

CONTRALORÍA GENERAL DE LA REPÚBLICA

PROYECTO MEJORAMIENTO DE LOS SERVICIOS DE CONTROL GUBERNAMENTAL PARA UN CONTROL EFECTIVO, PREVENTIVO Y FACILITADOR DE LA GESTIÓN DE PÚBLICA

| | NOMBRE | CÓDIGO |
|------------------|--|--------|
| COMPONENTE | Adecuado acceso a TIC en los procesos de control gubernamental | 3 |
| PRODUCTO | Implementación de una herramienta para la solución de correo electrónico en la nube | 3.6 |
| PROYECTO INTERNO | Mejoramiento de la Infraestructura de las Tecnologías de la Información y Comunicaciones en la Contraloría General de la República | 3.5 |



TÉRMINOS DE REFERENCIA

AMPLIACIÓN DE LICENCIAS DE LA HERRAMIENTA DE SOLUCIÓN DE CORREO ELECTRÓNICO EN LA NUBE PARA LA CONTRALORÍA GENERAL DE LA REPÚBLICA.

1. Introducción
2. Antecedentes
3. Objetivos
4. Descripción y características del servicio
5. Perfil del Personal Técnico para la solución del servicio
6. Obligaciones del proveedor
7. Plazo de entrega y ejecución del servicio
8. Lugar de la prestación del servicio
9. Entregables
10. Forma de pago
11. Conformidad del servicio
12. Responsabilidades del proveedor
13. Penalidades aplicables
14. Confidencialidad
15. Requisitos de calificación

MAYO 2023

TÉRMINOS DE REFERENCIA
AMPLIACIÓN DE LICENCIAS DE LA HERRAMIENTA DE SOLUCIÓN DE CORREO
ELECTRÓNICO EN LA NUBE PARA LA CONTRALORÍA GENERAL DE LA REPÚBLICA.

1. INTRODUCCIÓN

La Contraloría General de la República (CGR) es el órgano superior del Sistema Nacional de Control (SNC) que cautela el uso eficiente, eficaz y económico de los recursos del Estado, la correcta gestión de la deuda pública, así como la legalidad de la ejecución del presupuesto del sector público y de los actos de las instituciones sujetas a control; coadyuvando al logro de los objetivos del Estado en el desarrollo nacional y bienestar de la sociedad peruana.

La actual gestión de la Contraloría General de la República del Perú (CGR) tiene como uno de sus objetivos principales modernizar y mejorar el Sistema Nacional de Control (SNC) a fin de asegurar su eficacia y eficiencia en el control contra la corrupción y la inconducta funcional para así crear valor público.

2. ANTECEDENTES

El Proyecto de Inversión (CUI) N°2412703 “Mejoramiento de los Servicios de Control Gubernamental para un control Efectivo, Preventivo y Facilitador de la Gestión Pública-BID3” tiene como objetivo central contribuir a la mejora de los servicios de control gubernamental con el fin de mejorar la efectividad y eficiencia en el uso de los recursos del Estado.

El responsable de la ejecución del proyecto es la CGR y dicho Proyecto contempla la ejecución de los siguientes componentes:

- Componente 1. Adecuados procesos para un control efectivo y eficiente
- Componente 2. Adecuadas capacidades de los RRHH en temas de control gubernamental
- Componente 3. Adecuado acceso a TIC en los procesos de control gubernamental.
- Componente 4. Adecuada capacidad operativa para la prestación de servicios de control desconcentrados

El componente 3, tiene como objetivo Implementar las tecnologías de información y comunicaciones (TIC) que soporten adecuadamente los procesos misionales de la CGR ampliando sus capacidades y optimizando sus resultados mediante la implementación de una moderna arquitectura de soluciones, con énfasis en la integración e interoperabilidad de los sistemas, y con una arquitectura de datos enfocada en la consistencia, disponibilidad y accesibilidad, soportadas por una robusta infraestructura tecnológica.

El componente 3, cuenta con la acción “Implementación de una herramienta de correo electrónico que soporte el crecimiento de usuarios de la contraloría” por la que en este marco se crea el proyecto interno de la CGR denominado “Modernización de la infraestructura de las tecnologías de la información y comunicaciones en la CGR”.

Actualmente la CGR cuenta con correo electrónico Microsoft Office 365 con un total de 6500 licencias en formato suscripción, el cual constituye uno de los activos de vital importancia para las operaciones de la institución.

