, en horarios: 12m, 6am, 1pm y 7pm.
Backup diario (resto de servicios)	Backup incremental de lunes a domingo, a las 12m (medianoche).
Backup semanal	Backup ejecutado los domingos a las 12m (medianoche).
Backup mensual	Backup ejecutado el último día calendario del mes, a las 12m (medianoche).
Backup anual	Backup ejecutado el último día calendario del año, a las 12m (medianoche).

- g) La retención de backups deberá configurarse de la siguiente forma:

Backup diario	Retención de los últimos 07 días calendario
Backup semanal	Retención de las últimas 04 semanas
Backup mensual	Retención de los últimos 12 meses
Backup anual	Retención de los últimos 03 años

- h) El servicio de backups deberá estar operativo durante todo el plazo del contrato, y cubrir un incremento anual del 10% en el número de servidores/servicios cubiertos por el servicio.
- i) Las características y capacidades del almacenamiento en la nube para las copias de seguridad y respaldo de información estimado deberán ser la siguiente:

Almacenamiento de baja latencia	<ul style="list-style-type: none">• Debe admitir SSL para datos en tránsito y cifrado para datos en reposo• Debe permitir el versionado de los objetos almacenados.
Almacenamiento de consulta de datos poco frecuentes	<ul style="list-style-type: none">• Debe admitir SSL para datos en tránsito y cifrado para datos en reposo• Debe permitir el versionado de los objetos almacenados

- j) Se precisa que el “Almacenamiento de baja latencia” estará destinado a almacenar los backup rutinarios, y respecto al “Almacenamiento de consulta de datos poco frecuentes” estará destinado a los datos históricos. EL CONTRATISTA deberá configurar el servicio de backup para que los datos pasen de manera automática entre tipos de almacenamiento de acuerdo a lo siguiente:

Almacenamiento de baja latencia	<ul style="list-style-type: none">• Backups diarios• Backups semanales
Almacenamiento de consulta de datos poco frecuentes	<ul style="list-style-type: none">• Backups mensuales• Backups anuales

- k) EL CONTRATISTA deberá permitir al SENCICO la descarga y restauración de todos los datos almacenados en los sistemas de backups, hacia las instalaciones locales del SENCICO ubicadas en Lima, o a otras instalaciones que el SENCICO determine. EL CONTRATISTA deberá provisionar la infraestructura y el licenciamiento necesarios para los casos de almacenamiento temporal de datos en tránsito.

N. Disaster Recovery

- a) EL CONTRATISTA deberá implementar un servicio de Disaster Recovery, que garantice la continuidad de todos los servicios implementados en nube(s), implementando una arquitectura similar a la principal en centro(s) de datos de respaldo, que permita continuar operaciones ante cualquier incidente que genere indisponibilidad del entorno principal.
- b) EL CONTRATISTA deberá garantizar que el centro de datos de respaldo se encuentre a no menos de 700 (setecientos) kilómetros de distancia del centro de datos principal, o podrá alojarse en un continente distinto.
- c) EL CONTRATISTA debe garantizar que los dominios definidos por la(s) nube(s), sean dominios de disponibilidad en uno o más datacenters ubicados en una región o en múltiples regiones, se encuentren aislados unos de otros, cuenten con tolerancia a fallos, y que ante una falla de un dominio de disponibilidad no afecte a (los) otro(s) dominio(s).
- d) EL CONTRATISTA deberá elaborar un plan de Disaster Recovery, que deberá probarse dentro de los seis meses de iniciado el servicio contratado y como mínimo una vez cada año.
- e) EL CONTRATISTA deberá implementar el servicio de Disaster Recovery bajo las siguientes consideraciones para el RPO (Objetivo de Punto de Recuperación) y RTO (Objetivo de Tiempo de Recuperación):

Bases de Datos	RPO	Máximo 07 horas
	RTO	Máximo 04 horas
Resto del Entorno de Nube	RPO	Máximo 12 horas
	RTO	Máximo 07 horas

O. Monitoreo de Servicios

El Contratista deberá contar con una o más plataformas de monitoreo basados en nube, de acuerdo a lo siguiente:

- a) Las herramientas y plataformas deberán realizar un monitoreo en modalidad 24x7x365.
- b) El alcance del monitoreo es requerido para todos los servicios, servidores, bases de datos y aplicaciones web, de la Tabla N°1 y los que sean implementados por el Contratista en los entornos de nube.
- c) Se deberá monitorear la disponibilidad de los servicios implementados a nivel de puertos, protocolos y servicios instalados.

- d) Se deberá registrar la estadística de utilización de ancho de banda de todos los servicios, servidores y redes implementadas en la(s) nube(s), en el consumo entre servidores, entre servicios, entre nubes y hacia/desde internet.
- e) Se deberá monitorear las tareas de respaldo de la información que ha sido almacenado durante el mes.
- f) El servicio de monitoreo deberá almacenar información estadística de los últimos 12 meses.
- g) Todos los servicios monitoreados deberán contar con umbrales de alerta y notificación por correo electrónico u otros medios como slack, telegram o similares.
- h) Performance de Servidores y Servicios**
 - Se deberá registrar la estadística de monitoreo de los componentes de servicios y servidores: uso de CPU, memoria, almacenamiento, tasas de lectura y escritura en disco.
 - Se deberá monitorear el estado de procesos, servicios y aplicaciones implementados, como servicios web, apache, nginx, IIS, glassfish, y otros servicios que se identifiquen durante la implementación.
 - La solución podrá ser provista con soluciones nativas de nube, soluciones disponibles en marketplace's de nube o soluciones de terceros.
- i) Performance de Bases de Datos**
 - Se deberá contar con estadísticas del rendimiento de las bases de datos, con el fin de evaluar la carga de trabajo, detectar problemas de rendimiento e identificar instrucciones SQL que causan sobrecarga.
 - La solución podrá ser provista con soluciones nativas de nube, soluciones disponibles en marketplace's de nube o soluciones de terceros
- j) Performance de Aplicaciones Web**
 - Se deberá contar con un monitoreo de aplicaciones de tipo APM (Application Performance Monitoring), que permita realizar un seguimiento al comportamiento de las aplicaciones, medir el impacto en los usuarios finales en tiempo real
 - Se deberá contar con rastreo de errores y excepciones en la arquitectura de las aplicaciones y obtener visibilidad completa del rendimiento de cada aplicación
 - Se deberá contar con métricas de performance por aplicación.
 - Deberá soportar aplicaciones de tipo .Net, .Net Core 3, PHP 7.2, NodeJS 10.19, Glassfish, Java 8.2, .Net Framework 3.5,
 - La solución podrá ser provista con soluciones nativas de nube, soluciones disponibles en marketplace's de nube o soluciones de terceros.
- k) Analítica de eventos**
 - EL CONTRATISTA deberá implementar un servicio de recopilación y normalización de eventos (logs), que incluya conectores para reunir los registros de varias fuentes, analizar los datos y mostrarlos en un formato de lectura común.
 - Se deberá recoger información de los eventos en todos los servicios, servidores y componentes implementados en la(s) nube(s), incluyendo a los eventos de los servicios de copia de seguridad.
 - Así mismo, el servicio debe registrar los eventos (logs) generados sobre cualquier alteración (alta, baja, modificación) de los componentes y configuraciones habilitados en la plataforma de nube(s), como supervisión de auditoría a las operaciones de usuarios administradores.
 - La solución podrá ser provista con soluciones nativas de nube, soluciones disponibles en marketplace's de nube o soluciones de terceros.

P. Entornos de Desarrollo / Calidad

El SENCICO requiere la implementación de entornos de "Desarrollo / Calidad" para los procesos y ciclos de desarrollo y prueba de soluciones de software generados por la Entidad.

a) Aplicaciones web

EL CONTRATISTA deberá implementar lo siguiente, de forma adicional a lo descrito en la Tabla Nro. 01:

- Se deberá proveer e implementar entornos para aplicaciones web, basados en plataformas administradas de tipo PaaS (Platform-as-a-Services) o contenedores.

- EL CONTRATISTA deberá provisionar los entornos necesarios para implementar cada una de las siguientes aplicaciones web:

Nro	Servicio	Plataforma	Tipo
1	APP_DEV_01	Windows	Net Core / .Net
2	APP_DEV_02	Windows	Net Core / .Net
3	APP_TST_01	Windows	Net Core / .Net
4	APP_TST_02	Windows	Net Core / .Net

Se precisa que lo descrito en la tabla predecesora, corresponde a entornos adicionales a lo indicado en la Tabla Nro 1.

