

Términos de Referencia

“Servicio de alojamiento de Hosting, seguridad y respaldo de aplicación Web y archivos basados en Nube (Cloud Computing) en la modalidad de Plataforma como Servicio (PAAS)¹ y Software como Servicio (SAAS)”

1. Finalidad pública

El Tribunal Constitucional, como casi todas las entidades tanto públicas como privadas, cuenta con una página web en la que se publican, desde las resoluciones que emite cotidianamente hasta información sobre las actividades que desarrolla, como parte de la función institucional. Adicionalmente, con la finalidad de dar cumplimiento a los objetivos estratégicos institucionales prevé desarrollar nuevos servicios, entre ellos mejorar los servicios ofrecidos por las ventanillas tanto virtual y administrativa, así como la implementación del acceso a los servicios de la intranet de manera segura y fiable desde fuera del recinto institucional. En virtud a ello se hace necesaria la contratación de un servicio que permita disponer de dos servidores seguros y de altas prestaciones que nos permitan solventar las demandas de servicios tanto de nuestros usuarios externos como internos. Hoy en día las nuevas tendencias tecnológicas, entre ellas, la denominada computación en la nube (Cloud Computing), permiten disponer de servidores de altas prestaciones tanto en eficiencia, seguridad, disponibilidad y escalabilidad. En virtud a lo anteriormente expresado se considera necesaria la contratación del servicio solicitado.

2. Antecedentes

El Tribunal Constitucional es el supremo intérprete de la Constitución, y entre las funciones que le ha encargado la Constitución y su Ley Orgánica se encuentra resolver en última y definitiva instancia los recursos de tutela de derechos y resolver en última y definitiva instancia los procesos de inconstitucionalidad y los conflictos competenciales. En esa condición todos y cada uno de las resoluciones que emite el Tribunal Constitucional deben ser de conocimiento público, mediante su portal web. Si bien el Tribunal Constitucional cuenta con un centro de datos; no obstante, el alojar la información que se debe publicar en el portal web no podría alojarse en dichos servidores tanto por razones de seguridad, tecnológicas e incluso de economía, debido que en la actualidad resulta más rentable contratar los servicios de alojamiento en el ciberespacio que alojar la información en servidores locales.

3. Objetivos de la contratación

Contratar los servicios de una empresa o persona jurídica que implemente una arquitectura diseñada en Cloud Computing, dicha infraestructura de servicios en la nube debe alojar la

¹ El proveedor de este servicio en la nube se encarga de entregar una plataforma a la organización cliente. El cliente no administra ni controla la infraestructura, pero tiene el control sobre las aplicaciones instaladas y su configuración, y puede incluso instalar nuevas aplicaciones. Definición contenida en los “Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano”



Tribunal Constitucional

información que el Tribunal Constitucional publica en su página web, aplicaciones internas y externas. A su vez debe proporcionar los servicios de seguridad y respaldo correspondientes a las aplicaciones y archivos de cada servidor. De acuerdo a los Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado la categoría Plataforma como servicio (PAAS)

4. Alcance

El servicio de Nube por parte del proveedor está destinado a proporcionar almacenamiento, soporte, mantenimiento y recursos de capacidad de cómputo en nube que permita el desarrollo de una herramienta informática con el objetivo de brindar información adecuada en cada nivel de servicio.

Asegurar la continuidad del servicio de las aplicaciones web y del servicio web del Tribunal Constitucional.

5. Características y condiciones del servicio a contratar

5.1. Descripción y cantidad del servicio a contratar

El servicio de alojamiento del Tribunal se basará en una modalidad de alojamiento en la nube denominada Plataforma como servicio (PAAS) que debe permitir al Tribunal Constitucional publicar un conjunto de servicios para uso de los justiciables, comunidad jurídica en general y al personal del Tribunal Constitucional. La Entidad actualmente cuenta con un servicio PAAS y es la responsable del compilado de sus aplicaciones.

Existirán ciertos servicios tales como Backups, compartición de archivos y análisis de aplicaciones que estarán basadas en el servicio tipo SAAS ya que son software contratados como servicio.

- Para todos los servicios de cada servidor, el proveedor es responsable de la configuración y ejecución de Backups, así como la restauración en caso sea necesario.
- Para el caso de aplicaciones y Bases de datos en los diferentes servidores, se debe permitir la recuperación en cualquier instante de tiempo, de un periodo anterior no superior a los 20 minutos previos a la caída del sistema, durante el periodo de backup. Vale decir que en caso de contingencia o conmutación por error / failover los recursos destinados a superar la contingencia sean equivalentes o superiores al o los servidores afectados.
- Los respaldos, deberán ser almacenados en un sitio seguro bajo custodia, y de accesos con permisos a quien se le solicite.
- El proveedor deberá realizar pruebas de restauración de los backups, cuya coordinación y verificación estará a cargo del responsable designado por la Oficina de TI del Tribunal Constitucional.





Tribunal Constitucional

Disponibilidad de infraestructura (HA), El proveedor deberá revisar y asegurar que la infraestructura implementada para los servidores y sus servicios, estén configurados en alta disponibilidad, por lo que los usuarios deben poder ingresar a los servicios publicados sin ninguna restricción y dentro del nivel de servicio solicitado.

El servicio de protección de seguridad, el proveedor debe velar por el cumplimiento y aplicación de las siguientes condiciones:

- ✓ *Garantizar que los servicios web alojados en el Cloud cuenten con buenas prácticas y una buena gestión de la seguridad de la información. Estas prácticas deberán mitigar los riesgos de ataques de Man in the middle, Ip Spoofing, Identity-Spoofing y phishing.*
- ✓ *El proveedor deberá de proporcionar el servicio de Protección Perimetral al Servicio de Cloud o Nube Privada, considerando como mínimo los servicios de: Next Generation Firewall, IPS, Antivirus, DLP, Control de aplicaciones, Sandboxing, antiDDoS y VPN(SSL & IPSEC), con la finalidad de garantizar la integridad y disponibilidad de la información publicada a través de los servicios contratados, los cuales deben de tener protección de ataques de denegación de servicio, así como protección contra ataques a las Bases de datos. La protección de seguridad aplica para toda la infraestructura y en todas las superficies de ataque, la protección debe cumplir con los siguientes lineamientos de la industria: ISO27001 / CVE / CWE / ATT&CK / NIST / OWASP Top 10 / OSINT².*
- ✓ *Debe permitir la administración de perfiles (realizar las altas, bajas y modificaciones a los derechos de acceso), y credenciales de seguridad para el Usuario.*
- ✓ *Debe permitir el Soporte de escaneo de vulnerabilidades para Linux y Windows.*



5.2. Actividades

En el anexo adjunto se presenta un cuadro sumario de las características del servicio solicitado.