3. OBJETIVO

Ampliar la cantidad de suscripciones de la herramienta de solución de correo electrónico en la nube, con el cual ya cuenta la Contraloría General de la República a través de Internet en la modalidad de categoría de software como servicio (SaaS); asimismo, incluya: alta disponibilidad, nivel de seguridad contra las amenazas de correo, capacidad de

almacenamiento, respaldo de la información para la toda la solución ofertada propiamente dicho, que incluyan los servicios de interacción en tiempo real; chat de texto, voz, video, edición de archivos compartidos y otros adicionales que ofrecen dentro del servicio. Dicho servicio debe estar garantizado a través de un soporte técnico. Asimismo, el servicio debe tener como alta prioridad la seguridad de la información de la Institución, a través de diversos controles tanto lógicos como físicos.

4. DESCRIPCIÓN Y CARACTERÍSTICAS MÍNIMAS DEL SERVICIO

4.1. ALCANCE

Mediante el presente servicio se requiere la contratación de la herramienta para la solución de correo electrónico en la nube Microsoft Office 365 para la Contraloría General de la República, en la modalidad de software como servicio y dotar las licencias en alquiler. Cada licencia debe incluir el servicio de correo, protección ante código malicioso para el acceso al correo electrónico, mensajería instantánea para la solución de correo, gestor de documentos para la solución de correo y uso compartido de archivos online para la solución de correo, para dos mil setecientos (2,700) colaboradores; la solución se debe integrar con el servicio de correo que ya cuenta la institución, bajo el mismo dominio de correo, así como también se debe gestionar desde la misma consola de administración de la plataforma actual.

El proveedor debe considerar que la solución ofertada cumpla con los lineamientos para el uso de servicios en la nube para Entidades de la Administración Pública del Estado Peruano, según la Resolución de Secretaría de Gobierno Digital N° 001-2018-PCM/SEGDI.

4.2. CORREO ELECTRÓNICO EN LA NUBE

El servicio de correo electrónico en la nube (empresarial) a contratar deberá cumplir con las siguientes características como mínimo:

- a. Habilitar el correo electrónico en la nube para dos mil setecientos (2,700) buzones de correo contratados por el plazo de tres (3) años o durante el plazo de ejecución de los servicios conexos del Convenio N°001-2020-CG-UE002/BID. El proveedor debe considerar todos los servicios necesarios para su funcionamiento y uso para los usuarios finales.
- b. Cada buzón debe tener como mínimo 50GB de almacenamiento como mínimo.
- c. Permitir adjuntar archivos con una capacidad como mínimo de 100 MB, con opción a filtrar determinado tipo de archivos.
- d. Protección del correo electrónico contra código malicioso.
- e. Brindar una solución de protección AntiSpam propia, la cual debe ser parte de la solución de correo en la nube, habilitada para la totalidad de los buzones de correo solicitados.
- f. Brindar el acceso a una consola de administración general que gestione la modificación, creación o eliminación de usuarios, para los administradores del servicio de correo de la CGR.
- g. Garantizar el acceso seguro de los clientes hacia la solución de correo bajo conexión HTTPS, utilizando certificados reconocidos internacionalmente, deberá incluir el certificado digital con validación extendida según la solución propuesta.
- h. Permitir visualizar el correo en dispositivos móviles (teléfonos móviles, tablets, entre otros).
- i. Permitir el acceso vía web, a través de cualquier navegador existente.
- j. Permitir trabajar con o sin conexión a Internet.
- k. Permitir archivado de los correos.
- l. Permitir definir remitentes bloqueados.
- m. Permitir definir remitentes seguros.
- n. Permitir enviar correos con niveles de importancia.

- o. Permitir enviar correos de auto respuesta de acuerdo a reglas definidas por el usuario.
- p. Permitir configurar reglas para mover, clasificar o eliminar correos entrantes.
- q. Permitir definir y reservar recursos (como salas de reuniones).
- r. Permitir generar una firma personal para envíos de correos electrónicos.
- s. Permitir etiquetar un correo.
- t. Permitir el uso de “notificaciones de recibo” y “lectura de correo electrónico”.
- u. Permitir recuperar correos electrónicos eliminados del buzón de correo.
- v. Permitir recuperar contenido que ha sido borrado del ambiente de elementos eliminados, así como recuperar correos enviados a un destinatario en particular.
- w. Permitir a los usuarios iniciar sesión usando un usuario y contraseña y/o certificado digital, dicho usuario y contraseña debe ser validado contra el directorio de usuarios de la organización, además la herramienta debe asignar privilegios y perfiles al usuario, según los ya configurados.
- x. Tener disponible la funcionalidad de deshabilitar el acceso de los usuarios desde la red externa.
- y. La solución propuesta por el proveedor debe ejecutarse en un ambiente de tipo nube (Cloud).
- z. El proveedor debe asegurar mantener un acceso restringido de sus empleados y el fabricante de la solución a las bases de datos que contienen la información generada por la CGR, así como mantener el cumplimiento de los requisitos de confidencialidad impuestos a sus empleados. Esta información debe ser sustentada por una declaración jurada del proveedor para la firma de contrato.
- aa. Capacidad de búsqueda de correos electrónicos.
- bb. Capacidad de arrastrar y soltar citas.
- cc. Configurar recordatorio de cita a reunión para un día y hora específico.
- dd. Permitir crear tareas.
- ee. Configurar recordatorio de tareas para un día y hora específico.
- ff. Capacidad de crear contactos personales.
- gg. Capacidad de crear listas de distribución personal.
- hh. Contar con una lista global de correos común a todos los usuarios, incluyendo los usuarios de directorio activo de la institución.
- ii. La solución debe de tener un nivel de servicio del 99.9% mensual para todos los componentes del correo ofertados en el esquema de nube, la cual debe sustentarse con una declaración jurada del proveedor para la firma de contrato. El nivel de servicio solicitado solo aplica para los componentes de la solución ofrecidos por el proveedor. La indisponibilidad del servicio producto de incidencias en la plataforma de la CGR no afectará al proveedor.
- jj. Capacidad para implementar políticas de envío y recepción de correos según dominios específicos por cuenta de usuario y/o grupo.
- kk. La solución propuesta debe incluir de una herramienta licenciada en la nube y local que permita realizar (copia de respaldo y restauración), a demanda (manual) y programada de la configuración e información de la institución.