- EL CONTRATISTA deberá proveer e implementar balanceadores webs de tipo aplicaciones, para cada una de las aplicaciones web desplegadas.
- EL CONTRATISTA deberá provisionar certificados de seguridad SSL para cada una de las aplicaciones web desplegadas en plataformas.
- EL CONTRATISTA deberá configurar cada plataforma para que pueda conectarse a los servicios de bases de datos Oracle, Microsoft SQL y MySQL, y a los servicios de Active Directory.
- EL CONTRATISTA deberá utilizar versiones de sistema operativo que no cuenten con “EOL” (End of Life) o “EOS” (End of Support) declarado por los fabricantes durante el plazo de contratación. En caso de que exista una declaración oficial con fechas programadas dentro del plazo del contrato, EL CONTRATISTA deberá realizar el proceso de migración y actualización de los sistemas operativos a las versiones soportadas por los fabricantes.
- El Contratista podrá utilizar las mismas características de los servidores clasificados como “Aplicaciones web” descritas en la sección “B. Habilitación de ambientes cloud. Tabla Nro 1”.

b) Bases de Datos

EL CONTRATISTA deberá considerar lo siguiente durante la implementación de servidores asociados a los servicios de bases de datos (Desarrollo / Calidad):

- EL CONTRATISTA deberá proveer servicios administrados y/o plataformas administradas para entornos de bases de datos Oracle y Microsoft SQL, contemplando la gestión del sistema operativo, gestión del motor de base de datos, acciones de monitoreo, mantenimiento y optimización.
- EL CONTRATISTA deberá proveer el licenciamiento necesario para cada una de las soluciones de base de datos, de acuerdo a su levantamiento de información.
- EL CONTRATISTA deberá contar con personal especialista, para implementar los entornos de base de datos de acuerdo a las buenas prácticas de cada fabricante.
- EL CONTRATISTA deberá provisionar los siguientes entornos:

Nro	Servidor	Servicio	Versión
1	SERVIDOR 52	Oracle Dev	Oracle SE2 19c
2	SERVIDOR 53	Microsoft SQL Dev/Test	MS-SQL 2016
3	SERVIDOR 54	Oracle Test	Oracle SE2 19c
4	SERVIDOR NUEVO	MariaDB Dev/Test	MariaDB 10.4

Se precisa que los ítems “SERVIDOR 52”, “SERVIDOR 53” y “SERVIDOR 54” se corresponden con la Tabla Nro 1, en donde indica las capacidades requeridas. Así mismo, las capacidades de almacenamiento se describen en la “sección G. Almacenamiento, punto b”).

Se precisa que el ítem “SERVIDOR NUEVO” corresponde a un servicio adicional a lo descrito en la Tabla Nro 1, por lo que actualmente no existe. Así mismo, se precisa que las características requeridas para este servidor son: 2 vCPU, 4Gb RAM, disco 36Gb.

- EL CONTRATISTA deberá implementar conexiones de “Linked-Server” entre las bases de datos Microsoft SQL y Oracle.
- EL CONTRATISTA deberá verificar que las versiones de los motores de bases de datos implementados no cuenten con “EOL” (End of Life) o “EOS” (End of Support) declarado por los fabricantes y/o nube(s) durante el plazo de contratación. En caso de que exista una declaración oficial con fechas programadas dentro del plazo del contrato, EL CONTRATISTA deberá realizar el proceso de migración y actualización de los motores a las versiones soportadas por los fabricantes.

- EL CONTRATISTA deberá generar y automatizar un flujo de transferencia de información para la actualización de datos en las bases de datos de “Desarrollo” y “Calidad/TST” con información del entorno “Producción”. El SENCICO realizará solicitudes continuas de actualización de información para el conjunto de base de datos y/o para una base de datos específica.

c) Plataforma de Aula Virtual

EL CONTRATISTA deberá considerar lo siguiente durante la implementación del servidor asociado a la plataforma de Aula Virtual:

- EL CONTRATISTA deberá provisionar los siguientes entornos de infraestructura:

Nro	Servidor	Servicio	Plataforma
1	SERVIDOR NUEVO	Aula Virtual	Moodle

Se precisa que lo descrito en la tabla predecesora, corresponde a un entorno adicional a lo indicado en la Tabla Nro 1.

- EL CONTRATISTA deberá provisionar el servidor con las siguientes capacidades:

CPU	RAM
2	8

- Se precisa que el almacenamiento a provisionar deberá ser en tamaño idéntico al “Servidor Nro 32”.
- EL CONTRATISTA deberá generar y automatizar un flujo de clonación desde el “SERVIDOR 32” hacia el “SERVIDOR NUEVO” requerido, con el fin mantener actualizado el entorno de desarrollo de la plataforma de aula virtual. El SENCICO realizará solicitudes continuas de clonación para esta plataforma.
- EL CONTRATISTA deberá realizar el proceso de clonación de la base de datos relacionada al “SERVIDOR 32”, ubicada en el “Servicio de Base de Datos”, con el fin de permitir el acceso del entorno de desarrollo requerido.

d) Plataformas de desarrollo

- EL CONTRATISTA deberá proveer una plataforma que proporcione gestión al ciclo de vida de las aplicaciones, mediante el control de versiones con repositorios GIT ilimitados, generación de informes, gestión de requisitos, gestión de proyectos, gestión de Test Plans, compilaciones automatizadas, y conexión a múltiples IDE, que soporte principalmente tecnologías de desarrollo Microsoft.
- Se precisa que el SENCICO cuenta con la plataforma Microsoft Azure DevOps. EL CONTRATISTA deberá proveer una plataforma equivalente/similar, y realizar el proceso de transferencia de datos y configuraciones al nuevo entorno.
- EL CONTRATISTA deberá proveer licencias de uso para un mínimo de 20 usuarios simultáneos. Así mismo, deberá realizar las configuraciones necesarias para automatizar los flujos de integración/distribución continua (CI/CD) hacia los entornos Desarrollo, Calidad/TST y Producción del “servicio de aplicaciones web”.
- Adicionalmente, EL CONTRATISTA deberá proveer entornos de “escritorio remoto virtual” de asignación permanente (no multisesión) para un mínimo de 20 usuarios del área de Desarrollo. Estos entornos deberán provisionarse y licenciarse con “Microsoft Windows 10 Pro” y “Microsoft Office 365 o Professional”, contar con IDE’s de desarrollo y conexión a bases de datos. EL CONTRATISTA podrá proveer una interfaz web en donde el personal de desarrollo pueda encender/apagar su “escritorio remoto virtual” a demanda. Así mismo, deberán tener una capacidad equivalente a 04 cores, 08Gb de RAM y 100Gb de espacio en disco disponible para el usuario.

Q. Migración de información

EL CONTRATISTA deberá tener en cuenta las siguientes consideraciones para el traslado de la información hacia la(s) nube(s) que se implemente:

- a) EL CONTRATISTA deberá migrar sin excepción, todos los datos almacenados en los servidores, aplicaciones, servicios y base de datos del SENCICO descritos en la Tabla Nro 01, hacia la nueva plataforma de nube(s) ofertada(s).
- b) EL CONTRATISTA deberá proponer estrategias de migración de información a nube para cada uno de los servidores y servicios, basadas en rehosting, replatform, repurchasing, refactoring, rearchitecting, retire, retain o estrategias similares que garanticen la consistencia de la información migrada.

- c) EL CONTRATISTA deberá actualizar las versiones de sistema operativo que cuenten con “EOL” (End of Life) o “EOS” (End of Support) declarado por los fabricantes. EL CONTRATISTA deberá realizar el proceso de migración y actualización de los sistemas operativos a las versiones soportadas por los fabricantes durante la fase de implementación y migración.

d) Bases de Datos

EL CONTRATISTA deberá contemplar adicionalmente las siguientes precisiones respecto a la migración de información de Bases de Datos:

- EL CONTRATISTA deberá contar con personal experto en los productos y versiones de base de datos solicitados en el presente TDR, que garantice una correcta migración de datos hacia el nuevo entorno.
- EL CONTRATISTA deberá asegurar que se migren los datos, instancias, roles y permisos, y configuraciones de bases de datos al nuevo entorno.
- EL CONTRATISTA deberá migrar todas las bases de datos productivas sin excepción hacia el nuevo entorno:

Ambiente	Servidor	Plataforma	Bases de Datos	GB Total
Producción	SERVIDOR 1	Oracle	26	1500
Producción	SERVIDOR 2	MS-SQL	10	580

- Se precisa que los entornos de base de datos Desarrollo y Calidad/TST, deberán iniciar desde una copia del nuevo ambiente Producción implementado.
- EL CONTRATISTA deberá realizar el desacoplamiento de bases de datos locales de los siguientes servidores, y alojarlos en el entorno productivo del “Servicio de Bases de Datos”, para lo cual deberá efectuar la migración correspondiente:

Nro	Servidor	Plataforma Actual	Bases de Datos	GB Total
1	SERVIDOR 32	MariaDB	1	30
2	SERVIDOR 43	MySQL	1	1
3	SERVIDOR 51	MariaDB	1	5

El SENCICO brindará el apoyo con la información de configuración necesarias para que EL CONTRATISTA realice la migración respectiva.

e) Aplicaciones Web

EL CONTRATISTA deberá contemplar adicionalmente las siguientes precisiones respecto a la migración de los sistemas relacionados al “Servicio de Aplicaciones Web”:

- El SENCICO proveerá los empaquetados/compilados de las aplicaciones web destinadas a este servicio.
- EL CONTRATISTA será responsable de desplegar, implementar y configurar los empaquetados/compilados en los nuevos entornos y asegurar la operatividad de las aplicaciones, comunicación hacia las bases de datos y hacia el “webservice de almacenamiento”, para lo cual el SENCICO brindará el apoyo y proveerá los detalles técnicos que EL CONTRATISTA requiera.
- Todo ajuste que se requiera en las aplicaciones será ejecutado por SENCICO.

f) Servicios Conexos

EL CONTRATISTA deberá realizar la migración de información del resto de servidores conexos, manteniendo en todo momento las configuraciones e integridad de los datos almacenados en ellos.

