Generando Energía con Responsabilidad Social

TÉRMINOS DE REFERENCIA

SERVICIO DE BACKUP EN NUBE PARA LOS ACTIVOS DE INFORMACION (SISTEMAS DE INFORMACIÓN) DE EGASA

Área Usuaria o área técnica estratégica	*División de Tecnologías de Información y Comunicaciones*
Objetivo/Meta del POI vinculado	*Fortalecimiento del plan de sistemas de información*
Requerimiento incluido en CMN	SI

I. FINALIDAD PÚBLICA

Brindar una infraestructura tecnológica escalable y segura en la nube, que permita el almacenamiento automatizado y descentralizado de respaldos de los sistemas de información de EGASA, independiente de su ubicación física. Este servicio busca garantizar la disponibilidad de espacio para contingencias de almacenamiento, y facilitar el cumplimiento de buenas prácticas de continuidad operativa, contribuyendo a la modernización de la plataforma tecnológica institucional.

II. OBJETIVO DE LA CONTRATACIÓN

Contratar un servicio de suscripción de licencias de almacenamiento en la nube, que permita contar con una solución de respaldo remoto, seguro y escalable, destinada a alojar respaldos automatizados de activos de información institucional. Este servicio tiene como fin garantizar la disponibilidad geográfica de los datos respaldados y fortalecer la estrategia de contingencia tecnológica de EGASA.

III. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

Se requiere contratar el servicio de Backup en la Nube para los Activos de Información de EGASA.

IV. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

4.1 Descripción del servicio a contratar

Ítem	Descripción del servicio
01	Servicio de Licenciamiento de Backup en la nube 05 TB.

4.2 Atributos del sistema

- El contratista deberá ofrecer como almacenamiento en nube de 1 Tb hasta 05 Tb durante la suscripción anual de la licencia.

a) Características de los centros de datos y la infraestructura física:

- El servicio debe tener al menos cuatro centros de datos ubicados en diferentes ubicaciones geográficas, a una distancia mínima de 160 kilómetros entre ellos.
- Todos los centros de datos deben estar ubicados en países de conformidad con el artículo 45(1) del Reglamento General de Protección de Datos (RGPD) de la Unión Europea.
- Todos los centros de datos deben estar ubicados en países de acuerdo con el Capítulo V de la Ley Brasileña No.13.709 del 14 de agosto de 2018 (Ley General de Protección de Datos).
- La entidad responsable de administrar los centros de datos debe ser miembro del Marco del Escudo de privacidad UE-EE. UU.
- Los centros de datos deben ser auditados y cumplir con las pautas de seguridad PCI DSS (Payment Card Industry Data Security Standards).
- Los centros de datos deben ser auditados y cumplir con las normas ISO 9001:2015 e ISO/IEC 27001:2013.
- Si los centros de datos están ubicados en los Estados Unidos, deben ser auditados y cumplir con las pautas de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por sus siglas, health insurance portability and accountability act).
- Si los centros de datos están ubicados en Europa, deben ser auditados y cumplir con las directrices de OHSAS 18001:2007.
- Todos los centros de datos deben ser auditados y contar con las certificaciones SOC 1 Tipo 2 y SOC 2 Tipo 2, cumpliendo con las normas SSAE 16 / ISAE 3402, equivalentes a la clasificación Tier IV.
- Si los centros de datos están ubicados en los Estados Unidos, deben ser auditados y cumplir con los requisitos de NIST 800-53 y fisma (Ley Federal de Administración de la Seguridad de la Información).
- Los centros de datos deben estar en edificios no relacionados, para una mayor privacidad y anonimato sobre su ubicación.
- El acceso físico a los centros de datos debe realizarse exclusivamente a través de medios de seguridad biométrica.
- Los centros de datos deben tener las siguientes medidas de seguridad adicionales con respecto al acceso físico:
    - Muros altos.
    - Videovigilancia de circuito cerrado.
    - Guardias de seguridad.

- Detectores de movimiento.
- Puertas dobles blindadas, tipo mantrap.