4.3. MENSAJERÍA INSTANTÁNEA PARA LA SOLUCIÓN DEL CORREO

- a. Permitir realizar a los usuarios sesiones de mensajería instantánea de uno a uno y hacia múltiples usuarios. Permitir configurar grupos de usuarios a la red social empresarial.
- b. Permitir hacer uso de la solución a través de un cliente web, en el cual tendrá que instalarse un componente o un cliente en la estación de trabajo de los usuarios a utilizar la solución.

- c. Permitir comunicarse con plataformas de mensajería pública tales como Skype, Hangouts u otros similares para que los usuarios a través de ellas puedan establecer comunicación con el personal autorizado de la CGR.
- d. Brindar una plataforma centralizada que permita la gestión de los perfiles a nivel de funcionalidades de la solución de mensajería instantánea y comunicación de los usuarios de la CGR.
- e. Permitir crear privilegios y perfiles de usuario de la CGR.
- f. Permitir reuniones, llamadas, reuniones en chat y conversaciones en cualquier momento.
- g. Permitir a los usuarios iniciar sesión usando un usuario y contraseña, dicho usuario y contraseña debe ser validado contra el directorio de usuarios de la CGR, además la herramienta debe asignar privilegios y perfiles al usuario, según los ya configurados.

4.4. GESTOR DE DOCUMENTOS PARA LA SOLUCIÓN DEL CORREO

- a. Permitir realizar flujos de trabajo y la administración de los mismos.
- b. Ofrecer una plataforma centralizada que permita la gestión de documentos para almacenar, organizar y compartir información desde cualquier dispositivo.
- c. Acceder a dicha información rápidamente y de manera segura.
- d. Control de versiones.
- e. Crear documentos de ofimática y guardarlos directamente en la solución.
- f. Permitir crear contenidos en distintos formatos, los cuales deben ser desde la realización de un enlace con su respectivo título hasta la realización de un contenido complejo que incluya documentos de ofimática con los que trabaja la CGR.
- g. Protección de contenido confidencial con permisos en el nivel del documento.
- h. Permitir gestionar privilegios y perfiles de usuario.
- i. Permitir aislar al usuario no autorizado de las fuentes de información, garantizando la seguridad e integridad de las mismas mediante el acceso a través de una pantalla de acceso.
- j. Permitir a los usuarios poder iniciar sesión usando certificados digitales de autenticación y/o un usuario y contraseña, dicho usuario y contraseña debe ser validado contra el directorio de usuarios de la CGR, además la herramienta debe asignar privilegios y perfiles al usuario, según los ya configurados.
- k. Permitir crear comunidades de trabajo.
- l. Crear espacios (incluso 'subsitios' dentro del mismo espacio) para el trabajo en grupo, donde colaborar, compartir contenidos y organizar el trabajo mediante calendarios, y tareas asociadas a usuarios.
- m. Permitir compartir archivos de gran tamaño.
- n. Compartir actualizaciones de estado e información detallada personal con compañeros de trabajo.
- o. Permitir el uso de gadgets como un calendario en el cual según sus privilegios podrá colocar actividades.
- p. Soportar la carga y descarga de los formatos de archivos más comunes tales como .doc, .ppt, .xls, .pdf, .jpg, rar, .zip.
- q. La solución propuesta por el proveedor debe contar con un foro.
- r. Permitir el monitoreo integrado en tiempo real y mantener el histórico de los flujos de trabajo.
- s. La solución propuesta debe coexistir con los sistemas y programas instalados en las estaciones de trabajo tales como el sistema de gestión documentaria, herramientas de ofimática, compatibilidad con navegadores más utilizados como Internet Explorer, Firefox, Chrome.