Nro	ID	Zona
1	SERVIDOR 30	Produccion
2	SERVIDOR 31	Produccion
3	SERVIDOR 33	Produccion
4	SERVIDOR 34	Produccion
5	SERVIDOR 35	Produccion
6	SERVIDOR 36	Produccion
7	SERVIDOR 37	Produccion
8	SERVIDOR 39	Produccion
9	SERVIDOR 40	Produccion
10	SERVIDOR 41	Produccion
11	SERVIDOR 42	Produccion
12	SERVIDOR 43	Produccion
13	SERVIDOR 44	Produccion
14	SERVIDOR 45	Produccion

15	SERVIDOR 46	Produccion
16	SERVIDOR 47	Produccion
17	SERVIDOR 48	Produccion
18	SERVIDOR 49	Produccion
19	SERVIDOR 50	Produccion
20	SERVIDOR 51	Produccion

R. Protocolo de Pruebas Funcionales

- EL CONTRATISTA, dentro del plazo de implementación, deberá ejecutar un protocolo de pruebas para cada uno de los servicios, servidores y aplicaciones.
- SENCICO brindara un inventario de pruebas a realizar referente a los servicios, servidores y aplicaciones desarrolladas por la Entidad.
- EL CONTRATISTA deberá asegurarse, mediante reuniones de trabajo, la operatividad de las funcionalidades descritas en el inventario de pruebas, así como complementarlas con pruebas adicionales que identifique durante las reuniones de trabajo.
- El protocolo de pruebas será aplicado durante la etapa de “Pre-Producción” y “Pase a Producción”, para lo cual no deberá contar con observaciones en su ejecución, como requisito para la conformidad del servicio de implementación.

S. Pruebas de Estrés

- EL CONTRATISTA, dentro del plazo de implementación, deberá ejecutar un protocolo de pruebas de estrés para cada una de las aplicaciones desplegadas. Se aclara que, lo que se busca medir la capacidad de la infraestructura, los tiempos de respuesta de las aplicaciones correspondiente a un número incremental de usuarios y el número límite de usuarios antes de la denegación de servicio de la plataforma.
El Contratista deberá considerar la cantidad de ciclos necesarios para garantizar el correcto funcionamiento de las aplicaciones; en las condiciones de mayor carga, alta concurrencia y el número límite de usuarios antes de la denegación de servicio de la plataforma.
El Contratista deberá considerar la cantidad de escenarios necesarios para garantizar el correcto funcionamiento de las aplicaciones, en las condiciones de mayor carga, alta concurrencia y el número límite de usuarios antes de la denegación de servicio de la plataforma.
Las pruebas de estrés son pruebas diferentes al protocolo de prueba funcionales.
- EL CONTRATISTA deberá emitir un informe de rendimiento por cada aplicación sujeta a estrés, describiendo el alcance máximo en concurrencia de usuarios.
- Así mismo, EL CONTRATISTA deberá incluir, durante el periodo de servicio de cloud computing, 75 pruebas de estrés por año (totalizando 225 pruebas), las cuales serán acumulables durante todo el servicio, para las aplicaciones de los ambientes “Producción, Calidad y Desarrollo”.
El Contratista deberá considerar la cantidad de ciclos necesarios para garantizar el correcto funcionamiento de las aplicaciones; en las condiciones de mayor carga, alta concurrencia y el número límite de usuarios antes de la denegación de servicio de la plataforma.

El Contratista deberá considerar la cantidad de escenarios necesarios para garantizar el correcto funcionamiento de las aplicaciones, en las condiciones de mayor carga, alta concurrencia y el número límite de usuarios antes de la denegación de servicio de la plataforma.

T. Entorno de Pre-Producción

- El Contratista y la(s) nube(s) deberá(n) brindar un entorno de pre-producción en su plataforma, antes de su pase a operación y producción, de mínimo quince (15) días calendarios, el mismo que deberá estar dentro del plazo de implementación del servicio, con el fin de verificar y modelar la operatividad, disponibilidad, integridad, seguridad y funcionalidad de los servicios, aplicaciones, sistemas y bases de datos del SENCICO.
- El entorno de pre-producción deberá estar disponibles con todos los servidores, servicios y componentes de nube requeridos, así como la migración de datos solicitados.
- En el entorno de pre-producción deberá estar implementado el servicio de copia de seguridad.

- d) La disponibilidad del entorno pre-producción estará sujeta a lo descrito en la sección “Disponibilidad del Servicio” del “Servicio de Solución Corporativa Cloud Computing”, en la categoría “Producción”.
- e) Se aceptará que el entorno de pre-producción pueda pasar a modo “Producción”. EL CONTRATISTA es el responsable de migrar las aplicaciones y configuraciones del entorno de Pre-producción a la modalidad de Producción con toda la información actualizada.

U. Pase a Producción

- a) EL CONTRATISTA deberá garantizar, según su metodología de implementación, que la migración de los servicios sea transparente para los usuarios finales.
- b) EL CONTRATISTA deberá elaborar un Plan de Pase a Producción, indicando el detalle de actividades, responsables, franjas horarias, hitos de avance y cumplimiento, así como el detalle de las actividades de rollback.
- c) EL CONTRATISTA deberá realizar el “Pase a Producción” en una franja horaria que no impacte la continuidad de los servicios del SENCICO, para lo cual el SENCICO otorgará una ventana de migración con una franja horaria adecuada para las actividades.
- d) El SENCICO requiere que EL CONTRATISTA realice como mínimo una (01) simulación de la ejecución del Plan de Pase a Producción, con el fin de verificar la correcta migración de los servicios.

V. Servicio de Solución Corporativa Cloud Computing

EL CONTRATISTA deberá brindar el servicio de acuerdo a lo siguiente:

- a) EL CONTRATISTA se encargará de mantener en operación el Servicio de Cloud Computing implementado con alcance a todos los servicios y componentes desplegados: servidores, servicios, bases de datos, plataformas PaaS y/o IaaS y/o SaaS, integraciones, nubes, software y/o soluciones nativas y/o de terceros.
- b) EL CONTRATISTA otorgará treinta (30) días calendario para la desactivación del servicio, luego de finalizado el plazo de servicio de solución corporativa Cloud Computing.
- c) EL CONTRATISTA brindará acceso al portal o portales de administración de la solución de nube(s), utilizando un mecanismo de autenticación seguro. El SENCICO podrá ingresar al portal o portales para visualizar el estado del servicio, si se requiere realizar cambios sobre la infraestructura deberán realizarse en coordinación con el contratista, siendo este último el responsable de la ejecución de los cambios requeridos.
- d) EL CONTRATISTA brindará acceso al SENCICO a todos los portales y/o consolas de administración de los servicios implementados.

W. Capacidades de Cómputo a Demanda

- a) EL CONTRATISTA y la(s) nube(s) deberán contar con esquemas y/o plantillas prediseñadas para desplegar capacidades de cómputo de acuerdo a la necesidad del SENCICO.
- b) Las capacidades de cómputo podrán reducirse en horarios de baja demanda.
- c) Las capacidades de cómputo podrán aumentarse de ser necesario, de manera que los usuarios no se vean afectados y el SENCICO pueda optimizar los recursos contratados.
- d) Se precisa que EL CONTRATISTA podrá aumentar, reducir o detener las capacidades de cómputo previa autorización escrita (por correo electrónico) del personal responsable de administrar el servicio, asignado por el Departamento de Informática del SENCICO.
- e) Se precisa que, los ítems b) y c), se enmarcan en la sección “W. Capacidades de cómputo a demanda”, que se corresponde con la sección “Z. Sistema de Contratación y modalidad de facturación, Tabla Nro. 2 – Precios Unitarios”, por lo que la ampliación y/o reducción de capacidades deberá reflejarse en la facturación mensual por consumo (renta variable).
- f) EL CONTRATISTA podrá realizar reservas anticipadas de capacidades de cómputo en base a información estadística histórica del comportamiento de los servidores y servicios; sin embargo, deberá facilitar al SENCICO la ampliación o reducción de capacidades según necesidad. Se precisa que, lo solicitado le permite al Contratista, de considerarlo, aplicar las reservas anticipadas en su estrategia de optimización de costos. Así mismo, este ítem se enmarca en la sección “W. Capacidades de cómputo a demanda”, que se corresponde con la sección “Z. Sistema de

Contratación y modalidad de facturación, Tabla Nro. 2 – Precios Unitarios”, por lo que los costos asociados deben reflejarse en los conceptos de facturación mensual por consumo (renta variable).

- g) Se precisa que personal del SENCICO podrá solicitar aumentar, reducir o detener las capacidades de cómputo mediante una solicitud de atención de requerimiento al área de soporte del Contratista, por correo electrónico o a través del portal de atención.

X. Disponibilidad del Servicio

El CONTRATISTA deberá asegurar la disponibilidad de los servicios de cloud computing implementados en la plataforma de nube ofertada. La disponibilidad total mensual de la infraestructura base, servidores y servicios deberá establecerse como mínimos bajo los siguientes parámetros:

Ambiente	Entorno	Disponibilidad Mensual
Producción	Servicios de Bases de Datos	99.95%
Producción	Servicios de Seguridad Perimetral y Protección de Bases de Datos	99.99%
Producción	Resto de Servicios y Servidores	99.95%
Producción	Copias de Seguridad	99.90%
Desarrollo	Servicios Bases de Datos	99.90%
Desarrollo	Resto de Servicios y Servidores	99.90%
Desarrollo	Copias de Seguridad	99.90%
Calidad	Servicios Bases de Datos	99.90%
Calidad	Resto de Servicios y Servidores	99.90%
Calidad	Copias de Seguridad	99.90%

Y. Optimización de Recursos

- a) EL CONTRATISTA deberá realizar un análisis mensual del rendimiento de los servidores y servicios implementados, con el fin de informar los consumos reales y las recomendaciones de ajuste a las capacidades asignadas.
- b) Las capacidades de cómputo podrán aumentarse, reducirse o reasignarse de forma temporal o permanente, para atender la demanda del servicio, con previa autorización del SENCICO.