5.3. Procedimiento

El servicio estará constituido por una combinación de hardware y software, que permita la adecuada prestación de los servicios solicitados.

El servicio deberá tener una disponibilidad mínima de 99.975 ³% del total de horas por mes, para lo cual el proveedor deberá de contar los mecanismos tanto de hardware como de

² Se absuelve consulta N°56 del participante AMERICATEL PERU S.A.

³ Se absuelve consulta N°57 del participante AMERICATEL PERU S.A.



Tribunal Constitucional

software que garanticen al Tribunal Constitucional que los servicios ofrecidos en los servidores materia de los presentes términos de referencia se encuentren disponibles cuando estos sean requeridos con un nivel de tolerancia de ausencia de servicio no superior al 0.1%.

El servicio deberá considerar todo el licenciamiento y elementos de seguridad incluidos en las capas 3, 4 y 7 del modelo de capas OSI como también el protocolo SSL, en la capa de transporte, sin incurrir en costos ocultos. Dicho componente de seguridad debe contar con servicio DDoS Firewall de aplicaciones y protección de DNS.

Los servicios serán gestionados por el proveedor ante cualquier incidencia con la infraestructura Cloud o servidor, esto quiere decir, que el proveedor debe garantizar un soporte técnico que cubra todos los niveles (1, 2, 3 y 4) de la estructura de soporte técnico multinivel generalmente aceptados, bajo los estándares N1, N2, N3 y N4. Para los temas de backup en línea y compartición de archivos se deberá contar con cifrado multinivel certificado por NIST⁴.

La disponibilidad requerida sobre el servicio es del 99.975⁵% mensual para el acceso a los servicios contratados. Este parámetro está referido a averías imputables al proveedor. El tiempo de inoperatividad del servicio se calculará desde el reporte de la falla por parte del Tribunal Constitucional hasta la verificación de la solución de la avería por parte también de la oficina informática del Tribunal Constitucional.

El proveedor apoyará en las pruebas a realizar referente a las aplicaciones y en las adecuaciones específicas (mantenimiento, upgrade y/o migración de sistema operativo, actualización de parches), con el fin de probar la integración y conectividad de las aplicaciones y servicios.

Los cambios en la configuración de la infraestructura, mantenimiento del servicio serán coordinados y autorizados previamente por la Oficina de TI del Tribunal Constitucional.

5.4. Plan de trabajo

Visitas previas y conocimientos de la información a alojar: Los postores podrán visitar las instalaciones del Tribunal Constitucional a fin de elaborar una propuesta más precisa y de acuerdo a las necesidades expresadas por la Oficina de Tecnologías de la Información y de la infraestructura actual. Asimismo, podrán recabar información acerca de los volúmenes de información actualmente alojados, flujos diarios y mensuales de información almacenada y estadísticas de demandas de visitas al portal web institucional. Para las Visitas se deberá coordinar con el Ingeniero Jilver Rodriguez Neyra al correo jrodriguez@tc.gob.pe.

⁴ Absolución a la consulta N°01 del participante AMBER CLOUD INC S.A.C

⁵ Se absuelve consulta N°57 del participante AMERICATEL PERU S.A.





Tribunal Constitucional

Una vez determinado el postor ganador, éste tendrá un plazo no mayor a siete (7) días calendario para poner totalmente operativo el portal web y sus aplicaciones, de modo tal que en ningún instante el Tribunal Constitucional deje de contar con este importante medio de comunicación con la sociedad. Se indica que el postor deberá de poner totalmente operativo el portal web, base de datos, aplicaciones web, configuraciones servidor, base de datos y correo. La entidad se encargará de migrar las aplicaciones; de manera adicional la adecuación a dicho servidor debe ser competencia del proveedor en coordinación con la Entidad.

5.5. Requisitos según leyes, reglamentos técnicos, normas metrológicas y/o sanitarias, reglamentos y demás normas

El proveedor acreditará ser proveedor o distribuidor de servicios de computación en la nube pública (Cloud Computing). Para lo cual podrá hacerlo mediante certificado y /o carta del fabricante/marca de la nube **pública** a ofertar garantizando que el postor sea un proveedor/distribuidor de Nube pública.

Para casos de proveedores de nube privada, deberán sustentarlo mediante declaración jurada con coordenadas geográficas de alojamiento físico del Data Center de la nube privada o colocación.

El proveedor deberá someterse a los "Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano", especialmente a los aspectos vinculados los Requisitos en materia de seguridad de la información y los Requisitos en materia de protección de los datos personales, contenidos en los puntos 4 y 5 de los lineamientos citados.

5.6. Prestaciones del servicio

5.6.1. Mantenimiento preventivo

Las labores de mantenimiento preventivo del servidor de alojamiento estarán bajo responsabilidad del proveedor del servicio, debiendo establecer un programa para este servicio, si lo considerara conveniente, el mismo que deberá hacerse, en lo posible, en hora de menor demanda de tráfico de datos en el país.

Para el caso de conectividad, seguridad, backup, autenticación, disponibilidad y administración, El PROVEEDOR debe cuantificar los servicios de manera integral y considerar los Componentes-Productos necesarios para lograr esto en su plataforma Cloud.

El proveedor deberá realizar reuniones de trabajo propias del cierre y transferencia del servicio y considerar la disponibilidad, datos, información, accesos, formatos, facilidades, recursos, etc. con el fin de que se realice la migración y transición, de una manera correcta, de todos los servicios (configuraciones, información, etc.), en caso corresponda.





Tribunal Constitucional

- ✓ El proveedor debe analizar el rendimiento de los servicios, comunicar de manera oportuna a la Oficina de TI, cuando estos se encuentren cerca de los umbrales establecidos y detectar de forma proactiva posibles errores, así como diagnóstico de problemas.

5.6.3. Capacitación y/o entrenamiento

Como parte del servicio, el proveedor deberá brindar cuanto menos 40 horas de capacitación sobre la administración de la solución en Cloud PAAS y SAAS a implementarse, a tres (03) personas encargado de la administración del portal web del Tribunal Constitucional. El proveedor brindará un plan de capacitación y/o entrenamiento.

La capacitación deberá contemplar mínimo:

- ✓ Plataforma de capacitación, contenido de los cursos, Material referido a los productos a usar en el presente servicio
- ✓ Dicha capacitación podrá ser presencial o virtual.
- ✓ Manuales y Certificados



5.7. Lugar y plazo de prestación del servicio

5.7.1. Lugar

Si bien el servicio será prestado al Tribunal Constitucional; no obstante, los servicios, por su misma naturaleza, deberán tener un alcance global, vale decir el portal web que se aloje el portal web deberá ser visible en cualquier parte del mundo, salvo bloqueos por parte del país desde el cual se esté accediendo al portal.

5.7.2. Plazo

El plazo de ejecución del servicio es de doce (12) meses o 365 días contabilizados a partir del día siguiente de la habilitación y puesta en marcha del servicio.