- t. Permitir la generación de semáforos o alertas.
- u. La solución propuesta debe incluir de una herramienta licenciada en la nube y local que permita realizar (copia de respaldo y restauración), a demanda (manual) y programada de la configuración e información de la institución.

4.5. USO COMPARTIDO DE ARCHIVOS ONLINE PARA LA SOLUCIÓN DEL CORREO

- a. El espacio de almacenamiento en nube por cada usuario será mínimo de 1 TB, debe tener la capacidad de aumentar dicha capacidad, en caso sea necesario.
- b. Permitir a los empleados conectar con otras personas de la institución.
- c. Permitir compartir información con otros grupos o equipos de trabajo de la institución.
- d. Permitir el trabajo de colaboración creando comunidades organizadas por proyectos.
- e. Proteger los archivos de trabajo y obtener acceso a ellos en varios dispositivos.
- f. Permitir el uso de la bandeja de entrada para ver, clasificar por orden de prioridad y administrar el contenido más relevante de la red social corporativa.
- g. Permitir a los usuarios iniciar sesión usando un usuario y contraseña, dicho usuario y contraseña debe ser validado contra el directorio de usuarios de la CGR.
- h. La solución debe tener la capacidad de utilizar la herramienta mediante cualquier navegador de internet y también debe tener la capacidad de ejecutarse mediante un cliente en las estaciones de trabajo de los usuarios a utilizar la solución.
- i. La solución propuesta debe incluir de una herramienta licenciada en la nube y local que permita realizar (copia de respaldo y restauración), a demanda (manual) y programada de la configuración e información de la institución.

4.6. CARACTERÍSTICAS DEL SERVICIO A CONTRATAR

4.6.1. SEGURIDAD, PRIVACIDAD Y MONITOREO

- a. El proveedor debe reportar cualquier incidente de seguridad y evento que afecte el funcionamiento de los servicios contratados por la CGR. La CGR comunicará al proveedor la lista de contactos a utilizar para este fin.
- b. El proveedor y el fabricante no deben analizar o procesar el contenido de los correos electrónicos de la entidad para ningún propósito diferente al servicio contratado. Específicamente, el proveedor y el fabricante no podrán utilizar la información de la entidad con fines comerciales o publicitarios, con fines fraudulentos, ilegales, engañosos o discriminatorios. Las políticas de privacidad y seguridad de la información con las que cuenta el fabricante serán solicitadas por la CGR durante el periodo del servicio. Para lo cual, el postor deberá de presentar como documento para la firma de contrato: una declaración jurada en la cual deberá de indicar las URL del fabricante de la solución en idioma nativo o español a ofertar en el cual deba de sustentar lo solicitado.
- c. La generación de incidentes por parte de la CGR se podrá realizar por sistema de ticket, correo electrónico y teléfono.
- d. El proveedor del servicio se compromete en firmar y entregar al inicio del servicio el acuerdo de confidencialidad y cumplimiento de la Política de Seguridad de la Información de la CGR
- e. El proveedor y el fabricante deben garantizar la protección de los correos electrónicos contra el acceso no autorizado, modificaciones no autorizadas o negación de servicio; asimismo, debe considerar el cifrado de todos los datos antes de salir de y retorno a la Entidad.

4.6.2. GESTION DEL SERVICIO

- a. El proveedor debe asignar a un responsable del servicio, el cual será el único punto de contacto con la CGR, debe de relevar las necesidades de la CGR, estar a cargo de todas las coordinaciones con la CGR, y ser el responsable del cumplimiento de lo solicitado en el servicio y la entrega de la documentación contemplada en la sección Entregables.
- b. La Gerencia de Tecnologías de la Información designará a un representante para coordinar con el proveedor en todo lo referente a las tareas administrativas que conlleven a la ejecución del servicio.
- c. De ser necesario, la gestión de cambios en el servicio se hará mediante un formato de gestión de cambios el cual será definido por la GTI. Los cambios serán coordinados por la Subgerencia de Operaciones y Plataforma Tecnológica.
- d. Los cambios que pudiesen suscitarse durante la ejecución del servicio de ninguna manera afectarán los costos del servicio.
- e. Funciones de gestión del servicio.
- f. El gestor del servicio debe asignar personal técnico en sitio o remoto en las instalaciones de la CGR para atender las incidencias e inconvenientes relacionadas al servicio de Correo Electrónico y portal colaborativo en la nube.
- g. Los recursos mínimos asignados en local de la CGR por parte del proveedor deben de ser:
 - i. Gestor de servicio, con la responsabilidad de coordinar las actividades del servicio entre personal de la CGR y personal del proveedor asignado al servicio.
 - ii. Recursos técnicos de soporte que cuenten con la capacidad de revisar y atender las incidencias relacionadas al servicio de Correo Electrónico y Portal Colaborativo en la nube.