Z. Sistema de Contratación y modalidad de facturación

El servicio de solución corporativa Cloud Computing, deberá contar con dos sistemas de contratación, suma alzada y precios unitarios, la cual se detalla de la siguiente manera:

- a) Contratación por precios unitarios, en este caso la facturación mensual será de acuerdo al consumo de la cantidades o unidad de medidas definidas por cada concepto del servicio Cloud Computing, para lo cual se ha establecido una tabla de precios unitarios, para todos los servicios nativos estándar de nube, identificados de acuerdo al alcance del presente TDR.

Se precisa que para efectos de cotización y/u oferta, se ha puesto cantidades referenciales, las cuales son mensuales, por lo que los precios unitarios de cada concepto de los servicios nativos estándar de nube, deberá presentarse a la presentación de la oferta.

TABLA N°02 - PRECIOS UNITARIOS

Tipo Contratación	Concepto	*Cantidad x Periodo Mensual	Unidad de Medida
Precios Unitarios	BD Tipo 1 (Oracle) + Soporte Nativo de Nube	730	Hora
Precios Unitarios	BD Tipo 2 (Oracle) + Soporte Nativo de Nube	1,460	Hora
Precios Unitarios	BD Tipo 3 (MS-SQL) + Soporte Nativo de Nube	730	Hora
Precios Unitarios	BD Tipo 4 (MS-SQL) + Soporte Nativo de Nube	730	Hora
Precios Unitarios	Web Tipo 1 + Soporte Nativo de Nube	18,250	Hora
Precios Unitarios	Servidor Tipo 1 + Soporte Nativo de Nube	2,190	Hora
Precios Unitarios	Servidor Tipo 2 + Soporte Nativo de Nube	730	Hora



Precios Unitarios	Servidor Tipo 3 + Soporte Nativo de Nube	2,920	Hora
Precios Unitarios	Servidor Tipo 4 + Soporte Nativo de Nube	1,460	Hora
Precios Unitarios	Servidor Tipo 5 + Soporte Nativo de Nube	6,570	Hora
Precios Unitarios	Servidor Tipo 6 + Soporte Nativo de Nube	4,380	Hora
Precios Unitarios	Servidor Tipo 7 + Soporte Nativo de Nube	730	Hora
Precios Unitarios	Servidor Tipo 8 + Soporte Nativo de Nube	730	Hora
Precios Unitarios	Balanceador Web de Aplicaciones + Soporte Nativo de Nube	18,250	Hora
Precios Unitarios	BD Tipo 5 (MariaDB) + Soporte Nativo de Nube	730	Hora
Precios Unitarios	Licenciamiento Oracle	3	Unidad
Precios Unitarios	Licenciamiento Microsoft SQL	2	Unidad
Precios Unitarios	Servidor API Storage + Soporte Nativo de Nube	730	Hora
Precios Unitarios	Servicio SFTP + Soporte Nativo de Nube	730	Hora
Precios Unitarios	Transferencia de Datos SFTP + Soporte Nativo de Nube	5	GB
Precios Unitarios	Servicio SMTP + Soporte Nativo de Nube	12,000	Mensajes
Precios Unitarios	Transferencia de Datos SMTP + Soporte Nativo de Nube	1	GB
Precios Unitarios	Almacenamiento estándar + Soporte Nativo de Nube	17,292	GB
Precios Unitarios	Almacenamiento para BD + Soporte Nativo de Nube	2,080	GB
Precios Unitarios	Conexión Site-to-Site VPN o similar + Soporte Nativo de Nube	730	Hora
Precios Unitarios	Transferencia de Datos (Internet) + Soporte Nativo de Nube	10,000	GB
Precios Unitarios	IP pública + Soporte Nativo de Nube	31	IP
Precios Unitarios	Proteccion de Base de Datos	39	Base de Datos
Precios Unitarios	Certificado nativo de nube + Soporte Nativo de Nube	25	Unidad
Precios Unitarios	Certificado de CA externa	14	Unidad
Precios Unitarios	Licenciamiento Antivirus/Antirransomware	36	Unidad
Precios Unitarios	Licenciamiento de Escritorios Remotos	450	Usuario
Precios Unitarios	Servicio de Escritorios Remotos + Soporte Nativo de Nube	399	Hora
Precios Unitarios	Almacenamiento de baja latencia + Soporte Nativo de Nube	19,372	GB
Precios Unitarios	Almacenamiento de consultas poco frecuentes + Soporte Nativo de Nube	9,686	GB
Precios Unitarios	Disaster Recovery + Soporte Nativo de Nube	62	Servidores/ Servicios
Precios Unitarios	Performance de Servidores y Servicios	62	Servidores/ Servicios
Precios Unitarios	Performance de Bases de Datos	39	Base de Datos
Precios Unitarios	Performance de Aplicaciones Web	30	Aplicaciones
Precios Unitarios	Análítica de eventos	62	Servidores/ Servicios
Precios Unitarios	BD Tipo 6 (MariaDB) + Soporte Nativo de Nube	730	Hora
Precios Unitarios	Plataforma de desarrollo	20	Usuario
Precios Unitarios	Licenciamiento de Escritorios Remotos Desarrollo	20	Usuario
Precios Unitarios	Servicio de Escritorios Remotos Desarrollo + Soporte Nativo de Nube	1,600	Hora

**Este valor es referencial para la cotización y/u oferta, dado que la facturación mensual, deberá ser por lo consumido mensual, en cantidad o unidad de medida de cada concepto.*

***Se precisa que el concepto de “soporte nativo de nube”, se refiere al soporte brindado directamente por el fabricante de nube (ejm: AWS Support Plan, Azure Support Plan).*

- b) Contratación por suma alzada, en este caso la facturación es fija mensual, para lo cual se ha establecido una tabla de conceptos fijos mensual, de aquellos servicios, software y/o soluciones que no son directamente nativos de nube, de acuerdo al alcance a lo solicitado en los TDR. El pago se efectuará de acuerdo a los precios fijos mensuales definidos en la Oferta del Contratista.

Todo el alcance del servicio descrito en el presente TDR, que no se haya podido listar como conceptos dentro de la Tabla N°02 de Precios unitarios, deben estar incluidos en la Tabla N°03 de precios fijos; para lo cual el Contratista, debe considerar todo lo necesario, para brindar el servicio solicitado en el presente TDR, como licencias, herramientas, recursos, etc., con el fin que el Servicio de solución corporativa Cloud Computing, se preste de acuerdo al alcance del presente TDR.

La tabla de precios fijos mensual de los servicios, deberá presentarse a la presentación de la oferta.

TABLA N°03 – PRECIOS FIJOS

Tipo Contratación	Concepto	Cantidad x Período Mensual	Unidad de Medida
Suma alzada	DNS Publico + Soporte Nativo de Nube	2	Dominio
Suma alzada	Protección de Datos	1	Servicio
Suma alzada	Protección Perimetral / AntiDDOS	1	Servicio
Suma alzada	Protección de Aplicaciones Web / WAF	1	Servicio
Suma alzada	Evaluación continua de Vulnerabilidades	1	Servicio
Suma alzada	Postura de Seguridad	1	Servicio
Suma alzada	Licenciamiento de Copia de Seguridad	1	Servicio
Suma alzada	Pruebas de Estrés	1*	Servicio

*Lo descrito corresponde a un paquete de 75 horas anuales y 225 horas por todo el periodo del servicio. Para fines de presentación de cotización, el Postor puede dividir el precio de 01 año entre 12 meses, para hallar el precio fijo mensual o según corresponda.

- c) En caso se solicite requerimientos adicionales, que este fuera de la lista de conceptos de la Tabla N°02, este será tramitado por medio de una Adenda al Contrato.
- d) En caso se solicite requerimientos adicionales, que este fuera de la lista de los conceptos y cantidades de los conceptos de la Tabla N°03, este será tramitado por medio de una Adenda al Contrato.
- e) EL CONTRATISTA deberá proveer una plataforma de contabilización de la facturación para los servicios nativos de nube, en donde se visualice la facturación diaria y acumulada detallada por cada servicio nativo de nube(s). La información representada deberá mantenerse actualizada con un desfase máximo de 48 horas.
- f) EL CONTRATISTA deberá permitir al SENCICO el acceso a la plataforma de facturación para la visualización de información.
- g) EL CONTRATISTA deberá aplicar etiquetas a todos los recursos nativos de nube, con el fin de agruparlos e identificarlos en la facturación mensual.

7. Plan de Trabajo

Dentro de los quince (15) días calendarios siguientes de suscrito el contrato, El CONTRATISTA presentará el Plan de Trabajo con toda la información necesaria que corresponde a la implementación y migración del servicio. El cual deberá ser presentado por mesa de partes en formato digital o impreso. El Plan de Trabajo incluirá:

- Memoria descriptiva de la implementación.
- Metodología para la migración de los datos y servicios.
- Propuesta de la mejor arquitectura de la infraestructura tecnológica Cloud Computing que garantice la disponibilidad, integridad, seguridad y funcionalidad de los servicios, aplicaciones, sistemas y bases de datos, incluyendo diagramas, documentos y anexos.

- Cronograma de actividades, fecha de inicio y fin, restricciones, hitos, predecesoras, etc.– Formato Project.
- Documento de configuración de entornos, que deberá incluir:
 - Características técnicas de los elementos habilitados en la plataforma “Cloud Computing” y configuraciones realizadas en los ambientes.
 - Características de la región y ubicación geográfica donde se habilitarán los servicios.
- Plan de Disaster Recovery
- Procedimiento para la ejecución y almacenamiento de respaldos.
- Documento de medidas para la protección de datos en tránsito y cifrado en reposo.
- Equipo de trabajo (que deberá incluir al personal clave, contacto, roles y funciones).
- Lista de servicios, sistemas y aplicaciones de SENCICO a migrar a la nube.
- Protocolo de pruebas.
- Procedimiento de pase a producción y rollback.
- Temario de capacitación (syllabus)
- Documentos de acreditación de conocimientos del o los Capacitador(es) respecto al Syllabus a dictar.
- SCTR del personal involucrado en las actividades del servicio (opcional).
- Acuerdo de confidencialidad suscrito.