6. Requisitos y recursos del proveedor

Se contemplan en el **Anexo I**

7. Otras consideraciones para la ejecución de la prestación

7.1. Otras obligaciones

7.1.1. Otras Obligaciones del contratista

El ganador de la buena pro, se obliga a entregar un backup semanal de la información de las bases de datos alojados en el site. El cual deberá ser entregado mediante una dirección



Tribunal Constitucional

URL que deberá ser proporcionada por el proveedor del servicio para ser descargada desde ella.

El proveedor deberá otorgar todas las facilidades para la migración de los datos alojados en sus servidores con una anticipación no superior a los 7 días calendarios a la culminación de su contrato. Además, el proveedor tendrá hasta 30 (treinta) días calendario contados a partir del día siguiente de culminado el servicio para entregar a la Oficina de TI del Tribunal Constitucional todas las imágenes de servidores virtuales, todos los datos e informaciones que estén almacenados o alojados en el ambiente provisto por el contratista en los formatos previamente acordados con el Coordinador de Informática.



7.1.2. Recursos y facilidades a ser provistos por la Entidad

El Tribunal Constitucional deberá proporcionar todas las facilidades y coordinaciones necesarias con el proveedor actual para la migración de la información alojada en los servidores web.

7.2. Adelantos

No se contempla ningún tipo de adelantos, los pagos serán realizados al término de los períodos mensuales

7.3. Subcontratación

El ganador de la buena pro se hará responsable del contrato, responsabilizándose por eventuales subcontratos que tuviera con proveedores tanto nacionales como foráneos de los servicios ofrecidos. Se deberá tener en cuenta que la subcontratación estará permitida, siempre que se cumpla con lo estipulado en la Ley y su reglamento.

7.4. Confidencialidad

El proveedor del servicio debe garantizar la confidencialidad de la información en los servidores a contratar, respecto a las copias de respaldo que realice como parte de la prestación del servicio, debiendo dicho respaldo contar con mecanismos de cifrado de información.

El postor se compromete a firmar el Formato denominado "Acuerdo de Confidencialidad para Proveedores", que forma parte de los presentes Términos de Referencia.

En caso de que el proveedor incumpla con la confidencialidad, a sola discreción se podrá rescindir la contratación y además adoptar las acciones legales que correspondan.

Los productos, entregables, documentos, archivos y en general cualquier información o conocimiento generados durante el servicio, serán de propiedad única y exclusiva de la oficina de TI del Tribunal Constitucional, quedando prohibido el uso por parte del contratista, salvo autorización expresa del Tribunal Constitucional.



Tribunal Constitucional

5.6.2. Soporte Técnico

Las labores de soporte técnico estarán cargo del proveedor y las cuales deberán cubrir como mínimo:

- ✓ *El proveedor será responsable de brindar el apoyo, asesoramiento en mesas de trabajo a la Oficina de TI, en el uso de la plataforma y sus componentes, esto incluye configuraciones, rendimiento, seguridad, capacidad, continuidad, mejores prácticas, optimizando el uso efectivo de los recursos en todos los ambientes contratados.*
- ✓ *El proveedor deberá de asignar a un especialista Cloud y/o a un arquitecto Cloud, según sea el caso, para resolver los incidentes y requerimientos reportados por la oficina de TI. La asignación será a través de un correo electrónico a la Oficina de TI, indicando los datos solicitados, personal de contacto, correo electrónico, teléfono.*
- ✓ *Ante una indisponibilidad del servicio, el tiempo de respuesta para dar asistencia y soporte técnico no excederá de 1 horas, según sea el caso reportado por el proveedor.*
- ✓ *Respecto al LOG de la aplicación, el contratista debe brindar todas las facilidades para que la Oficina de TI pueda realizar el análisis de los errores de la aplicación y de las herramientas de monitoreo configuradas.*
- ✓ *Incorporar herramientas de monitoreo tales como acceso a un panel de control (Incluido el licenciamiento de CPANEL para cada dominio), hasta un máximo de 50 dominios, herramientas de administración de alojamiento (web host manager-WHM), creación y administración de cuentas de correo etc. que permitan la administración de cada uno de los servidores, así como servicios de software que permitan obtener estadísticas de acceso a las diversas páginas del website y otras que faciliten una administración ágil y segura de los servidores. Asimismo, la herramienta a utilizar deberá contener CPANEL para la administración de base de datos, correos y otros.*
- ✓ *Contar con oficinas físicas en Lima Perú y disponer de atención en las mismas si el Tribunal lo requiere y/o solicitar la presencia de un personal técnico del representante del fabricante (postor) a las instalaciones del TC, además de un Centro de Atención el cual monitoree y supervise la disponibilidad de los servicios las 24 horas del día, los 7 días de la semana, los 365 días del año.*
- ✓ *Contar con un Centro de Atención de Llamadas de reparación o asistencia técnica del servicio, de tal manera que le asegure el funcionamiento con un soporte las 24 horas del día, los 7 días de la semana, los 365 días del año. Las llamadas para atención se deberán atender de manera rápida, personalizada y continua a través de un número con prefijo 0800 y/o teléfono fijo y/o teléfono móvil. El centro de atención en primera instancia va ser por parte de Partner, con la posibilidad de escalar al fabricante, que será acreditada mediante carta, indicando la dirección, teléfonos y correos de contactos para contacto con el centro de atención.*
- ✓ *Elaborar reportes de fallas en los servicios, si se presentaran, detallando las causas de las mismas.*