4.6.3. SOPORTE TÉCNICO

- a. El proveedor debe brindar soporte técnico durante la ejecución del servicio, y de acuerdo a las siguientes características:
 - i. Soporte técnico presencial a demanda disponible 7 días por 24 horas.
 - ii. Soporte remoto: 7 días por 24 horas debe incluir feriados, sábados y domingos.
 - iii. Atención de incidentes: 7 días por 24 horas debe incluir feriados, sábados y domingos.
 - iv. Registrar incidentes por Teléfono o por correo electrónico o por sistema de ticket.
- b. El proveedor debe de asignar especialistas de la solución implementada para resolver los incidentes reportados por la CGR.
- c. El proveedor debe priorizar la atención y solución de los incidentes o consultas reportados por la CGR hacia el fabricante. La cantidad de consultas que se puedan realizar al fabricante a través del proveedor, con respecto al servicio ofertado, no debe de tener límites y debe de contar con los siguientes tiempos de respuestas máximo:
 - i. Consultas: 8 horas, dentro del horario laboral.
 - ii. Impacto bajo: 4 horas, dentro del horario laboral.
 - iii. Impacto medio: 3 horas.
 - iv. Impacto alto: 2 horas.

Debe de contar el proveedor con un contrato de soporte con el fabricante, el cual será sustentado como documento para la firma de contrato: Declaración jurada en el cual se indique que se cuenta con un contrato de soporte con el

fabricante adjuntando la factura o invoice de pago del soporte con el fabricante. Dicho invoice podrá ser presentado en su idioma nativo.

- d. El proveedor realizará, dentro del alcance del servicio, las instalaciones, actualizaciones y configuraciones necesarias para asegurar la integración y compatibilidad de la infraestructura de autenticación del servicio contratado con el directorio activo de la CGR.
- e. El proveedor debe de incluir dentro del alcance, 02 mantenimiento predictivo/preventivo a través de un arquitecto empresarial de la solución sin que esto represente costos adicionales para la institución. El servicio debe contar como mínimo de 32 horas de trabajo para los 02 mantenimientos.

4.6.4. NIVELES DE ATENCION PARA EL SOPORTE TÉCNICO

Para el registro de solicitudes de soporte técnico se utilizará los medios de comunicación oficial: sistema de tickets y/o teléfono y/o correo electrónico, los cuáles serán presentados al inicio del servicio.

Los acuerdos de niveles de servicio (SLA) para la atención de solicitudes de soporte técnico son:

Tiempos de atención para el inicio de la solución:

| Urgencia | Tiempo máximo de inicio de la solución (*) presencial o remoto | Tiempo máximo de solución (**) presencial o remoto |
|----------|---|---|
| Alta | 01 horas | 04 horas de su inicio |
| Media | 02 horas | 08 horas de su inicio |
| Baja | 03 horas | 24 horas de su inicio |

(*) El tiempo de solución se contabiliza a partir de la emisión, vía correo electrónico, de la solicitud del soporte técnico por parte de la CGR, hasta que se solucione la solicitud del soporte técnico.

- **Alta:** Son incidentes que necesita un tratamiento especial por lo que su impacto representa para la organización, por lo que requiere su inatención inmediata o podría afectar significativamente la operación del servicio.
- **Media:** Son incidentes con un tiempo de atención intermedio; su inatención afecta o podría afectar moderadamente la operación del servicio.
- **Baja:** Son incidentes con un tiempo de atención prolongado; su atención afecta o podría afectar levemente a la operación del servicio.

La clasificación de la urgencia la realizará el personal de la CGR en el registro del incidente.

El personal de la CGR verificará que se haya dado la solución al incidente antes de aceptar el fin del tiempo de solución.

(*) Tiempo que iniciara la atención del incidente presentado por parte del personal técnico de contratista.

(**) En caso el fabricante del servicio brindado supere el tiempo de la solución dentro del plazo, el contratista deberá brindar una solución total o parcial temporal para superar el incidente durante la indisponibilidad generada por parte del fabricante, asimismo, posterior a la resolución del incidente por parte del fabricante el contratista debe presentar el informe incluyendo las evidencias del fabricante indicando los tiempos y la causa de la indisponibilidad del servicio y la solución final. Este tipo de incidentes no se contabilizarán dentro de las penalidades, siempre y cuando se brinde la continuidad del servicio bajo las condiciones previamente indicadas.