El Departamento de Informática, tendrá como máximo siete (07) días calendarios, una vez recepcionado el plan de trabajo, para comunicar por correo electrónico, la aprobación del plan o alguna observación al contratista.

De existir observaciones, se le comunicará a EL CONTRATISTA, mediante correo electrónico, dándole un plazo de subsanación no menor a dos (02) días calendarios y no mayor a ocho (08) días calendarios, de acuerdo a la complejidad de las mismas.

8. PRESTACIONES ACCESORIAS

A. Capacitación

- a) El CONTRATISTA realizará una capacitación de la solución implementada, de los sistemas de monitoreo implementados, de las plataformas de desarrollo y sus flujos de integración, del servicio de disaster recovery, de los sistemas de seguridad y bases de datos, y de todo servicio contemplado en el TDR, con un mínimo de 36 horas, y como mínimo a 20 (veinte) personas, los cuales deberá incluir el uso de laboratorios virtuales en el temario de capacitación.
- b) La capacitación se dictará de manera presencial o virtual, para lo cual el CONTRATISTA proporcionará el temario, los equipos (físicos o en entorno virtual), materiales didácticos (digital formato PDF), laboratorios y lo crea conveniente para el dictado de los cursos. La determinación de la manera en que se llevará a cabo, se realizará como mínimo a los diez (10) días calendarios, antes de la fecha de inicio de la capacitación.
- c) La capacitación se desarrollará en coordinación con EL SENCICO, considerando cuatro (04) horas por día como máximo en horario laboral y de forma Inter diaria.
- d) Los laboratorios deberán estar disponibles 24x7, por el tiempo que se ejecute la capacitación.
- e) La capacitación deberá ser grabada.
- f) El inicio y horario de la capacitación deberá coordinarse con el Asesor en Sistemas e Informática al correo electrónico, con diez (10) días calendario, antes de la fecha de inicio de la capacitación.
- g) El Contratista deberá presentar el CV documentado del personal a dictar la capacitación (pueden ser varios capacitadores), dentro del Plan de trabajo, en el cual se acredite por medio de certificados, cursos, especializaciones u otro similar, que el personal cuenta con los conocimientos del Syllabus a dictar; SENCICO validará la documentación en conjunto con la aprobación del Plan de trabajo, por correo electrónico al Contratista.
- h) El CONTRATISTA deberá entregar una constancia de participación a los asistentes al finalizar la capacitación, donde especifique los nombres y apellidos del personal participante, fecha y duración del curso, debiendo estar firmado por el expositor.
- i) Se deberá presentar el syllabus detallado de la Capacitación en el Plan de Trabajo.

B. Soporte Técnico Gestionado

- a) El CONTRATISTA deberá asegurar la disponibilidad de los servicios contratados.

- b) El CONTRATISTA se encargará de mantener en operación y brindar soporte técnico a todos los servicios y soluciones implementados en nube(s).
- c) El CONTRATISTA deberá brindar soporte técnico 24x7x365 mediante correo y/o llamada telefónica y/o presencial, con un tiempo de respuesta y resolución de acuerdo a la sección “Acuerdo de Nivel de Servicio – SLA” y manteniendo el cumplimiento de la sección “Disponibilidad del Servicio”.
- d) El CONTRATISTA proporcionará los datos de contacto para la atención del servicio donde se deberá indicar el tipo y número de documento, nombres y apellidos completos, teléfono y correo electrónico de contacto, esto deberá ser remitido por correo electrónico junto con la asignación del ticket de atención.
- e) El servicio de soporte técnico ofrecido será prestado en idioma español.
- f) El CONTRATISTA será responsable de garantizar la disponibilidad, durabilidad y SLA de la infraestructura, plataforma, servicios e información que se encuentre almacenada en la plataforma de nube(s).
- g) EL CONTRATISTA deberá monitorear permanentemente los eventos y alertas generados por todos los servicios, servidores, plataformas, entornos, integraciones, software y/o soluciones implementadas en nube(s), y tomar acciones de remediación para la continuidad de los servicios.
- h) Se entenderá por avería a una interrupción parcial o total del servicio, así como un decremento en la calidad del mismo.
- i) Cada llamada será asociada un número de registro de Atención al Cliente (Número de ticket de incidencia), con el cual se podrá realizar el adecuado seguimiento, atención y/o resolución del incidente.
- j) Plataforma de Mesa de Ayuda
EL CONTRATISTA deberá proveer una plataforma propia de mesa de ayuda, que cuente con los siguientes elementos:
- Portal de Servicios: Portal web en donde un usuario autorizado podrá reportar las incidencias y gestionar requerimientos. Esto incluye el alta, baja y modificación de servicios.
 - Aprovisionamiento y retiro de capacidades: Proceso para requerir y/o retirar capacidades a los servicios.
- k) Portales de Servicios
EL CONTRATISTA deberá proveer los siguientes portales de gestión de servicios:
- Portal(es) de Monitoreo: Portales web en donde se visualice la información de monitoreo, performance, análisis de vulnerabilidades, postura de seguridad, de todos los servicios, servidores y plataformas implementadas en nube.
 - Portal(es) de Copias de Seguridad: Portal web en donde se visualice el estado de las tareas de copias de seguridad (backup) y el estado del almacenamiento de los mismos.
 - Portal(es) de Disaster Recovery: Portal web en donde se visualice el estado del servicio de Disaster Recovery, y estado de la sincronización de datos.
 - Portal(es) de Facturación: Portal(es) web en donde se visualice a detalle la facturación diaria, acumulada y reportaría de todos los servicios nativos de nube.
- l) Acuerdo de Nivel de Servicio – SLA
EL CONTRATISTA deberá cumplir con los siguientes acuerdos de nivel de servicio:

Tabla N° 04 –ACUERDO DE NIVEL DE SERVICIO “SLA” - INCIDENTES

Severidad	Descripción	Tiempo máximo de generación de Ticket	Tiempo de resolución (contabilizado desde la generación del Ticket)
Alta	Incidente: Asociado a indisponibilidad o degradaciones significativas de los servicios y requiere atención inmediata.	30 min	4 horas
	Problema: Errores comunes que se repiten más de 3 veces en menos de 24 horas, ocasionando indisponibilidad o degradaciones significativas.	30 min	4 horas o de acuerdo a lo programado en *conformidad con SENCICO.
Media	Incidente: Asociado a pérdidas y degradaciones moderadas de los servicios, pero el trabajo puede continuar parcialmente a pesar de la incidencia.	1 hora	6 horas

	Problema: Errores comunes que se repiten más de 3 veces en menos de 1 semana que ocasionan degradaciones moderadas.	1 hora	6 horas o de acuerdo a lo programado en *conformidad con SENCICO
Bajo	Incidente: Asociado a fallas de menor importancia que no afecten el procesamiento, ni la prestación del servicio.	2 horas	12 horas
	Problema: Errores comunes que se repiten más de 3 veces en menos de 1 semana, de menor importancia que no afecten la prestación del servicio.	2 horas	12 horas o de acuerdo a lo programado en *conformidad con SENCICO

**La conformidad por parte de Sencico, debe estar acreditada por medio de correo electrónico, como evidencia fehaciente de dicho acuerdo.*

**Tabla N° 05 –ACUERDO DE NIVEL DE SERVICIO “SLA” -
REQUERIMIENTOS**

Servicio	Descripción	Tiempo máximo de generación de Ticket	Tiempo de atención de requerimiento
REQUERIMIENTO TIPO 1	Solicitudes de configuraciones, habilitación de servicios, etc. dentro del alcance y capacidades especificadas en el TDR del presente Contrato.	1 hora	4 horas o de acuerdo a lo programado en conformidad con SENCICO, contabilizado desde la asignación del ticket.
REQUERIMIENTO TIPO 2	Solicitudes de nuevos servidores, nuevas configuraciones, nuevos servicios, etc. fuera del alcance y capacidades especificadas en el TDR del presente Contrato, el mismo que se tratará con una Adenda.	No aplica	7 días calendarios, para remitir la Cotización, contabilizado desde la remisión de la solicitud. El plazo de atención del requerimiento, será de acuerdo a la cotización del Contratista y la aceptación de la misma por la Entidad.

**La conformidad por parte de Sencico, debe estar acreditada por medio de correo electrónico, como evidencia fehaciente de dicho acuerdo.*

m) Se define los siguientes términos:

- **Incidente:** Se define como la interrupción no planificada o reducción de la calidad en los servicios habilitados en nube (todos los componentes, servicios, productos utilizados en la plataforma Cloud Computing por EL SENCICO en el periodo que dure el contrato). Un incidente también podrá ser originado como resultado de las alertas generadas por las herramientas de monitoreo y gestión de servicio.
- **Problema:** Se define como la causa desconocida de un incidente (Por ejemplo: no se tiene un reporte o solución previa documentado en la base de conocimiento) o múltiples incidentes con síntomas comunes, que afectan a los servicios habilitados en la nube(s).
- **Requerimiento:** Es una petición de servicio que realiza EL SENCICO al CONTRATISTA, mediante los canales de atención establecidos.

n) Se deberá remitir un Reporte de atención a los tres (03) días calendario como máximo de haber cerrado el ticket de incidencia y/o requerimiento, de manera digital por correo electrónico a la personal que designe el Departamento de Informática, el cual incluirá:

- Número de Ticket.
- Incidente, problema o requerimiento presentado
- Actividades realizadas
- RCA – Análisis de Causa Raíz
- Nivel de escalamiento

9. PERFIL DEL CONTRATISTA

- El contratista deberá estar inscrito en el Registro Nacional de Proveedores (RNP).
- El contratista no deberá estar impedido para contratar con el Estado Peruano.