Tribunal Constitucional

- ✓ *Elaborar un reporte de rendimiento y de incidencias ante ataques vía fuerza bruta en los diferentes servicios brindados.*
- ✓ *Contar con mecanismos de atención de averías basado en llamada telefónica, mensajes de correo, tickets de atención de averías, etc.*
- ✓ *Creación y configuración de nuevos ambientes, componentes o servicios disponibles en la plataforma.*
- ✓ *Ejecutar los planes de continuidad operativa en caso de Desastres, para lo cual el proveedor deberá contar con un Plan de Recuperación de Desastres (Disaster Recovery Plan), que permita minimizar el RTO⁶. Con un RTO máximo de 25 o 30 minutos, para este propósito las características de la contingencia, deberían ser equivalentes a los servidores de producción.*
- ✓ *El proveedor es responsable del control del acceso a los servicios de plataforma, según las políticas de seguridad, restablece contraseñas, administra cuentas de usuario (crear/actualizar/eliminar), grupos de usuarios y solicitudes de servicio. Las políticas y lineamientos necesarios para la gestión de accesos serán elaboradas de manera conjunta entre el proveedor y la oficina de TI del Tribunal Constitucional).*
- ✓ *El historial de todo cambio, script o ejecución realizado contra los ambientes de la Plataforma debe estar reflejado en reportes en línea y en los informes presentados en los entregables.*
- ✓ *Los servicios provistos desde el Cloud deberán ser visualizados por el personal de TI del Tribunal Constitucional, a través de una consola de administración web con capacidad de monitoreo del servicio brindado.*
- ✓ *El proveedor deberá monitorear e implementar herramientas de monitoreo disponibles para la oficina de TI, que realice:*
 - *Transferencias de datos mensual y/ Transacciones de Almacenamiento mensual.*
 - *Monitoreo de los principales componentes en los servidores (Utilización de CPU, Memoria, Discos lógicos y físicos).*
 - *Estado de procesos, servicios y aplicaciones.*
 - *Monitoreo de los logs de eventos de los servidores, diferenciados entre logs de usuarios regulares y logs propios de la administración.*
 - *Monitoreo básico de la seguridad en los sistemas, el cual debe considerar como mínimo Denegación de Servicio, Validación de reputación del visitante, Protección SSH / Telnet / Puertos FTP (desactivación de los puertos como SSH, FTP y Telnet).*
 - *Monitoreo del respaldo de la información que ha sido almacenada durante el mes.*
 - *Monitoreo de los sistemas el cual debe considerar como mínimo el estado de los servicios publicados (iniciado, detenido).*



⁶ Absolución de consulta N°35 del participante AMERICA MOVIL PERU S.A.C.



Tribunal Constitucional

A excepción de⁷:

1. Cuando la información en cuestión haya sido de difusión o acceso público;
2. Cuando la información en cuestión haya sido publicada antes de haber sido puesta a disposición del postor;
3. Cuando la información en cuestión ya obre en poder del postor y no esté sujeta a cualquier otro impedimento o restricción que le haya sido puesto de manifiesto;
4. Cuando la información en cuestión haya sido recibida a través de terceros sin restricciones y sin que implique incumplimiento del Contrato;
5. Cuando la información en cuestión haya sido independientemente desarrollada por el postor, siempre que no se hubiese utilizado para ello otra información confidencial; o
6. Cuando la información en cuestión deba ser revelada a alguna autoridad autorizada para dar cumplimiento a una orden de naturaleza judicial o administrativa, bastando para ello informar a la Entidad la recepción de dicha orden.



7.5. Propiedad intelectual

Todas las publicaciones que el Tribunal realice en su portal web son de propiedad intelectual del Tribunal Constitucional, quedando prohibido el uso con fines comerciales, por parte del proveedor del servicio.

7.6. Medidas de control durante la ejecución contractual

El Proveedor deberá presentar un informe mensual sobre las actividades de naturaleza agresiva que haya sufrido el portal durante el periodo transcurrido, realizando las recomendaciones que considere necesarios para evitar o mitigar ataques de Denegación de Servicios o intentos de intrusión al portal.

7.7. Conformidad de la prestación

La conformidad de la prestación del servicio deberá ser realizada por la Oficina de Tecnologías de la Información.

7.8. Forma de pago

El ciclo de facturación del servicio solicitado deberá ser mensual y deberá efectuarse en moneda nacional de acuerdo a ley, y en forma mensual.

En el caso que la facturación se efectúe en moneda extranjera, el pago se efectuará en moneda nacional al tipo de cambio (venta oficial) emitida por la Superintendencia de Banca, Seguros y AFP a la fecha de la prestación del precio de la oferta, por parte del proveedor.

⁷ Absolución a la consulta N° 26 del participante AMERICA MOVIL PERU S.A.C.



Tribunal Constitucional

7.9. Otras penalidades

De conformidad con el artículo 163 del Reglamento de la Ley de Contrataciones del Estado se establecen las siguientes penalidades:

Indisponibilidad del servicio contratado en hosting y servicios Cloud.	Por cada 30 minutos de servicio caído en el día	0.5 % UIT
Indisponibilidad o degradación de los servicios en la plataforma Cloud mayor a 1 hora	Por cada 60 minutos de servicio caído en el día	1 % UIT
Tiempo de respuesta en soporte técnico de la plataforma Cloud	Por cada 30 minutos de retraso, luego de haber comunicado mediante llamada, correo electrónico al Centro de atención.	0.5 % UIT

7.10. Sistema de contratación

A suma alzada.

8. Requisitos de Calificación





Tribunal Constitucional

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/. 400.000.00 (Cuatrocientos Mil con 00/100), 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.

En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/. 50,000.00 (Cincuenta Mil con 00/100 soles), por la venta 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. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa. Se consideran servicios similares a los siguientes;

- ✓ Alojamiento de hosting profesional y/o servidores virtuales
- ✓ Servicios de continuidad de negocio basados en respaldo en la nube
- ✓ Seguridad en la Nube y servicios de Cyberseguridad.
- ✓ Soporte multinivel o cualquier despliegue derivado de la computación en la nube en cualquiera de sus 3 niveles.
- ✓ Servicio de Hosting
- ✓ Hosting de servicio
- ✓ Servicio de Infraestructura en la Nube
- ✓ Servicio de Web Hosting y/o Servicio de almacenamiento de información a través de la nube.

Además de⁸;

- ✓ Servicios de Cloud en general y/o servicios de Project online profesional y Microsoft 365 estándar y/o Servicio de infraestructura y plataforma en la nube (CLOUD COMPUTING) para el PGRH y/o Servicio de infraestructura y plataforma en la nube y/o Servicio de Suscripción a plataforma de correo en nube y/o Servicio De Project online profesional y Microsoft 365 business standard, Servicios de Cloud (SaaS y/o IaaS) y/o nube publica y/o housing o colocation y/o data center y/o máquinas virtuales y/o servicios cloud varios y/o Servicio Nube Publica Huawei Cloud, ⁹Servicio Administrado de Infraestructura en la Nube y/o hosting y/o housing y/o servicio híbrido (housing y hostin).

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 vócher 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 pago¹⁰, correspondientes a un máximo de veinte (20) contrataciones.

En caso los postores presenten varios comprobantes de pago para acreditar una sola





Tribunal Constitucional



contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso sólo 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, sólo 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

⁸ Absolución de consulta N° 30 del participante AMERICA MOVIL PERU S.A.C.

⁹ Absolución de consulta N° 47 del participante AMERICATEL PERU S.A.

¹⁰ 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".