5. PERFIL DE PERSONAL TÉCNICO PARA LA SOLUCIÓN DEL SERVICIO

UN GESTOR DEL SERVICIO

Requisitos

- a. Certificación vigente en Gerencia de proyectos Project Management Professional (PMP), podrá presentarse en su idioma original.

Acreditación

Se acreditará con copia simple del certificado antes señalado.

UNO O DOS CONSULTOR(ES) ESPECIALISTA(S) DE SOPORTE

El proveedor podrá presentar un consultor o dos consultores especialista(s) de soporte, en caso sean dos personas se podrá reunir las certificaciones solicitadas en conjunto.

Requisitos

- a. Certificado o Transcript sobre la plataforma de Correo Electrónico y/o Portal colaborativo y/o mensajería y/o Certified Solutions Associate, que el proveedor oferte.
- b. Certificación en Secure Cloud Services y/o Certified Security Administrator Associate.
- c. Certificado o Transcript como Experto en Plataforma e Infraestructura de la Nube y/o Certified Solutions Expertt: Cloud Platform and Infrastructure.

Acreditación

Se acreditará con copia simple de los certificados antes señalados.

Notas:

Los requisitos solicitados en el numeral Requisitos que deberá cumplir el Proveedor serán acreditados para el perfeccionamiento del contrato.

6. OBLIGACIONES DEL PROVEEDOR

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

El proveedor deberá confirmar la operatividad completa de la solución ofertada, así como la autenticación a través del directorio de usuarios de la organización de la CGR. El consultor especialista de soporte deberá brindar atención inmediata en caso de presentarse fallas o incidentes reportados por la CGR.

El proveedor deberá presentar en la propuesta técnica un certificado de seguridad de la información ampliamente reconocido y basado en estándares internacionales, el mismo que tiene que ser emitido por una organización de auditoría independiente. Asimismo, debe contemplar en la solución ofertada los niveles de seguridad en términos de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

El proveedor deberá cumplir con los lineamientos establecidos en el Decreto Supremo N° 103-2020-EF para la aplicación obligatoria de los Protocolos Sanitarios Sectoriales en prevención del COVID-19; con las Normas y Protocolos Sanitarios en prevención del COVID-19 establecidas por el Ministerio de Salud; así como el Plan para la Vigilancia, Prevención y Control de COVID-19 y demás protocolos sanitarios establecidos por la CGR y otros que sean necesarios, para el ingreso a las instalaciones a nivel nacional durante la ejecución de los servicios contratados, a efectos de proteger la salud del personal que participará en la ejecución del servicio.

7. PLAZO DE ENTREGA Y EJECUCIÓN DEL SERVICIO

El plazo de entrega del adicional de cuentas de correo de la solución en la nube que cuenta la Contraloría será máximo de quince (15) días calendario, contados a partir del día siguiente de la suscripción del contrato.

El plazo de ejecución del servicio contratado es por tres (3) años, contados a partir de la fecha de suscrito el acta de inicio del servicio. Dentro de los primeros tres (3) días calendario contados a partir del día siguiente de la firma de contrato se debe realizar la reunión de Kick Off para las coordinaciones del presente servicio.

8. LUGAR DE LA PRESTACIÓN DEL SERVICIO

El servicio se brindará en las instalaciones de la sede central de la CGR (Jr. Camilo Carrillo 114 - Jesús María, Lima - Perú).

9. ENTREGABLES

El lugar de entrega de los documentos por parte del proveedor será en la Mesa de Partes de la Sede Central de la CGR, en el horario de lunes a viernes de 09:00 a 16:30 horas, con atención a la Subgerencia de Operaciones y Plataforma Tecnológica de la Gerencia de Tecnologías de la Información con copia a la Dirección Ejecutiva de Gestión de Proyectos. Los documentos presentados deben estar foliados.

El proveedor deberá presentar el plan de trabajo en un plazo máximo de 10 días calendario, contados a partir del día siguiente de la firma de contrato que contenga, como mínimo la siguiente estructura:

- Título.
- Objetivos.
- Metas.
- Estrategias.
- Cronograma.
- Actividades.
- Recursos.
- Evaluación.
- Recomendaciones.

a. Entregable 1:

- Informe del proveedor indicando el tipo y la cantidad de licencias alquiladas, debe incluir las características del servicio contratado, las cuales deben ser como mínimo las definidas dentro la sub sección Alcance y Descripción.
- El proveedor debe entregar una carta donde indique claramente los medios de comunicación, a través del cual se reportarán los incidentes del presente servicio (teléfonos, correo electrónico y sistema de atención de tickets o similar).