10. PERSONAL CLAVE DEL SERVICIO

Los profesionales propuestos, titulados, deberán estar colegiados y habilitados al inicio de la participación efectiva de la ejecución del Contrato, de corresponder.

El CONTRATISTA deberá contar como mínimo con el siguiente equipo de trabajo:

Un (01) Jefe de Proyecto:**Funciones y actividades:**

- Responsable de la Gestión del Proyecto.
- Realizar las coordinaciones necesarias para la ejecución del proyecto en el plazo solicitado por el SENCICO.
- Reportar cualquier incidencia o restricción en el proyecto, que no permita la continuidad del proyecto, de forma inmediata al SENCICO.
- Presentar reportes semanales de avance.
- Presentar cronogramas semanales actualizados, de corresponder.
- Presentar actas de reuniones.
- Presentar el informe final y entregables definidos.
- Finalizado la implementación, el Jefe de Proyecto deberá transferir las actividades del servicio al Gestor de Servicios, con el fin de que se inicie la operación del servicio.
- Firma en la documentación del proyecto, como: Actas de reunión, Acta de conformidad, Informes, Protocolo de pruebas, etc.

Un (01) Arquitecto en Cloud Computing**Funciones y actividades:**

- Responsable del diseño de la solución en la especialidad de arquitecturas cloud IaaS, PaaS y SaaS.
- Responsable de las configuraciones críticas y complejas en la especialidad de servidores, plataformas de almacenamiento, conectividad y software
- Supervisar todas las actividades relacionadas a la implementación del servicio en la especialidad de servidores, plataformas de almacenamiento, conectividad y software.
- Absolver las consultas técnicas, realizadas por el Departamento de Informática en la especialidad de arquitecturas cloud IaaS, PaaS y SaaS.
- Firma en la documentación técnica del proyecto, como: Actas de reunión, Informes, protocolo de pruebas, etc., que contenga información correspondiente a la especialidad de arquitecturas cloud.
- Responsable técnico de la ejecución del protocolo de pruebas en la especialidad de arquitecturas cloud.

Un (01) Especialista en Networking**Funciones y actividades:**

- Responsable del diseño de la solución en la especialidad de networking en cloud computing.
- Responsable de las configuraciones técnicas en la especialidad de networking en cloud computing.
- Supervisar todas las actividades relacionadas a la implementación del servicio en la especialidad de networking en cloud computing.
- Absolver las consultas técnicas, realizadas por el Departamento de Informática en la especialidad de networking en cloud computing.
- Firma en la documentación técnica del proyecto, como: Actas de reunión, Informes, protocolo de pruebas, etc. Que contenga información correspondiente a la especialidad de networking en cloud computing.
- Responsable técnico de la ejecución del protocolo de pruebas en la especialidad de networking en cloud computing.

Un (01) Especialista en Bases de Datos**Funciones y actividades:**

- Responsable del diseño de la solución en la especialidad de bases de datos transaccionales (MS-SQL, Oracle).
- Responsable de la migración, configuraciones críticas y complejas en la especialidad de bases de datos transaccionales.
- Supervisar todas las actividades relacionadas a la implementación del servicio en la especialidad de bases de datos transaccionales.
- Absolver las consultas técnicas, realizadas por el Departamento de Informática en la especialidad de bases de datos transaccionales.
- Firma en la documentación técnica del proyecto, como: Actas de reunión, Informes, protocolo de pruebas, etc. Que contenga información correspondiente a la especialidad de bases de datos transaccionales.
- Responsable técnico de la ejecución del protocolo de pruebas en la especialidad de bases de datos transaccionales.

Un (01) Especialista en Seguridad**Funciones y actividades:**

- Responsable del diseño de la solución en la especialidad de seguridad perimetral, de la información y comunicaciones en cloud computing.
- Responsable de la migración, configuraciones críticas y complejas en la especialidad de seguridad perimetral, de la información y comunicaciones en cloud computing.
- Supervisar todas las actividades relacionadas a la implementación del servicio en la especialidad de seguridad perimetral, de la información y comunicaciones en cloud computing.
- Absolver las consultas técnicas, realizadas por el Departamento de Informática en la especialidad de seguridad perimetral, de la información y comunicaciones en cloud computing.
- Firma en la documentación técnica del proyecto, como: Actas de reunión, Informes, protocolo de pruebas, etc. Que contenga información correspondiente a la especialidad de seguridad perimetral, de la información y comunicaciones en cloud computing.
- Responsable técnico de la ejecución del protocolo de pruebas en la especialidad de seguridad perimetral, de la información y comunicaciones en cloud computing.

Un (01) Gestor de Servicios**Funciones y actividades:**

- Gestionar integralmente los servicios, asegurando el cumplimiento eficiente de los SLAs.
- Responsable de la revisión de facturación y acciones de mejora de los entornos de cloud computing.
- Responsable de atender los incidentes y requerimientos del SENCICO, y escalar las gestiones operativas del servicio para la solución oportuna los mismos.
- Realización de reuniones mensuales con el equipo técnico del SENCICO para la presentación y exposición de los Informes mensuales del servicio.
- Responsable de elaborar y remitir el **Reporte de atención** de cada ticket generado, a los tres (03) días de solucionado la incidencia (cerrado el ticket), en el cual se deberá detallar: incidencia suscitada, causa de la avería, solución aplicada por el operador, medidas preventivas para que no vuelva a ocurrir.

Para la firma de Contrato, se deberá presentar los siguientes certificados, de acuerdo al personal clave:

- Jefe de proyecto: certificado PMP vigente.
- Arquitecto de Cloud Computing: certificación oficial vigente de la marca de nube ofertada en el nivel Professional o Experto o su equivalente. En caso de ofertas multinivel, se deberá acreditar como mínimo la certificación oficial vigente de la nube con la mayor cantidad de servicios ofertados en el nivel Professional o Experto o su equivalente.
- Especialista en Networking de Cloud Computing: certificación Oficial vigente de la marca de nube ofertada en el nivel de Architech o Advanced Networking o su equivalente. En caso de ofertas multinube, se deberá acreditar como mínimo la certificación oficial vigente de la nube con la mayor cantidad de servicios ofertados en el nivel de Architech o Advanced Networking o su equivalente.
- Especialista en Bases de Datos: certificación Oficial vigente de la marca de nube ofertada en el nivel de Database Specialty o Database Administrator o su equivalente. En caso de ofertas multinube, se deberá acreditar como mínimo la certificación oficial vigente de la nube con la mayor cantidad de servicios ofertados en el nivel de Database Specialty o Database Administrator o su equivalente.
- Especialista en Seguridad: Certificación Oficial vigente de la marca de nube ofertada en el nivel de Security Specialty o Security Engineer o su equivalente. En caso de ofertas multinube, se deberá acreditar como mínimo la certificación oficial vigente de la nube con la mayor cantidad de servicios ofertados en el nivel de Security Specialty o Security Engineer o su equivalente.
- Gestor de Servicios: certificación oficial vigente de la(s) marca(s) de nube(s) propuesta(s) en el nivel de Administrador o su equivalente; y Certificación oficial vigente en ITIL v4. En caso de ofertas multinube, se deberá acreditar como mínimo la certificación oficial vigente de la nube con la mayor cantidad de servicios ofertados.

11. PLAZO DE EJECUCIÓN DEL SERVICIO

PRESTACION	DESCRIPCIÓN	PLAZOS
Principal	Servicio de implementación y migración	La implementación y migración del servicio será de setenta (70) días calendarios, contabilizado desde el día siguiente de aprobado el Plan de Trabajo.
	Servicio mensual Cloud Computing	El servicio será de un mil noventa y cinco (1095) días calendarios, e iniciará desde el día siguiente de firmado el Acta de Aceptación de la Implementación del Servicio.
Accesoria	Soporte Técnico	Un mil noventa y cinco (1095) días calendarios, contabilizado desde el día siguiente de firmado el Acta de Aceptación de la Implementación del Servicio.
	Capacitación	Treinta (30) días calendarios, contabilizados desde el día siguiente de firmado el Acta de Aceptación de la Implementación del Servicio.

12. ENTREGABLES:

Se deberá entregar en formato digital por mesa de partes virtual <https://app.sencico.gob.pe/prd/waMesaPartes/MesaPartes>, la siguiente documentación.