Tribunal Constitucional

- *Al calificar la experiencia del postor, 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 objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las 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".*

Importante

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*
- *El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de estos. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*
- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*



ANEXO I

1.- SERVIDOR VDS DE PRODUCCIÓN CLOUD LAMP - PLATAFORMA COMO SERVICIO - PAAS

Hardware	Software	Seguridad	Soporte técnico
Procesador Intel Xeon 8 cores de 3.5 GHz 8va Generación o superior	Sistema operativo cloud Linux Alma, última versión estable.	Servicio de backup de alta disponibilidad según ANS (DR-Recuperación de Desastres)	<ul style="list-style-type: none"> - Soporte técnico de 24 x 7 x 365. - Soporte ilimitado para generación de tickets. - Soporte ilimitado para número de atenciones por mes. - Asignación de gerente de cuentas para gestión de soporte. - Backup en servidor Externo. - Monitoreo proactivo 24/7/365 de los principales componentes en los servidores (Utilización de CPU, Memoria, Discos lógicos y físicos).
Memoria RAM DDR4 32 GB	Antivirus, antispam		
Disco duro para S.O 2 TB SSD o NMVe	Panel de Control (Cpanel), WHM	Multi Certificados SSL (Cifrado en la capa de transporte) durante la vigencia del contrato para cada dominio y subdominio.	
Disco duro para Backup de archivos 8TB SSD			
Tarjeta de red 1000 Mbps	Certificado SSL/TLS Certificado SSL WILDCARD		
Ancho de banda de 10,000 GB Mensual	Cuentas FTP, SFTP, SSH Ilimitadas		
Estabilidad y disponibilidad 99.975 ⁸ % de la red	Soporte para:	Deberá contar con WAF	
Servidor con IP dedicado	CGI-BIN, Perl, Python		
VDS privado 100 %	PHP w / Zend y eAccelerator		
	Imagemagick w / GD.		
	Mailman, GNU Mailing List Manager (Moderador de envío a listas de correo)		
	soportar Base de Datos:		
	MySQL (MariaDB) (Versión 10.6.17)		
	Consultas MySQL Hasta 100 mil x hora en la edición comunitaria.		
	PostgreSQL y Python		
	Apache 2.4.58		
	phpMyAdmin versión: 5.2.1		
	full control (reboot)		
	Debe permitir realizar		
	-Dominios propios		
	- Sub Dominios ilimitados		

⁸ Se absuelve consulta N°57 del participante AMERICATEL PERU S.A.

2. -SERVIDOR VDS DE PRODUCCIÓN CLOUD TOMCAT JAVA - PLATAFORMA COMO SERVICIO – PAAS.

Hardware	Software	Seguridad	Soporte técnico
Procesador Intel Xeon 8 cores de 3.5 GHz 8va Generación o superior	Sistema operativo cloud Linux Alma, versión estable	Servicio de backup de alta disponibilidad según ANS (DR-Recuperación de Desastres)	<div>- Soporte técnico de 24 x 7 x 365.</div> <div>- Soporte ilimitado para generación de tickets.</div> <div>- Soporte ilimitado para número de atenciones por mes.</div> <div>- Asignación de gerente de cuentas para gestión de soporte.</div> <div>- Backup en servidor Externo.</div> <div>- Monitoreo proactivo 24/7/365 de los principales componentes en los servidores (Utilización de CPU, Memoria, Discos lógicos y físicos).</div>
Memoria RAM DDR4 64 GB	Antivirus, antispam	Multi Certificados SSL (Cifrado en la capa de transporte) durante la vigencia del contrato para cada dominio y subdominio	
Disco duro para S.O 8 TB SSD o NMVe	Panel de Control (Cpanel), WHM		
Disco duro para Backup de archivos 12 TB SSD	Software RAID 0		
Tarjeta de red 1000 Mbps	Certificado SSL/TLS Certificado SSL WILDCARD	Deberá contar con WAF	
Ancho de banda de 10,000 GB Mensuales	Cuentas FTP, SFTP, SSH Ilimitadas		
Estabilidad y disponibilidad 99.975 ⁹ % de la red	Soporte para:		
Servidor con IP dedicado	CGI-BIN, Perl, Python		
VDS privado 100 %	PHP w / Zend y eAccelerator		
	Imagemagick w / GD.		
	WAR Deployment		
	soportar Base de Datos:		
	MySQL (MariaDB) (Versión 10.6,17)		
	Consultas MySQL Hasta 100 mil x hora en la edición comunitaria.		
	PostgreSQL y Python		
	phpMyAdmin versión: 5.2.1		
	Apache 2.4.58		
	Full control		
	Apache Tomcat 7.0.67		
	Debe permitir realizar		
	-Dominios propios		
	- Sub Dominios ilimitados		



⁹ Se absuelve consulta N°57 del participante AMERICATEL PERU S.A.

3. SERVIDOR VDS DE DESARROLLO CLOUD TOMCAT JAVA - PLATAFORMA COMO SERVICIO - PAAS (SERVIDOR DEDICADO DE GAMA ALTA)

Hardware	Software	Seguridad	Soporte técnico
Procesador Intel Xeon 4 cores de 3.5 GHz 8va Generación o superior	Sistema operativo cloud Linux Alma, versión estable	Servicio de backup de alta disponibilidad según ANS (DR-Recuperación de Desastres)	<ul style="list-style-type: none">- Soporte técnico de 24 x 7 x 365.- Soporte ilimitado para generación de tickets.- Soporte ilimitado para número de atenciones por mes.- Asignación de gerente de cuentas para gestión de soporte.- Backup en servidor Externo.- Monitoreo proactivo 24/7/365 de los principales componentes en los servidores (Utilización de CPU, Memoria, Discos lógicos y físicos).
Memoria RAM DDR4 32 GB	Antivirus, antispam		
Disco duro para S.O 2 TB SSD o NMVe	Panel de Control (Cpanel), WHM	Multi Certificados SSL (Cifrado en la capa de transporte) durante la vigencia del contrato	
Disco duro para Backup de archivos 2 TB SSD			
Tarjeta de red 1000 Mbps	Certificado SSL/TLS Certificado SSL WILDCARD		
Ancho de banda de 10,000 GB Mensual	Cuentas FTP SFTP, SSH Ilimitadas (24x7)		
Estabilidad y disponibilidad 99.975 ¹⁰ % de la red	Soporte para:		
Servidor con IP dedicado	CGI-BIN, Perl, Python		
VDS privado 100 %	PHP w / Zend y eAccelerator		
	Imagemagick w / GD.		
	WAR Deployment		
	soportar Base de Datos:		
	MySQL (MariaDB) (Versión 10.6)		
	Consultas MySQL Hasta 100 mil x hora en la edición comunitaria.		
	PostgreSQL y Python		
	phpMyAdmin versión: 5.2.1		
	Apache 2.4.58		
	Apache Tomcat 9.0.75		
	Full control		
	Debe permitir realizar		
	-Dominios propios		
	- Sub Dominios ilimitados		



¹⁰ Se absuelve consulta N°57 del participante AMERICATEL PERU S.A.



Tribunal Constitucional

4. LICENCIA DE FIREWALL CLOUD (WAF) EN LA CAPA DE APLICACIÓN 02 LICENCIAS

Requerido para la protección del sitio web institucional. Se describe a continuación los tipos de incidentes que deberá cubrir y cumplir con las siguientes directivas de la industria: ISO27001 / CVE / CWE / ATT&CK / NIST / OWASP Top 10¹¹.