- Los centros de datos deben tener enlaces a Internet redundantes con un ancho de banda de al menos 10 Gbps.
- Los centros de datos deben ser monitoreados y administrados en un 24/7/265 a través de un NOC (Network Operation Center).
- Para una mayor disponibilidad, los servicios ofrecidos deben depender de la redundancia de servidores / nodos.
- Los nodos de almacenamiento empleados por el servicio ofrecido deben basarse en la tecnología de auto reparación para una mayor resistencia a los errores.
- El servicio prestado debe tener un Acuerdo de Nivel de Servicio (SLA) de al menos 99.995% de disponibilidad.
- El disco duro y/o las unidades de estado sólido removidas para mantenimiento, reparación o reemplazo deben tener su contenido eliminado de acuerdo con NIST 800-88 rev.1 ("Directrices para la desinfección de medios").
- En caso de cancelación del servicio y/o eliminación de la cuenta, los datos deben ser eliminados inmediatamente, quedando permanentemente inaccesibles a partir de entonces.

b) Prácticas y procesos de seguridad de la entidad responsable del servicio:

- El acceso a los sistemas de producción (incluidas las aplicaciones, las redes, las bases de datos y los datos conexos, los sistemas operativos y los servidores) y a la información de los clientes debe limitarse a las personas debidamente autorizadas.
- El acceso físico a las instalaciones del centro de datos, equipos informáticos, medios y documentos debe limitarse a las personas autorizadas.
- La configuración inicial del entorno debe hacerse de forma completa y precisa.
- Las funciones y responsabilidades dentro de la organización deben planificarse, ejecutarse y gestionarse sistemáticamente.
- El acceso a los cortafuegos y dispositivos de red debe limitarse al personal autorizado y los datos de los clientes deben estar protegidos contra el acceso no autorizado desde Internet.
- Las implementaciones y/o modificaciones de los elementos del sistema de producción deben ser aprobadas, documentadas, probadas y desplegadas de manera completa y precisa.
- El servicio de soporte técnico al cliente debe estar disponible y responder a su debido tiempo a cualquier problema o pregunta relacionada con la prestación del servicio.

- Las pruebas de vulnerabilidad deben ser realizadas por terceros de forma continua y automatizada.
- Debe haber una metodología integral para las aplicaciones de parches y las nuevas versiones en los sistemas de producción.
- La supervisión de la disponibilidad del servicio y los acuerdos de nivel de servicio (SLA) deben ser continuos y distribuidos.
- Verificación en tiempo real para garantizar que los datos leídos son correctos antes de que se ponen a disposición del cliente.
- Opción de centro de datos múltiple para la protección de datos con redundancia geográfica, lo que garantiza la protección contra todos los incidentes, incluida la destrucción total del centro de datos.
- Control de cambios y gestión automatizada de la configuración para minimizar los riesgos y los eventos de indisponibilidad derivados de los cambios.
- Segregación interna de responsabilidades, adoptando el modelo de privilegio mínimo requerido.
- Verificación de antecedentes profesionales de todos los empleados.
- Revisión y auditoría continuas de registros y registros de seguridad.
- Validación del cliente y modelo de administración delegada para mitigar los riesgos de pretexto/phishing.

c) Características de seguridad implementadas por el componente de software de la solución:

- Cifrado SSL/TLS durante la transmisión de datos dentro o fuera del centro de datos.
- Cifrado AES-256 de datos almacenados en disco ("en reposo").
- Acceso controlado basado en perfiles y diferentes niveles de permisos.
- Garantizar el anonimato de los datos y evitar el acceso no autorizado.
- Debe proporcionar un factor de autenticación doble.

d) Copia de seguridad como servicio (BaaS)

- Disponer de una interfaz web, accesible al menos a través de los navegadores Internet Explorer, Mozilla Firefox o Google Chrome, que proporcione un acceso rápido a la información de soporte técnico, manuales en línea y asistentes.
- Contar con un panel de gestión web del entorno de backup con soporte para visualizar el estado de todas las tareas de backup, con opciones para generar informes en línea y enviarlos por correo electrónico.
- Disponer de una aplicación para la descarga e instalación de actualizaciones de productos, de forma manual o sin intervención del administrador.

- Realizar copias de seguridad mediante tecnología de imagen (snapshot) de servidores físicos y virtuales, soportando los sistemas operativos mencionados en la matriz de compatibilidad del fabricante, realizando copias completas de volúmenes, incluyendo información como sistemas operativos, aplicaciones, datos y configuraciones de los mismos.
- A partir de cualquier copia de seguridad realizada, ya sea completa o incremental, deberían ser posibles las siguientes opciones de restauración de datos:
- Restaure cualquier archivo o carpeta del servidor en cuestión, aunque ese archivo no se haya modificado en la fecha en que se realizó la copia de seguridad.
- Restaure las bases de datos de Microsoft SQL Server 2005 y versiones posteriores.
- Restaurar bases de datos de Microsoft Exchange Server 2007, 2010, 2013 y 2016.
- Backup de servidores virtuales en plataforma VMware, sin agentes.
- Suportar VMWare ESX/ESXi, vCenter Server e vCenter Server Appliance versiones 4.x, 5. x e 6.x, 7.x.
- Copia de seguridad de servidores virtuales en la plataforma Hyper-V, sin agentes.
- Compatibilidad con las versiones de Microsoft Hyper-V Server 2012 R2 o superior.
- Soporte de Microsoft Windows Server Hyper-V versiones 2012 y superiores.
- La actualización de la herramienta para futuras versiones, deberá realizarse como parte de la prestación del servicio, sin costo adicional para el CONTRATISTA.
- Compatibilidad de agentes de software de copia de seguridad con plataformas Windows Server 2003 y 2008, 2008 R2, 2012, 2012 R2, 2016 y 2019,32 y 64 bits.
- Compatibilidad de los agentes de software de copia de seguridad con las plataformas Windows 10.
- Compatibilidad de agentes de software con plataformas Linux:
    - Ubuntu 12 +.
- La solución debe tener al menos las siguientes opciones de recuperación desde la nube:
    - Recuperación granular de archivos y directorios directamente desde el navegador.

Recuperación granular de archivos, directorios y bases de datos de servidores Windows desde el montaje del punto de recuperación y acceso a través de SFTP (Secure File Transfer Protocol)

El CONTRATISTA deberá entregar un informe de activación del servicio, en donde se indique la cantidad de TB contratados incluyendo la vigencia de los mismos.

4.3 Lugar y plazo de prestación del servicio

4.3.1 Lugar

La entrega del servicio se realizará en modalidad remota desde las oficinas del contratista, empleando la infraestructura en la nube de Office 365 de la entidad contratante, en coordinación con la División de Tecnologías de Información y Comunicaciones de EGASA.

4.3.2 Plazo

El plazo de vigencia del servicio de BACKUP en nube es de 365 días calendario, el mismo que se computa al día siguiente de notificado el pedido de compra.

VI. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

6.1 Otras obligaciones

6.1.1 Otras obligaciones de la Entidad

- EGASA debe brindar los recursos solicitados por el proveedor del servicio de manera oportuna, de tal forma que no genere retrasos ni incumplimientos.
- EGASA nombrará un supervisor del contrato que interactuará con el especialista.

6.2 Adelantos

No aplica.

6.3 Confidencialidad

EL CONTRATISTA se compromete a no revelar, comentar, suministrar o transferir de cualquier forma a terceros, cualquier información que hubiese recibido directa o indirectamente de Empresa de Generación Eléctrica de Arequipa S.A- EGASA, o que hubiese sido generada como parte del servicio. El incumplimiento de esta obligación será causal de resolución del contrato respectivo, y de ser el caso, Empresa de Generación Eléctrica de Arequipa S.A - EGASA, se reserva el derecho de interponer las acciones legales que correspondan, en caso de que el locador incumpla esta condición, aún después de ejecutado el servicio.

6.4 Conformidad de la prestación

La conformidad de la prestación se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley 32069, Ley General de Contrataciones Públicas. La

conformidad es otorgada por la División de Tecnologías de Información y Comunicaciones en el plazo máximo de siete (7) días computados desde el día siguiente de producida la recepción del informe de activación del servicio.

6.5 Forma de pago

EGASA efectuará el pago total dentro de los diez (10) días hábiles siguientes de emitida la conformidad de la prestación, conformidad que será otorgada por la División de Tecnologías de la información y comunicaciones luego de la presentación del informe de activación del servicio, que deberá ser entregado hasta los 15 días de notificado el Pedido de compra, juntamente con el expediente de pago a la entidad mediante la dirección mesapartes@egasa.com.pe; expediente que estará conformado por los siguientes documentos:

- Comprobante de pago y su archivo XML
- Pedido de compra emitido por EGASA
- Hoja de entrada de servicios emitida por el Área Usuaria
- Acta de conformidad (cuando culmine el servicio)
- Informe de activación del servicio

6.6 Modalidad de Pago

La presente contratación se rige por la modalidad de suma alzada, de conformidad con el artículo 130 del reglamento, de conformidad con el artículo 130 del Reglamento.

6.7 Penalidades

6.7.1 Penalidades por mora

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del presente servicio, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, de conformidad con el artículo 120 del Reglamento.

6.8 Responsabilidad por vicios ocultos

La recepción conforme de la prestación por parte de LA ENTIDAD CONTRATANTE no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la Ley N° 32069, Ley General de Contrataciones Públicas y 144 de su Reglamento aprobado por Decreto Supremo N° 009-2025-EF.

El plazo máximo de responsabilidad del contratista es de un (1) año contado a partir de la conformidad otorgada por LA ENTIDAD CONTRATANTE.

6.9 Requisitos de Seguridad, Salud Ocupacional y Medio Ambiente

No Aplica.

6.10 Cláusula anticorrupción y antisoborno.

A la suscripción del contrato o notificado el pedido de compra, EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación[1] y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

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

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

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

[1] Artículo 9 de la Ley N°32069, Ley General de Contrataciones Públicas.
[2] Literal d) del Numeral 68.1 del Artículo 68 de la Ley N°32069, Ley General de Contrataciones Públicas.
[3] Literal d) del artículo 274 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas
[4] Numeral 122.6 del artículo 122 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.

6.11 Solución de controversias.

Todos los conflictos que se deriven de la ejecución e interpretación de la presente contratación son resueltos mediante trato directo, conciliación y en caso no se llegue a conciliar se recurrirá al arbitraje, para lo cual en el caso de llegar a éste último, todos los conflictos que se deriven de la ejecución e interpretación del presente Pedido de Compra o Contrato, incluidos los que se refieran a su nulidad e invalidez, serán resueltos de manera definitiva e inapelable mediante arbitraje de derecho, de conformidad con lo establecido en la normativa de Contrataciones Públicas.
Las partes expresamente se someten al Centro de Arbitraje de la Cámara de Comercio e Industria de Arequipa.

El Arbitraje será resuelto por un Tribunal Unipersonal de acuerdo a las reglas procesales y el Reglamento del Centro de Arbitraje de la Cámara de Comercio e Industria de Arequipa.
El Laudo arbitral emitido es vinculante para las partes y pondrá fin al procedimiento de manera definitiva, siendo inapelable ante el Poder Judicial o ante cualquier instancia administrativa.

Los costos, gastos y honorarios en que sea necesario incurrir para llevar a cabo el Arbitraje, serán asumidos por el contratante respecto del cual resultara adverso el laudo arbitral.

6.12 Resolución de contrato.

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas.

Por mutuo disenso según lo dispuesto en el Art. 1313° del Código Civil.

6.13 Gestión de riesgos.

No aplica.

6.14 Otros aspectos

El presente requerimiento no se encuentra definido en:

i) Una ficha homologada incluida en el Listado de Requerimientos Homologados,
ii) Una ficha técnica de Listado de Bienes y Servicios Comunes y
iii) Catálogo Electrónico de Acuerdos Marco.

Fecha 19/08/2025

VII. REQUISITOS DE CALIFICACIÓN

7.1 Documentos Adicionales presentados por el Postor

Requisitos:

El postor deberá contar con certificación y/o carta de autorización vigente emitida por el fabricante de la solución de backup ofertada, que lo acredite como distribuidor o partner autorizado para la comercialización y provisión de licencias en el territorio nacional.

Acreditación:

Certificación y/o carta de autorización vigente emitida por el fabricante, en la que se indique claramente que el postor está habilitado para la distribución y provisión de las licencias de la solución de backup.

Firmado digitalmente por QUIROZ GOMEZ Jorge Luis FAU 20216293593 hard
Fecha: 2025.08.20 10:39:37 -05'00'

Firmado digitalmente por CHIRINOS VELA Maryluz Concepcion FAU 20216293593 hard
Motivo: DEC
Fecha: 2025.08.20 10:53:50 -05'00'