El plazo máximo para la presentación del Entregable 1 es de diez (10) días calendario, contados a partir del día siguiente de la firma del contrato.

b. Entregable 2:

- Informe anual del proveedor por el servicio de soporte técnico y niveles de servicio. El informe debe tener como mínimo, las actividades realizadas durante el periodo; indicando la disponibilidad de servicio, la fecha, hora, actividades preventivas, los problemas reportados y las acciones resolutivas, entre otros.

El plazo máximo para la presentación del Entregable 2, es a los diez (10) días calendario siguiente de finalizado cada servicio anual.

10. FORMA DE PAGO

El pago se realizará previa conformidad emitida por la Subgerencia de Operaciones y Plataforma Tecnológica, en moneda nacional y a la presentación del comprobante de pago por parte del proveedor, de acuerdo con lo siguiente:

- i. Primer Pago, 40% del costo del servicio. Se efectuará una vez recibida la conformidad por parte de la Subgerencia de Operaciones y Plataforma Tecnológica, en relación al Entregable 1.
- ii. Pago Anual, 20% del costo del servicio prorrateado en 3 años. Se efectuará una vez recibida la conformidad por parte de la Subgerencia de Operaciones y Plataforma Tecnológica, con respecto a los Entregable 2

Para efectos del pago de las contraprestaciones ejecutadas por el proveedor adjudicado, la CGR debe contar con la siguiente documentación:

- Conformidad por parte del área usuaria, previo informe técnico del administrador del servicio de la Subgerencia de Operaciones y Plataforma Tecnológica de la validación de la documentación presentada por el proveedor, emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

11. CONFORMIDAD DEL SERVICIO

Las conformidades del servicio serán otorgadas por la Subgerencia de Operaciones y Plataforma Tecnológica, a través de la verificación del cumplimiento de las condiciones establecidas en los términos de referencia en el plazo máximo de diez (10) días de producida la recepción de la prestación (total o parcial, de ser el caso) efectuada.

12. RESPONSABILIDAD DEL PROVEEDOR

El proveedor es responsable por la calidad ofrecida y por los vicios ocultos de los servicios ofertados por un plazo no menor de tres (3) años contado a partir de la conformidad otorgada por la Entidad.

13. PENALIDADES APLICABLES

13.1. Penalizaciones por Mora

En caso de retraso injustificado del proveedor en la ejecución de las prestaciones objeto del contrato/orden de servicio, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso hasta por el monto máximo del 10% del monto del contrato/orden de servicio vigente. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

$$Penalidad\ diaria = \frac{0.10 \times \text{monto}}{F \times \text{plazo en días}}$$

Donde F tiene los siguientes valores:

- a. Para plazos menores o iguales a sesenta (60) días: F 0.40.
- b. Para plazos mayores a sesenta (60) días: F = 0.25

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato/orden de servicio o del ítem que debió ejecutarse o, en caso que estos involucraran obligaciones de ejecución periódica o entregas parciales, a la prestación individual que fuera materia de retraso.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando el proveedor acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En ese último caso, la calificación del retraso como justificado por parte de la Entidad no da lugar al pago de gastos generales ni costos directos de ningún tipo.

13.2. Otras penalidades

Se establecen penalidades distintas a la penalidad por mora, objetivas, razonables, congruentes y proporcionales con el objeto de la contratación. Para estos efectos, incluir los supuestos de aplicación de penalidad, distintas al retraso o mora, la forma de cálculo de la penalidad para cada supuesto y el procedimiento mediante el cual se verifica el supuesto a penalizar.

| SUPUESTO DE APLICACIÓN DE PENALIDAD | FORMA DE CÁLCULO | PROCEDIMIENTO |
|---|--|---|
| <p>Penalidad por incumplimiento en el tiempo de solución, de los niveles de atención para el soporte técnico:</p> <p>Se aplicará penalidad por cada fracción u hora de incumplimiento en el tiempo de solución, de acuerdo a lo establecido en los niveles de atención.</p> | <p>Monto total de la penalidad = 10% x (valor de la UIT) x T</p> <p><u>Donde:</u> UIT: Unidad Impositiva Tributaria T = Tt – Ts: Total de horas o fracción acumuladas en el retraso de tiempo de la solución (*). Ts: Tiempo de solución definido según niveles de atención (numeral 4.6.4) Tt: Tiempo de solución total del proveedor. (*) La fracción acumulada será considerada como una (01) hora.</p> | <p>El tiempo total de solución se contabiliza a partir de la emisión, vía correo electrónico, de la solicitud del soporte técnico por parte de la CGR, hasta que la CGR reciba el correo electrónico del proveedor señalando la solución a lo solicitado. El personal de la CGR verificará que se haya dado la solución para aceptar el fin del tiempo de solución.</p> |

14. CONFIDENCIALIDAD

El proveedor deberá mantener estricta confidencialidad sobre la información a que tendrá acceso durante la ejecución del servicio, no podrá disponer de la misma para fines distintos al desarrollo del servicio. El proveedor y su personal, deben comprometerse a mantener las reservas del caso y no transmitir los datos e información de la CGR a ninguna persona (natural o jurídica) que no sea debidamente autorizada por la CGR.