Características		Cantidad		Soporte
Firewall (WAF)	<ul style="list-style-type: none">- Mitigación de emergencia contra ataques avanzados amplificados DDoS (Capa 3 y 4) Mitigación de ataques DDoS (Denegación de servicio con una protección de volumetría superior a 150GB por segundo).- CDN (Red de entrega de contenidos)- Secuencia de comandos (XSS).- Referencias a objetos inseguras.- Suplantación de identidad mediante credenciales rotas.- Redirección a sitios fraudulentos.- Deficiencia en la configuración de seguridad.- Almacenamiento inseguro de datos criptográficos.- Insuficiencia en restricción de acceso URL.- Insuficiencia en la capa de transporte.- Redireccionamientos inválidos.- Bloqueo de ataques dirigidos.- Bloqueo de ataques vía backdoors- Bloqueos de ataques por fuerza bruta.- Filtro de tráfico malicioso botnet.- Control de blacklist en buscadores y spam.- Reparación de vulnerabilidades en tiempo real.- Prevención de ataques de día cero.- Optimización e incremento en un 50% en la velocidad del website y reportes de incidencias.- Soporte para filtro por países.- Soporte de filtro para los tops 10 OWASP, estos deben ser personalizables.- Soporte para creación de reglas personalizadas.- Soporte de reglas por backend, ruta o dominio bajo el mismo Balanceador.- Soporte para modo de captura o modo de bloqueo de request maliciosos.- Soporte de reportes detallados de request para detección de falsos positivos.	- Licencia 2 PARA DOS DOMINIOS	1 licencia Enterprise con	<ul style="list-style-type: none">- Configuración de políticas de firewall para vds del hosting web y servidores vps- Lanzamiento de Parches de Seguridad para Ataques de Día Zero.- Actualizaciones constantes de Parches y reglas del servidor para proteger su sitio.- Bloqueo de ataques DDoS- Mitigación de ataques de Denegación de Servicio (DDoS) con red global Anycast y firewall de aplicaciones web (WAF).- Parches de vulnerabilidades y bloqueo de amenazas con sistemas de prevención de intrusiones integrado en el WAF.
			- Soporte 1 Dominio - soporte de 33 subdominios	<ul style="list-style-type: none">- Páginas protegidas- Protección de capa adicional con acceso autenticado para determinadas páginas confidenciales habilitando la función Página protegida.- Capacidad de agregar contraseñas, CAPTCHA, 2FA (a través de Google Authenticator) o lista de IP permitidas.- Lista de direcciones IP permitidas- Gestión de direcciones de IP en listas corporativas.- Restricción de paneles de administración.- Detección de firma- Análisis de todo el tráfico web HTTP/HTTPS- Inspección heurísticas basadas en firmas- Bloqueo de solicitudes maliciosas y patrones de ataque.
			1 licencia pro 1 dominio	<ul style="list-style-type: none">- Protección de sitio web contra códigos maliciosos- Sistema de prevención de intrusiones (IPS)- Bloqueo de bots y ataques automatizados- Bloqueo de ataques DDoS de capa 3, 4 y 7.- Ancho de banda seguro durante los ataques- Detención de ataques basados en volumen y protocolos- Detención de ataques a aplicaciones (capa 7)- Detención de ataques de fuerza bruta y el descifrado de contraseñas.- Prevención de ataques de robots- Limite los inicios de sesión a una dirección IP o rango específico

¹¹ Se absuelve consulta N°62 del participante AMERICATEL PERU S.A.



Tribunal Constitucional

5. ESCÁNER DE SEGURIDAD WEB DAST: 16 LICENCIAS

Se requiere una solución de escáner de análisis y reparación de vulnerabilidades para sitios web, BBDD y cumplir con las siguientes directivas de la industria: ISO27001 / CVE / CWE / ATT&CK / NIST / OWASP Top 10¹². Se describe a continuación sus características:

Características	Cantidad	Soporte
<p>- Control de blacklist en buscadores y spam.</p> <p>- Análisis de código malware inserto.</p> <p>- Herramienta inteligente para remover automáticamente el 98% malware conocido.</p> <p>- Análisis de aplicación y variantes de ataque.</p> <p>- Análisis de red y puertos abiertos.</p> <p>- Análisis de CMS, Plugins y otros ficheros sospechosos.</p> <p>- Análisis de código obsoleto o desfasado.</p> <p>- Análisis de validación de certificados SSL.</p> <p>- Análisis de otras advertencias de seguridad.</p> <p>- Administración con Panel de Control Centralizado.</p>	16 licencias scanner web DAST Pro.	<p>- Soporte técnico de 24 x 7 x 365.</p> <p>- Soporte ilimitado para generación de tickets.</p> <p>- Soporte ilimitado para número de atenciones por mes.</p> <p>- Asignación de gerente de cuentas para gestión de soporte.</p> <p>- Monitoreo proactivo 24/7/365</p> <p>Monitoreo de los principales componentes en los servidores (Utilización de CPU, Memoria, Discos lógicos y físicos).</p>
<p>- Verificación de nombre de dominio</p> <p>Verificación la propiedad del dominio mediante la carga de archivos o el registro DNS TXT</p> <p>- Escaneo SSL</p> <p>Verificación si un certificado SSL, una capa importante en el cifrado web, está instalado y activo en el dominio.</p> <p>- Análisis de malware</p> <p>Análisis de los sitios web desde el punto de vista del usuario (de afuera hacia adentro) para detectar signos de malware y enlaces antes de que lo hagan los motores de búsqueda y potencialmente podría dañar o dañar el sitio web del usuario.</p> <p>- Análisis de spam</p> <p>Análisis de la IP y el dominio de un sitio web comparándolos con las principales listas negras de correo electrónico y bases de datos de spam para comprobar si figura como spammer, lo que ayuda a garantizar la capacidad de entrega del correo electrónico.</p>		
<p>- Escaneo de inyección SQL</p> <p>Escaneo de penetración en un sitio con métodos de inyección SQL para encontrar vulnerabilidades que impidan la fuga de datos a los piratas informáticos.</p> <p>- Escaneo de secuencias de comandos entre sitios (XSS)</p> <p>Búsqueda de vulnerabilidades que inserten scripts maliciosos destinados a robar datos de los visitantes o engañarlos para que proporcionen datos a terceros.</p> <p>- Puntuación de riesgo de composición y estructura del sitio web</p> <p>Se analizan más de 500 variables diferentes en tres categorías clave (número de páginas, tipo de CMS, cantidad de visitantes) y se proporciona una evaluación de riesgo alto, medio o bajo para ayudarle a comprender dónde es vulnerable y las opciones disponibles para reducirlo.</p>		
<p>- Escaneo de plataforma</p> <p>Comprobación de las aplicaciones comunes de sitios web de CMS para verificar que estén actualizadas y libres de vulnerabilidades.</p> <p>- Escaneo inteligente</p> <p>SMART (Herramienta de eliminación y alerta segura de malware) realiza un escáner de malware de adentro hacia afuera para detectar códigos maliciosos incrustados en su servidor. Funciona junto con un escáner externo para realizar un análisis completo de las amenazas de su sitio web.</p> <p>- Modificación personalizada de configuración SMART</p> <p>Modificación de la configuración SMART en el panel.</p> <p>- Advertencia de actualización de Parches, temas o plugins de vulnerabilidades encontradas</p> <p>Notificaciones por correo electrónico sobre cualquier vulnerabilidad encontrada por nuestro análisis completo.</p>		

ESCANER DE
SEGURIDAD
WEB DAST



¹² Se absuelve consulta N°63 del participante AMERICATEL PERU S.A



Tribunal Constitucional

6. SERVICIO DE RESPALDO Y BACKUPS EN LINEA: 10 Licencias

Se requiere una solución respaldo único y centralizado para los backups seguros de la nube.

Seguridad	Cantidad licencias	Soporte técnico
Entornos Soportados: <ul style="list-style-type: none">• Ordenadores Windows 7 o superior• Servidores Windows Server 2008 o superior, Linux, MAC, Dispositivos móviles, VM. Almacenamiento 10 TB		
Características: <ul style="list-style-type: none">• Backup Automático (A nivel de fichero, discos y configuración BMR)• Backup inteligente Incremental/Bloques diferenciales/Delta.• Backup en caliente y en modo servicio.• Backup con tecnología de duplicación de datos.• Análisis de vulnerabilidades y vector de ataque del parque informático/Agentes instalados.• Protección contra ataques Ransomware y Minería de datos.• Protección Antivirus/Antimalware bajo demanda con detección de archivos infectados en el cloud.• Protección contra ficheros corruptos (Retenciones)• Protección de aplicaciones en ejecución.• Gestión de inventario de hardware.• Acceso consola web securizada a los datos y notificaciones de gestión.	10 licencias de respaldo en línea , y será distribuido de la siguiente manera: <ul style="list-style-type: none">- 6 licencias para los VDS dedicados.- 1 licencia para estación de escritorio físico.- 1 licencia de seguridad avanzada con lo siguiente: Protección antivirus y antimalware con detección basada en firmas locales (con protección en tiempo real), Prevención contra explotación de ataques de día cero, Filtrado de URL, Gestión de firewall de endpoint, Copia de seguridad forense, Análisis de copias de seguridad en busca de malware, Recuperación segura, Lista blanca corporativa, Análisis de copia de seguridad centralizado para malware y Borrado remoto.- 1 licencia de copias de seguridad avanzada con lo siguiente: Oracle DB, SAP HANA, Mapa de protección de datos, Protección de datos continua, Certificación de las copias de seguridad, Copia Usuarios de Microsoft 365, Copia de Google Workspace y Copias de seguridad en caliente de MariaDB.	<ul style="list-style-type: none">- Soporte asistencia remota securizada multinivel y multicanal 24/07/365- Soporte ilimitado para generación de ticket.- Soporte ilimitado para número de atenciones por mes.- Asignación de gerente de cuentas para gestión de soporte.- Backup de configuración Servidor Externo.- Monitoreo proactivo 24/7/365
Características: <ul style="list-style-type: none">• Backup Automático (A nivel de fichero, discos y configuración BMR)• Backup inteligente Incremental/Bloques diferenciales/Delta.• Backup en caliente y en modo servicio.• Backup con tecnología de duplicación de datos.• Análisis de vulnerabilidades y vector de ataque del parque informático/Agentes instalados.• Protección contra ataques Ransomware y Minería de datos.• Protección Antivirus/Antimalware bajo demanda con detección de archivos infectados en el cloud.• Protección contra ficheros corruptos (Retenciones)• Protección de aplicaciones en ejecución.• Gestión de inventario de hardware.• Acceso consola web securizada a los datos y notificaciones de gestión.		
Unidades <ul style="list-style-type: none">• Tráfico de datos ingreso/salida ilimitados.• Informes de cumplimiento y mapa de protección de datos estándar.• Backup en modo Offline- opcional• Restauración en línea de los datos guardados		
Almacenamiento y seguridad: <ul style="list-style-type: none">• Cifrado de los datos de principio a fin (Transferencia, almacenamiento y restauración) Basado en el marco NIST• Certificación ISO 9001 (Estándar para sistemas de gestión de calidad)• Certificación ISO 22301 (Estándar para sistemas de gestión para la continuidad de negocio)• Certificación ISAE 3402 Tipo 2 (Estándar Internacional de contratos para seguros y procesos internos)• Cumplimiento de la normativa internacional RGPD (Reglamento General de Protección de Datos)• Cumplimiento de la Normativa local LPDP (Ley de Protección de Datos Personales)• HIPAA para la protección y confidencialidad entornos de salud/médicos.• Datacenter redundantes Tier III+• Certificación ISO 27001 (Estándar para sistemas de gestión de seguridad de la información)• Copias redundantes de datos con acceso físico altamente seguro		





Tribunal Constitucional

7. SERVICIO COMPARTICIÓN SEGURA DE ARCHIVOS EN LA NUBE

Se requiere una solución para la compartición de archivos para la finalidad pública:

CARACTERISTICAS		Cantidad	Soporte
SERVICIO COMPARTICIÓN SEGURA DE ARCHIVOS EN LA NUBE	<ul style="list-style-type: none">- Permitir el seguimiento de los derechos del usuario, de la clasificación del contenido y de los flujos de trabajo en toda la empresa.- Alertas automáticas de posibles infracciones.- Método de autenticación sólido que se adecúa a las empresas, como SAML 2.0 (SSO), LDAP, biometría en dispositivos móviles, contraseñas temporales de un solo uso basadas en el tiempo (TOTP) y módulos de seguridad de hardware (HSM).- Gestión de repositorio seguro para contenido confidencial y restringido.- Los postores deberán adjuntar a su propuesta las certificaciones de seguridad de la información ampliamente reconocido y basado en estándares internacionales que cumplan con los "Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano"¹³.- Protección de los riesgos de seguridad provenientes de terceros países- Cumplimiento de las normativas locales en materia de protección de datos- Uso de interfaz intuitiva y perfectamente diseñada que no ralentiza a los equipos para trabajar con aplicaciones móviles, web y de escritorio fáciles de usar.	10 licencias	<ul style="list-style-type: none">- Soporte técnico de 24 x 7 x 365.- Soporte ilimitado para generación de tickets.- Soporte ilimitado para número de atenciones por mes.- Asignación de gerente de cuentas para gestión de soporte.- Monitoreo proactivo 24/7/365
	<ul style="list-style-type: none">- Compartición de contenido directamente a través de cualquier aplicación de productividad, como Microsoft Teams, Microsoft Outlook o Salesforce, gracias a conectores seguros y cifrados de extremo a extremo.- Actualizaciones a las últimas versiones de los archivos sincronizados siempre disponible para todos, en el espacio de trabajo, escritorio y aplicaciones móviles.- Garantizar de una mayor seguridad con restricciones de acceso estricto y cifrado de seguridad en la capa de transporte (TLS)- Automatización de transferencias, etiquetado de confidencialidad y opciones para borrar dispositivos tras varios intentos de acceso fallidos.- Creación y coedición de documentos en MS Word, Excel, PowerPoint y otros en tiempo real, usando una instancia de Microsoft 365 o equivalente alojada de forma segura.- Buscador de archivos con potentes filtros y funciones de búsqueda- Creación de carpetas seguras y compartidas y centros multimedia personalizados- Control del uso de los archivos, recepción de informes de uso, fechas de vencimiento,- Asignación de derechos de edición e impresión,		
	<ul style="list-style-type: none">- Gestión de archivos automatizada- Recuperación de archivos o carpetas perdidas,- Comparación de versiones y eliminación permanente de archivos desde todas las ubicaciones con un solo clic.- Aplicación de política de cumplimiento de normativas con controles, permisos, monitorizaciones y una pista de auditoría completa.- Soluciones globales que permiten trabajar de forma conjunta desde cualquier sitio y a cualquier hora, desde el móvil e incluso fuera de línea, con documentos sincronizados.- Disponibilidad en español.- Colaboración usando Microsoft Word, Excel y PowerPoint utilizando una instancia de Microsoft 365 o equivalente alojado de forma segura.- Compartición de archivos con enlaces en Microsoft Outlook.		
	<ul style="list-style-type: none">- DataRoom con 200 GB de espacio para compartición mínimo.- Administración de usuarios.- Edición de documentos Office online.- Trabajo con carpetas compartidas y colaborativas.- Visualización de informes sobre el uso de los archivos.- Uso de herramientas de transferencia avanzada.- Trazabilidad específica de las comparticiones y reportes de auditoría.		

¹³ Absolución a la consulta N°01 del participante AMBER CLOUD INC S.A.C



Tribunal Constitucional

Anexo II

ACUERDO DE CONFIDENCIALIDAD PARA PROVEEDORES

Conste en el presente documento privado, el acuerdo de confidencialidad para el bien/servicio brindado correspondiente a por parte de....., en adelante **EL PROVEEDOR**, con número de RUC....., y con domicilio en.....; y por la otra, el Tribunal Constitucional, en adelante **EL CONTRATANTE**, han acordado lo siguiente:

EL PROVEEDOR se precisa a mantener y guardar estricta reserva y absoluta confidencialidad sobre las características, términos y condiciones del presente contrato, incluyendo información objeto de derecho de autor, patentes, técnicas, modelos, invenciones, know – how, proceso, algoritmos, programas, ejecutables, investigaciones, detalles de diseño, información financiera, lista de clientes inversionistas empleados, relaciones de negocio y contractuales, pronósticos de negocios, planes de mercadeo y cualquier información revelada sobre terceras personas.

EL PROVEEDOR se compromete a respetar y aplicar en la ejecución del servicio del presente contrato, las políticas, procedimientos, estándares y controles de seguridad de la información establecidos por **EL CONTRATANTE**, los mismos que declara conocer y aceptar.

EL PROVEEDOR deberá proteger los activos de información ⁽¹⁴⁾ del **CONTRATANTE**, asimismo **EL PROVEEDOR** deberá respetar las políticas de acceso no autorizado, pérdida, modificación y/o destrucción, falsificación, robo, uso indebido y/o divulgación de los activos de información del Tribunal Constitucional.

EL PROVEEDOR se obliga a mantener y a guardar estricta reserva y absoluta confidencialidad por sus miembros autorizados de su equipo de trabajo todos los documentos e información del **CONTRATANTE** a los que tenga acceso en ejecución del presente contrato. Se entiende que la obligación asumida por **EL PROVEEDOR** está referida no solo a los documentos e información señalados como “confidenciales” sino a todos los documentos e informaciones que en razón del presente contrato o vinculado con la ejecución del mismo, pueda ser conocida por cualquier medio por **EL PROVEEDOR**. En consecuencia, **EL PROVEEDOR** deberá abstenerse de divulgar tales documentos, conversaciones, acuerdos de reuniones y comentarios que como parte de la función son de uso conocimiento, sea en forma directa o indirecta.

EL PROVEEDOR solo podrá revelar al personal que estrictamente sea necesario para la realización de las actividades materia del presente contrato, los documentos e informaciones a los que se refiere el numeral precedente.

En el caso que **EL PROVEEDOR** fuera requerido por alguna autoridad administrativa o judicial para revelar la información y/o documentación a la que se refiere la presente cláusula, **EL PROVEEDOR** deberá notificar anticipadamente al **CONTRATANTE** para que éste adopte las medidas que considere necesarias para proteger la confidencialidad de la información.

Se deja expresamente establecido que el deber de confidencialidad opera desde la fecha de suscripción del presente Contrato y se mantendrá vigente incluso hasta cinco (5) años posteriores a la extinción del mismo.

EL PROVEEDOR se compromete a devolver todo activo (software, documentación, equipos, tarjetas de acceso, entre otros) que le haya proporcionado **EL CONTRATANTE** para el desempeño de sus funciones, al momento de resolución o término del presente contrato, sin que sea necesario de éste se lo requiera.

¹⁴ () Datos/Información, Aplicaciones -Software, Equipo Informático - Hardware, entre los principales



Tribunal Constitucional

Este acuerdo solo podrá ser modificado o darse por terminado con el consentimiento expreso por escrito de **EL CONTRATANTE**

Toda información administrada es de propiedad exclusiva de **EL CONTRATANTE**. En consecuencia, **EL PROVEEDOR** no utilizará información para su propio uso.

El incumplimiento de las obligaciones que asume **EL PROVEEDOR** en las cláusulas precedentes constituye causal de resolución automática y de pleno derecho del presente contrato, de conformidad con lo previsto en el artículo 1430° de Código Civil, sin perjuicio de la obligación del **PROVEEDOR** de pagar al **CONTRATANTE** la indemnización correspondiente.

El presente Acuerdo requiere para su validez y perfeccionamiento la firma de las partes.

Por constancia, y en señal de aceptación, se firma el presente acuerdo, por las partes que en él han intervenido, a los... días del mes de.....

El PROVEEDOR

Tribunal Constitucional