PRESTACION	DESCRIPCIÓN	PLAZOS
Principal	Servicio de implementación y migración	El Informe final de implementación, deberá presentarse a los dos (02) días calendarios, contabilizado desde el día siguiente de culminado el plazo de implementación del servicio, el cual deberá contener lo siguiente: <ul style="list-style-type: none">• Descripción de la solución implementada• Suscripción de los servicios de nube(s) con el SENCICO por el periodo total del contrato.• Lista de configuraciones de cada servicio y componente implementado.• Lista de servidores y servicios implementado.• Procedimientos operativos de la gestión del Cloud Computing.• Procedimiento de atención del soporte técnico, donde se precise los niveles de acuerdo de servicio y niveles de escalamiento, en el cual se precise por cada nivel los siguientes datos: nombre completo del contacto, rol, número de teléfono fijo y celular.
	Servicio mensual Cloud Computing	El Informe mensual del servicio deberá presentarse a los cinco (05) días calendarios, contabilizado desde el día siguiente de culminado el periodo mensual del servicio, el cual deberá contener lo siguiente: <ul style="list-style-type: none">• Resumen Ejecutivo del Servicio mensual de Cloud Computing• Cuadro resumen y detalle del uso del servicio contratado.• Cuadro resumen de disponibilidad de los servicios implementados en nube.• Cuadro resumen y Reporte detallado en formato XLS del consumo mensual y facturación mensual por cada tipo de servicio.• Cuadro resumen y Reporte en formato XLS con la capacidad de almacenamiento utilizado por tipo de servicio.• Cuadro resumen y Reporte en formato XLS con el total de transferencias de datos mensual por tipo de servicio.• Análisis mensual de rendimiento.
Accesoria	Soporte Técnico	El Informe mensual de soporte técnico, deberá presentarse a los siete (07) días calendarios, contabilizado desde el día siguiente de culminado el periodo mensual de soporte técnico, el cual deberá contener lo siguiente:

		<ul style="list-style-type: none"> Resumen Ejecutivo del Servicio mensual del Servicio de Soporte Gestionado Cuadro resumen de incidentes, problemas y requerimientos del periodo mensual. Reporte de diagnóstico, resolución y escalamiento de problemas. Cuadro detalle de incidentes, problemas y requerimientos del periodo, describiendo los tiempos de interacción de cada ticket. Cuadro resumen de monitoreo (top's) de los principales servicios de nube. Reporte detallado del monitoreo de los servicios implementados en nube: <ul style="list-style-type: none"> Performance de servidores y servicios Performance de bases de datos y detallado de top queries Performance de aplicaciones web Estado de procesos, servicios y aplicaciones. Reporte de administración de la seguridad: <ul style="list-style-type: none"> Reporte detallado de ataques al servicio de protección perimetral. Reporte detallado de ataques al servicio WAF. Reporte detallado de ejecución de tareas de copias de seguridad y requerimientos de restauración. Reporte detallado del estado del servicio de Disaster Recovery Reporte detallado del servicio de protección antivirus/antiransomware. Resumen de la analítica de eventos. Reporte de la evaluación continua de vulnerabilidades. Reporte postura de seguridad Reporte de análisis y recomendaciones de optimización de recursos. Recomendaciones y conclusiones.
	Capacitación	<p>A los cinco (05) días calendarios, contabilizados desde el día siguiente de culminado la capacitación se deberá presentar lo siguiente:</p> <ul style="list-style-type: none"> Constancia de participación de la capacitación a todo el personal que participó. Lista de asistencia de todo el personal que participó. Se deberá entregar todo el material de la capacitación en formato digital, incluyendo las grabaciones o el link respectivo.

13. LUGAR DE LA PRESTACIÓN DEL SERVICIO

El lugar de la prestación del servicio se realizará en SENCICO ubicado en la Av. De la Poesía N° 351 San Borja y en la nube de la marca y/o Contratista.

14. CONFORMIDAD DEL SERVICIO

El Asesor de Sistemas e Informática del Departamento de Informática, otorgará la respectiva conformidad de servicio y entregable, previa verificación del cumplimiento de las condiciones establecidas en el artículo 168° del Reglamento de Contrataciones del Estado, en los plazos de acuerdo a la Ley de Contrataciones del Estado y su reglamento vigente.

De existir observaciones, el Asesor de Sistemas e Informática comunicará al contratista, por correo electrónico, indicando claramente el sentido de estas, otorgándole un plazo para subsanar las observaciones, de acuerdo a la Ley de Contrataciones del Estado y su reglamento vigente.

Se comunicará las observaciones al Contratista, mediante correo electrónico, en los plazos de acuerdo a la Ley de Contrataciones del Estado y su reglamento vigente.

15. FORMA DE PAGO

El pago se realizará de acuerdo al siguiente cuadro:

	DESCRIPCIÓN	PERIODICIDAD	DETALLE DE PAGO
Prestación Principal	Servicio de implementación y migración	Una sola vez	100%

	Servicio mensual Cloud Computing	Mensual	36 pagos mensuales de acuerdo a los sistemas de contratación de precios unitarios y suma alzada, descrito en el Numeral 6, inciso Z.
Prestación Accesorias	Soporte técnico	Mensual	Pagos mensuales: 36 pagos iguales
	Capacitación	Una sola vez	100%

El pago se efectuará mediante el respectivo abono en la cuenta bancaria individual del Contratista, de acuerdo a los plazos de la Ley de Contrataciones del Estado vigente y su reglamento, de encontrarse completo el expediente de pago, sea a través del Banco de la Nación o de cualquier otra institución bancaria del Sistema Financiero Nacional, para cuyo efecto EL CONTRATISTA comunicará su CODIGO DE CUENTA INTERBANCARIO (CCI).

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Informe del funcionario responsable del Departamento de Informática emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Entregable correspondiente de la prestación principal y/o accesorias.

16. RESPONSABILIDAD DEL CONTRATISTA

El Contratista es el único responsable ante SENCICO de cumplir con la contratación, no pudiendo transferir esa responsabilidad a otras entidades ni terceros en general.

Así también es responsable por la calidad ofrecida y por los vicios ocultos de los servicios ofertados por un plazo de tres (03) años contado a partir de la conformidad otorgada, de acuerdo a lo dispuesto en el artículo 40° de la Ley de Contrataciones del Estado.

17. PENALIDADES APLICABLES

En caso de retraso en la ejecución de las contraprestaciones ejecutadas por el contratista, se aplicará una penalidad al contratista por cada día de retraso hasta por el monto máximo del 10% del monto según lo dispuesto en los artículos 161° y 162° del Reglamento de la Ley de Contrataciones del Estado vigente.

18. OTRAS PENALIDADES

De conformidad con lo estipulado en el artículo 163° del Reglamento de la Ley de Contrataciones del Estado, se han establecido otras penalidades diferentes a la penalidad por mora, las cuales son objetivas, razonables y congruentes con el objeto de la convocatoria, las mismas que se detallan a continuación:

N°	SUPUESTO	MONTO APLICABLE S/	PROCEDIMIENTO
1	Incumplir con el plazo de entrega del PLAN DE TRABAJO	200.00	Por cada 1 (un) día excedente que el Contratista incumpla con el plazo de entrega del Plan de Trabajo, la penalidad será aplicada.
2	Incumplir con el plazo de subsanación de observaciones del PLAN DE TRABAJO	200.00	Por cada 1 (un) día excedente que el Contratista incumpla con el plazo de subsanación del Plan de Trabajo, la penalidad será aplicada.
3	Incumplir con el plazo de presentación de Informe Final de implementación y migración.	200.00	Por cada 1 (un) día excedente que el Contratista incumpla con el plazo de entrega del Informe Final de implementación, la penalidad será aplicada
4	Incumplir con el plazo de subsanación de observaciones del Informe final de implementación y migración.	200.00	Por cada 1 (un) día excedente que el Contratista incumpla con el plazo de subsanación del Informe final de Implementación, la penalidad será aplicada.
5	Incumplir con el plazo de presentación de Informe mensual del servicio y/o Informe mensual de soporte técnico y/o reporte de atención.	200.00	Por cada 1 (un) día excedente que el Contratista incumpla con el plazo de entrega del Informe mensual del servicio y/o Informe mensual de soporte técnico y/o reporte de atención, la penalidad será aplicada.

6	Incumplir con el plazo de subsanación de observaciones del Informe mensual del servicio y/o Informe mensual de soporte técnico y/o reporte de atención.	100.00	Por cada 1 (un) día excedente que el Contratista incumpla con el plazo de subsanación del Informe mensual del servicio y/o Informe mensual de soporte técnico y/o reporte de atención, la penalidad será aplicada.
7	Incumplir con los SLAs definidos en la – Tabla N°04	200.00	Por cada 1 (una) hora excedente que el contratista incumpla con los SLAs – Tabla N°04: la penalidad será aplicada.
8	Incumplir con los SLAs definidos en la Tabla N°05 – Requerimiento TIPO 1	100.00	Por cada 1 (una) hora excedente que el contratista incumpla con los SLAs – Tabla N°05 – Requerimiento TIPO 1: la penalidad será aplicada.
9	Incumplir con los SLAs definidos en la Tabla N°05 – Requerimiento TIPO 2	100.00	Por cada 1 (un) día excedente que el contratista incumpla con los SLAs – Tabla N°05 – Requerimiento TIPO 2: la penalidad será aplicada.
10	Incumplir con la disponibilidad mensual solicitada del Inciso X, de los términos de referencia.	10% de 1 UIT	Cada vez que el Contratista no cumpla con la disponibilidad mensual solicitada en el Inciso X del presente TDR, la penalidad será aplicada.
11	Ingreso no autorizado a la red y/o sistemas y/o equipos y/o aplicaciones y/o servicios, del SENCICO o alojados en la nube contratada por SENCICO.	50% de 1 UIT	Cada vez que el Contratista ingrese la red y/o sistemas y/o equipos y/o aplicaciones y/o servicios, del SENCICO o alojados en la nube contratada por SENCICO, de manera no autorizada y/o supervisada, la penalidad será aplicada.
12	Cambiar el Personal Clave sin la aprobación del SENCICO.	20% de 1 UIT	Cada vez que el Contratista cambien el personal clave sin la aprobación formal del SENCICO, la penalidad será aplicada.

El procedimiento para comunicar las penalidades, es la siguiente:

- El área usuaria es el responsable de comunicar al Contratista, mediante correo electrónico y/o Carta por correo electrónico, con copia al Departamento de Abastecimiento, los incumplimientos u omisión de obligaciones, como máximo a 10 días calendarios, contabilizado desde el día siguiente de ocurrido el incidente.
- El Contratista en un plazo no mayor a 05 días calendarios, contabilizados desde el día siguiente de recepcionado la comunicación por parte de la Entidad del Incidente, realizará su descargo correspondiente a través de mesa de partes virtual: <https://app.sencico.gob.pe/prd/waMesaPartes/MesaPartes>, caso contrario se asumirá que el Contratista acepta lo imputado.
- El área usuaria, comunicará oportunamente al Departamento de Abastecimiento, para la aplicación de la Penalidad, en caso corresponda.

19. CONFIDENCIALIDAD

El contratista se compromete a mantener en reserva, y no revelar a terceros, sin autorización escrita de SENCICO, la información que le sea suministrada por este último o a la cual tenga acceso, excepto en cuanto resultare estrictamente necesario para el cumplimiento del Contrato, y que restringirá la revelación de dicha información sólo a sus empleados, sobre la base de "necesidad de conocer".

En el Servicio y con el fin de resguardar la información de la entidad se prohíbe las siguientes actividades:

- Se prohíbe que el Contratista utilice softwares para capturar información de la Entidad, en caso se detecte que el Contratista tenga instalado un software de captura de información, este será retirado inmediatamente de la Entidad.
- Se prohíbe que el Contratista ingrese sin autorización y supervisión del Departamento de Informática, a la red y/o equipos y/o sistemas de la Entidad.

20. REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD TÉCNICA Y PROFESIONAL
A.1	CALIFICACIONES DEL PERSONAL CLAVE
A.1.1	FORMACIÓN ACADÉMICA
	Requisitos: Jefe de proyecto: Título Profesional de Ingeniero de Sistemas y/o Título Profesional de Ingeniero en Computación y/o Título Profesional de Ingeniero en Telemática y/o Título Profesional de Ingeniero en Informática y/o Título Profesional de

	<p>Ingeniero de Telecomunicaciones y/o Título Profesional de Ingeniero en Computación y Sistemas, del personal clave requerido como Jefe de Proyecto.</p> <p>Arquitecto Cloud Computing: Título Profesional de Ingeniero de Sistemas y/o Título Profesional de Ingeniero en Computación y/o Título Profesional de Ingeniero en Telemática y/o Título Profesional de Ingeniero en Informática y/o Título Profesional de Ingeniero de Telecomunicaciones y/o Título Profesional de Ingeniero en Computación y Sistemas y/o Bachiller en Ingeniería de Sistemas y/o Bachiller en Ingeniería de Computación y/o Bachiller en Ingeniería Telemática y/o Bachiller en Ingeniería de Informática y/o Bachiller en Ingeniería de Telecomunicaciones y/o Bachiller en Ingeniería de Computación y Sistemas, del personal clave requerido como Arquitecto de Cloud Computing.</p> <p>Especialista en Networking de Cloud Computing: Título Profesional de Ingeniero Electrónico y/o Título Profesional de Ingeniero de Sistemas y/o Título Profesional de Ingeniero en Computación y/o Título Profesional de Ingeniero en Telemática y/o Título Profesional de Ingeniero en Informática y/o Título Profesional de Ingeniero de Telecomunicaciones y/o Título Profesional de Ingeniero en Computación y Sistemas y/o Bachiller en Ingeniería de Sistemas y/o Bachiller en Ingeniería de Computación y/o Bachiller en Ingeniería Telemática y/o Bachiller en Ingeniería de Informática y/o Bachiller en Ingeniería de Telecomunicaciones y/o Bachiller en Ingeniería de Computación y Sistemas, del personal clave requerido como Especialista en Networking de Cloud Computing.</p> <p>Especialista en Seguridad: Título Profesional de Ingeniero Electrónico y/o Título Profesional de Ingeniero de Sistemas y/o Título Profesional de Ingeniero en Computación y/o Título Profesional de Ingeniero en Telemática y/o Título Profesional de Ingeniero en Informática y/o Título Profesional de Ingeniero de Telecomunicaciones y/o Título Profesional de Ingeniero en Computación y Sistemas y/o Bachiller en Ingeniería de Sistemas y/o Bachiller en Ingeniería de Computación y/o Bachiller en Ingeniería Telemática y/o Bachiller en Ingeniería de Informática y/o Bachiller en Ingeniería de Telecomunicaciones y/o Bachiller en Ingeniería de Computación y Sistemas, del personal clave requerido como Especialista en Seguridad.</p> <p>Especialista en Bases de Datos: Título Profesional de Ingeniero Electrónico y/o Título Profesional de Ingeniero de Sistemas y/o Título Profesional de Ingeniero en Computación y/o Título Profesional de Ingeniero en Telemática y/o Título Profesional de Ingeniero en Informática y/o Título Profesional de Ingeniero de Telecomunicaciones y/o Título Profesional de Ingeniero en Computación y Sistemas y/o Bachiller en Ingeniería de Sistemas y/o Bachiller en Ingeniería de Computación y/o Bachiller en Ingeniería Telemática y/o Bachiller en Ingeniería de Informática y/o Bachiller en Ingeniería de Telecomunicaciones y/o Bachiller en Ingeniería de Computación y Sistemas, del personal clave requerido como Especialista en Bases de Datos.</p> <p>Gestor de Servicios: Título Profesional de Ingeniero Electrónico y/o Título Profesional de Ingeniero de Sistemas y/o Título Profesional de Ingeniero en Computación y/o Título Profesional de Ingeniero en Telemática y/o Título Profesional de Ingeniero en Informática y/o Título Profesional de Ingeniero de Telecomunicaciones y/o Título Profesional de Ingeniero en Computación y Sistemas y/o Bachiller en Ingeniería de Sistemas y/o Bachiller en Ingeniería de Computación y/o Bachiller en Ingeniería Telemática y/o Bachiller en Ingeniería de Informática y/o Bachiller en Ingeniería de Telecomunicaciones y/o Bachiller en Ingeniería de Computación y Sistemas, del personal clave requerido como Gestor de Servicios.</p> <p><u>Acreditación:</u> El Grado 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 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.</p> <p>En caso el Grado o Título Profesional 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.</p>
A.1.2	<p>CAPACITACIÓN</p> <p>Jefe de proyecto: Treinta (30) horas lectivas en Curso o Especialización o Diplomados en: Gestión o Dirección de Proyectos, del personal clave requerido como Jefe de Proyecto.</p> <p>Gestor de Servicios Treinta (30) horas lectivas en Curso o Especialización o Diplomados en: Gestión de Servicios de TI o Gestión de Tecnologías de la Información o Administración de Centros de Datos, del personal clave requerido como Gestor de Servicios, culminado dentro de los últimos 24 meses.</p> <p><u>Acreditación:</u> Se acreditará con copia simple de constancias o certificados o diplomas u otros documentos que acredite fehacientemente lo solicitado, en caso el certificado no indique las horas lectivas, se podrá acreditar también con</p>



	<p>syllabus o información de la entidad que otorga el certificado o malla curricular o cualquier documento adicional; que acredite las horas lectivas de lo solicitado; según corresponda.</p> <div> <div>Importante</div> <div> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p> </div> </div>
A.2	<p>EXPERIENCIA DEL PERSONAL CLAVE</p> <p><u>Requisitos:</u></p> <p>Jefe de Proyectos: Deberá contar con una experiencia mínima de tres (03) años como Jefe de Proyectos o Gestor de proyecto o Gerente de Proyecto o Coordinador de Proyectos o subgerente de proyectos, en la especialidad de: Tecnología de la información y/o telecomunicaciones y/o redes de datos, del personal clave requerido como Jefe de proyectos.</p> <p>Arquitecto de Cloud Computing: Deberá contar con una experiencia mínima de tres (02) años en implementación y/o supervisor y/o configuración y/o instalación de soluciones de cloud computing, del personal clave requerido como Arquitecto de Cloud computing.</p> <p>Especialista en Networking de Cloud Computing: Deberá contar con una experiencia mínima de dos (02) años en implementación y/o supervisor y/o configuración y/o instalación de soluciones de conectividad, IP/VPN y/o WAN, del personal clave requerido como Especialista en networking de cloud computing.</p> <p>Especialista en Bases de Datos: Deberá contar con una experiencia mínima de dos (02) años en implementación y/o supervisor y/o configuración y/o instalación de bases de datos empresariales, del personal clave requerido como Especialista en bases de datos.</p> <p>Especialista en Seguridad Deberá contar con una experiencia mínima de dos (02) años en implementación y/o supervisor y/o configuración y/o instalación de soluciones: Seguridad gestionada y perimetral y/o seguridad gestionada y/o seguridad de la información, del personal clave requerido como Especialista en Seguridad.</p> <p>Gestor de Servicios Deberá contar con una experiencia mínima de dos (02) años en supervisión y/o administración y/o responsable y/o gestión de centros de servicios de TI o data center o centro de datos, del personal clave requerido como Gestor de Servicios.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></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> <div> <div>Importante</div> <div> <ul style="list-style-type: none"> Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación 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 En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo. Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas. Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases. </div> </div>
B	<p>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</p> <p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 10,000,000.00 (diez millones 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: servicios de implementación en cloud computing, servicios de migración a nubes públicas, servicios de hosting empresariales en nube y/o en servicios cloud y/o servicios hosting y/o servicios en infraestructura en nube y/o housing</p>

Acreditación:

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 pago¹, correspondientes a un máximo de veinte (20) contrataciones.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad

Importante

- *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia actividades que ejecutó el postor corresponden a la experiencia requerida.*
- *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

ING. HECTOR ROGER VARAS GRAUS
Asesor en Sistemas e Informática

¹ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"

(...)

"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".