15. REQUISITOS DE CALIFICACIÓN

A. CAPACITACIÓN TÉCNICA Y PROFESIONAL

A.1. CALIFICACIONES DEL PERSONAL CLAVE

A.1.1. FORMACIÓN ACADÉMICA

GESTOR DEL SERVICIO

Un (01) Gestor del Servicio, con la responsabilidad de coordinar las actividades del servicio entre personal de la CGR y personal del proveedor asignado al servicio.

Requisitos

Un (01) Profesional Titulado en una de las siguientes especialidades: Ingeniería Sistemas y/o Ingeniería Informática y/o Ingeniería en Computación y/o Ingeniería Electrónica y/o Ingeniería Industrial y/o Ingeniería en Seguridad Informática y/o Ingeniería en Telecomunicaciones y/o Ingeniería Empresarial y Sistemas.

Acreditación

El 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.

En caso el 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.

CONSULTOR(ES) ESPECIALISTA(S) DE SOPORTE

Un o dos Consultor(es) Especialista(s) de Soporte, con la responsabilidad de liderar y ejecutar las actividades técnicas del servicio.

Requisitos

Profesional Bachiller y/o Titulado en una de las siguientes especialidades: Ingeniería de Sistemas y/o Ingeniería de Sistemas e Informática y/o Ingeniería Informática y/o Ingeniería en Computación y/o Ingeniería Electrónica y/o Ingeniería Industrial y/o Ingeniería en Seguridad Informática y/o Ingeniería en Telecomunicaciones y/o Ingeniería Empresarial y Sistemas.

Acreditación

El 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.

En caso el 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.

A.1.2. CAPACITACIÓN

GESTOR DEL SERVICIO

Requisitos

- a. Certificación vigente en Gerencia de proyectos Project Management Professional (PMP), podrá presentarse en su idioma original.

Acreditación

Se acreditará con copia simple de constancia de la certificación.

UNO O DOS CONSULTOR(ES) ESPECIALISTA(S) DE SOPORTE

El proveedor podrá presentar uno o dos consultores(es) especialista(s) de soporte, en caso sean dos personas se podrá reunir las certificaciones solicitadas en conjunto.

Requisitos

- a. Certificado o Transcript sobre la plataforma de Correo Electrónico y/o Portal colaborativo y/o mensajería y/o Certified Solutions Associate, que el proveedor oferte.
- b. Certificación en Secure Cloud Services y/o Certified Security Administrator Associate.
- c. Certificado o Transcript como Experto en Plataforma e Infraestructura de la Nube y/o Certified Solutions Expertt: Cloud Platform and Infraestructure.

Acreditación

Se acreditará con copia simple de los certificados.

A.1.3. EXPERIENCIA DEL PERSONAL CLAVE

GESTOR DEL SERVICIO

Requisitos

Experiencia profesional mínima de un (01) año en gestión de proyectos de TI.

Acreditación

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.

La experiencia del gestor del servicio será contada a partir de la fecha de colegiatura correspondiente.

UNO O DOS CONSULTOR(ES) ESPECIALISTA(S) DE SOPORTE

Requisitos

Experiencia profesional mínima de un (01) año en proyectos de plataforma de correo electrónico en nube y/o portal colaborativo en nube y/o administrador de sistemas relacionados a la plataforma de correo electrónico en nube y/o administrador en plataforma e infraestructura en nube.

Acreditación

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.

La experiencia del consultor especialista de soporte será contada a partir de la fecha de colegiatura correspondiente.

A.2. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

El postor debe acreditar un monto facturado acumulado equivalente a S/ 800,000.00 (ochocientos mil con 00/100 soles) por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se considera servicios similares a los siguientes: Servicio de correo en la nube y/o servicio plataforma de correo y/o servicio de nube; o servicio de correo electrónico, portal colaborativo, mensajería instantánea y video conferencia en la nube; o cloud computing; o servicio de correo electrónico, portal colaborativo, mensajería instantánea y video conferencia en la nube; o servicio de habilitación y configuración de correo electrónico, mensajería instantánea y portal colaborativo en la nube; o servicio de adquisición de suscripciones de plataforma colaborativa y correo electrónico en la nube; o servicio de migración de plataforma de correo electrónico corporativo hacia correo electrónico en la nube; o servicio de web hosting o servicio de cloud hosting.

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 fehaciente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones.