Generando Energía con Responsabilidad Social

TÉRMINOS DE REFERENCIA

Servicio de Suscripción de licenciamiento anual en una Solución Cloud para Seguridad y Protección contra amenazas en herramientas de colaboración de Microsoft 365.

Área Usuaria o área técnica estratégica	División Tecnologías de Información y Comunicaciones.
Objetivo/Meta del POI vinculado	OEI 7. Gestionar la Modernización de la Empresa
Requerimiento incluido en CMN	Si

I. FINALIDAD PÚBLICA

El presente proceso de selección busca contar con las licencias de funcionamiento básico e indispensable para un software de protección en nube, de modo que se mantengan habilitados los servicios necesarios, que permitan la prevención y protección de los archivos almacenados en los repositorios digitales de las cuentas de Microsoft 365, debido a que es una de las herramientas de colaboración más utilizada en todo el mundo y es un agente de amenazas crítico para los ataques cibernéticos.

II. OBJETIVO DE LA CONTRATACIÓN

EGASA busca contar con el licenciamiento de una plataforma / solución Cloud para seguridad de archivos en herramientas de colaboración y almacenamiento SaaS para mantener, mejorar y proteger dicho servicio, en beneficio de los usuarios de EGASA.

III. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

Servicio de Suscripción de licenciamiento anual en una Solución Cloud para Seguridad y Protección contra amenazas en herramientas de colaboración de Microsoft 365.

IV. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

4.1 Descripción del servicio a contratar

Ítem	Descripción del servicio

1	Suscripción de licenciamiento anual en una Solución Cloud para Seguridad y Protección contra amenazas en herramientas de colaboración de Microsoft 365.

4.2 Actividades y Alcance del servicio.

- Activar el licenciamiento por suscripción anual a la Solución Cloud para Seguridad y Protección contra amenazas en herramientas de colaboración de Microsoft 365:

La Solución Cloud para Seguridad y Protección contra amenazas en herramientas de colaboración de Microsoft 365 debe considerar las siguientes características:

Requerimientos Generales y Arquitectura
La solución suministrada debe ser a través un servicio **SaaS** en nube.
El servicio SaaS debe contar con al menos alguna de estas certificaciones: • SOC 2, • ISO 27001
La solución debe ser reconocida como una solución líder en seguridad cloud por analistas terceros como Forrester o Gartner en los últimos 3 años
La disponibilidad del servicio SaaS debe ser de al menos 99.9%
La solución debe usar protocolos de cifrados modernos para salvaguardar la organización.
La solución debe ser escalable y nativa de nube para soportar crecimiento
La solución debe proteger de Ciber Amenazas para archivos en la nube Office 365
La solución debe soportar proteger de Ciber Amenazas, en las siguientes aplicaciones SaaS de Colaboración y Almacenamiento de archivos: ○ Slack ○ Microsoft Teams ○ Microsoft OneDrive ○ Microsoft SharePoint ○ Google Drive ○ Box ○ Dropbox ○ Citrix ShareFiles
La solución debe proporcionar un servicio para 250 usuarios y buzones
La solución debe proveer protección contra los siguientes Ciber ataques: • Prevención ataques (Phishing, Spoofing, Spam) • Prevención de Malware (en herramientas de colaboración y almacenamiento) • Prevención de Malware de día Cero con Sandboxing (en herramientas de colaboración) y Limpieza de Documentos CDR • Anomalías de usuarios e inicios de sesión anómalos (Indicios de robo de cuenta). • Uso no autorizado de aplicaciones SaaS también conocido como Shadow IT • Prevención de Fuga de Datos (DLP) en herramientas de colaboración
La solución debe permitir gestionar la detección, investigación y reparación de amenazas desde un panel de gestión de amenazas unificado.
La plataforma deberá poder ser administrada vía HTTPS y debe ser compatible con los navegadores Chrome, Firefox y Edge.
La solución debe ser fácil y rápida de usar, con configuraciones de políticas listas para usar.

Prevención Ataques
La solución debe proveer prevención en línea (no solo detección y/o remediación), es decir intercepción de enlaces antes que lleguen al usuario final.
La solución debe permitir el despliegue automático por integración nativa de API sin requerir cambios en los registros MX de DNS para prevenir ataques por correo.
La integración por API debe ser automática y sencilla de gestionar, debe permitir reglas granulares por usuarios y/o grupos que pueden estar en prevención y/o remediación y no requerir de configuraciones manuales del lado de la plataforma Microsoft 365.
La solución debe inspeccionar los metadatos, archivos adjuntos, enlaces e idioma de la comunicación, dominios, OCR, QR codes, así como todas comunicaciones históricas, para determinar relaciones de confianza previas entre el emisor y el recepto del correo para de identificar la suplantación de identidad del usuario o de los mensajes fraudulentos.
La solución debe ser totalmente compatible con los siguientes mecanismos de autenticación: • Sender Policy Framework (SPF), • Domain Keys Identified Mail (DKIM), • Domain-based Message Authentication, Reporting & Conformance (DMARC).
La solución debe contar con la opción de configuración de listas blancas y listas negras.
La solución debe detectar cuando los piratas informáticos utilizan el dominio de una empresa para hacerse pasar por la marca o sus empleados.
La solución debe inspeccionar enlaces cuando el usuario hace clic en la URL, Es decir re-escribir el(los) enlace(s).
La solución debe emular (sandboxing) los enlaces URL re-escritos para exponer indicadores de phishing ocultos.
La solución debe permitir a los administradores detectar a los usuarios que hicieron clic en los enlaces que resultaron maliciosos y que requieren mayor educación y capacitación para evitar hacer clic en enlaces maliciosos
La solución debe interactuar con Microsoft a través de la API, no debe generar interferencia cuando MS ATP o Defender inspecciona la URL antes que se reescriba la URL. Por lo tanto, puede usarse con MS ATP o Defender, como una capa adicional de protección.
La solución debe soportar la rescritura de URL embebidas incluso si son códigos QR.
La solución debe permitir que el administrador personalizar las plantillas que usaría para notificar a los usuarios finales sobre las amenazas
La solución debe tener un periodo de retención de archivos originales cuarentenados por al menos 180 días.
La solución debe tener un periodo de retención de los metadatos analizados maliciosos por al menos 180 días
La solución debe tener la capacidad de remediación las amenazas que llegan a las cuentas de los usuarios, desde la interfaz de gestión debe poder realizar la identificación, el análisis y la corrección. Si llega un archivo, y se pueden tomar medidas inmediatas en miles de bandejas de entrada con unos pocos clics, sin PowerShell ni codificación de ningún tipo.
La solución debe permitir que los usuarios puedan ayudar a detectar ataques perdidos y permitir que los administradores de seguridad bloqueen los ataques detectados y prevenir ataques similares en el futuro.
La solución debe integrarse con el este mecanismo reporte de suplantación de identidad de MS Outlook.
La solución debe permitir al administrador realizar personalizaciones o configurar excepciones en las reglas de seguridad basándose en al menos las siguientes opciones: • Hosts, • direcciones IP, • Usuarios,

• Dominios, • Cabeceras / Headers • Asunto • Links • Adjuntos
La solución debe permitir a los administradores bloquear automáticamente las URL procedentes de las fuentes de indicadores de compromiso (IOC)
Prevención de Malware en herramientas de colaboración y almacenamiento SaaS
Debe escanear malware a través de análisis estático
La solución debe tener protección antivirus/malware basado en firmas.
La solución debe permitir a los administradores configurar la lista de bloqueo cualquier tipo de archivo y marcado como malware y para los tipos de archivos (PDF, EML, HTML) optar por bloquear estos archivos en función de si contienen enlaces o no.
La solución debe detectar archivos como protegidos con contraseña al menos de las siguientes extensiones Documentos: Word, Excel, PowerPoint y PDF. Archivos: ZIP, 7Z, RAR, CAB, TAR, TAR.GZ, TGZ, GZ, BZ2, XZ, TXZ, TBZ2, TB2, TBZ, ISO, TAR.XZ, TAR.BZ2, CHM, IZH, RPM, WIM, ARJ, CPIO, CRAMFS, QCOW2, UDF, AR e IMG, ISO, AR.
Si un archivo esta como protegido con contraseña, la solución debe intentar extraer la contraseña mediante varias técnicas, como buscar la contraseña en el cuerpo del correo electrónico y si se encuentra la contraseña, debe usar la contraseña para descifrar el archivo e inspeccionarlo en busca de malware.
Si no se encuentra la contraseña, el administrador debe poder seleccionar alguna de las siguientes acciones: • Requerir que el usuario final ingrese una contraseña • El usuario recibe el correo electrónico con una advertencia. • Cuarentena. • Identificar el archivo como sospechoso de malware
Escanea todos los archivos intercambiados interna y externamente en busca de enlaces maliciosos, códigos u otros componentes de ataques avanzados".: Google Drive,ShareFile, OneDrive, Sharepoint, Box, Dropbox: de malware, ransomware, ataques laterales
La solución debe escanear y analizar cada archivo en busca de enlaces maliciosos que luego bloquear en todas sus aplicaciones para compartir archivos.
La solución debe detectar directamente el comportamiento malicioso y pone en cuarentena los archivos antes de que la amenaza se propague.
Brinda protección contra enlaces de phishing, código o archivos maliciosos y fuga de datos en plataformas de chat empresarial.
La solución debe a los administradores permitir y bloquear direcciones URL exactas y dominios completos en mensajes de Teams y Slack
Para Aplicaciones como OneDrive, SharePoint debe permitir por política dos tipos de acciones de remediación Cuarentena y Vault Folder (Carpeta bóveda)
Prevención de Malware de día Cero (sandboxing) en herramientas de colaboración y almacenamiento SaaS y Limpieza de Documentos
La solución debe incluir capacidades de “Sanboxing” resistente a la evasión para bloquear el malware de día cero, con un análisis dinámico en un entorno virtual aislado y escalable basado en la nube
La solución debe incluir el uso del análisis de sandboxing para revisar los archivos adjuntos y los recursos web asociados a los hipervínculos incluidos en los mensajes. Incluso debe tener la capacidad de ver un vídeo del resultante de la emulación.

El análisis de sandboxing debe obtener un veredicto respecto de un archivo adjunto o del recurso web asociado a un hipervínculo en un lapso no mayor a 5 minutos.
La solución debe ser capaz de sandboxing al menos los siguientes tipos de archivos: EXE, DLL, DOC, DOCX, XLS, XLSX, PPT, PPTX, JPG, PNG, PDF, SWF, JAVA (.jar, .js/.jse), VBS, scripts y archivos PowerShell (.ps1).
La solución debe permitir a los administradores puedan seleccionar los sistemas operativos que utilizará el sandbox del Anti-Malware para emular archivos. La Emulación debe soportar hacerlo en Win7, Win8.1, Win10 o inclusive Win11.
La solución debe admitir capacidades CDR (Content disarm and Reconstruction) es decir, podrá limpiar los documentos o imágenes adjuntos en los correos electrónicos de contenido malicioso.
La Solución CDR debe ser capaz al menos los siguientes tipos de archivos PDF, FDF, XLSX, XLSB, XLSM, XLTX, XLTM, XLAM, XLSB, XLS, PPTX, PPTM, POTX, POTM, PPAM, PPSX, PPSM, PPT, PPS, POT, PPA, DOCX, DOCM, DOTX, DOTM, DOC, DOT
Anomalías de usuarios y Detección de Cuentas comprometidas
La solución debe evitar ataques avanzados de apropiación de cuentas aumentando los procesos de autenticación, evitar usuarios no autorizados y los dispositivos comprometidos accedan a las aplicaciones SaaS
La solución debe contar con un motor analiza el comportamiento utilizando un algoritmo de aprendizaje automático utilizando un algoritmo de aprendizaje automático que crea un perfil basado en eventos históricos que incluyen ubicaciones y horas de inicio de sesión, comportamiento de transferencia de datos y patrones de mensajes.
La solución debe contar detecta comportamientos y acciones que parecen anormales cuando se observan en el contexto de una organización y la actividad histórica de un usuario.
Para identificar cuentas potencialmente comprometidas, Debe incluir un motor de inteligencia artificial para inspeccionar todos los parámetros de los eventos de inicio de sesión para identificar los realizados por actores malintencionados: • Detección basada en Inteligencia artificial de inicios de sesión anómalos • Iniciar la sesión desde una dirección IP maliciosa • Primera vez en un nuevo país • Acceso inusual desde un país • Acceso desde una geográfica sospechosa (viaje imposible) • Error de inicio de sesión sospechoso en MFA • El cliente es un navegador vulnerable.
La solución debe identificar un evento de seguridad que brinda el contexto e información necesaria para la investigación, debe clasificar como crítica o sospechosa.
La solución debe tener la capacidad de tomar las siguientes acciones de respuesta cuando detecte cuentas potencialmente comprometidas o cuentas secuestradas: • Bloquear la cuenta; • Restablecer la contraseña.
Las Anomalías Críticas y de inicio de sesión identificados de los usuarios comprometidos podrán ser bloqueadas automáticamente.
La solución debe permitir a los administradores configurar un buzón dedicado al que se enviarán alertas sobre cuentas comprometidas.
Bloqueo de cuentas que inicien se sesión desde direcciones IPs conocidas como maliciosas por una base de inteligencia del fabricante (TIP)
Entre los eventos que la solución debe analizar para identificar cuentas secuestradas (“account takeover”) deben incluirse: • El inicio de sesión;

• La ubicación desde donde se hizo el inicio de sesión; • Anomalías recientes • Acciones del usuario recientes
Shadow IT & Application Control
La solución detectará y proporcionará informes de aplicaciones de Shadow IT y top de usuarios.
La solución debe proporcionar un informe de evaluación de riesgos de la aplicación.
La solución debe indicar el uso de las aplicaciones a lo largo del tiempo
La solución debe Presentar las aplicaciones usadas según su categoría.
La solución debe permitir a probar una aplicación o crear lista blanca la aplicación
Data Lost Prevention (DLP) para herramientas de colaboración y almacenamiento SaaS
La solución debe contar con un motor de prevención de pérdida de datos (DLP) debe proteger los datos de la organización de posibles violaciones de datos o transmisiones de filtración de datos.
El motor DLP debe analizar archivos adjuntos, archivos compartidos y mensajes de texto publicados en las plataformas de colaboración y detecta patrones de datos que no deben compartirse con personas o destinos no autorizados.
El motor DLP debe permitir crear políticas para controlar cómo se comparten los archivos entre usuarios internos y externos. DLP identifica y marca archivos que contienen información confidencial, financiera y de identificación personal, incluidos números de tarjetas de crédito, números de seguro social, números de ruta bancaria o datos protegidos por HIPAA, etc.
La solución de DLP deberá admitir Expresiones Regulares, Diccionarios, personalizados definidos por el cliente.
La solución debe permitir configurar alertas por correo electrónicos para los administrados y usuarios para los correos electrónicos entrantes o salientes detectados que contienen una infracción de DLP.
La solución debe permitir a los administradores puedan configurar su directiva DLP para que los correos electrónicos se envíen cifrados
La solución debe permitir a los administradores puedan personalizar el portal agregado imágenes o logotipos.
La solución debe tener capacidad de integración cifrado de Microsoft 365 y Cualquier correo electrónico detectado no se entregará al destinatario y el usuario puede volver a enviar el correo electrónico como correo electrónico cifrado de Microsoft.
La solución debe permitir lista de remitentes / destinatarios individuales o dominios completos de la inspección de DLP para granularidad sobre la política.
Para Aplicaciones como OneDrive, SharePoint debe permitir por política dos tipos de acciones de remediación Cuarentena y Vault Folder (Carpeta bóveda)
La solución debe definir sensibilidades personalizadas para las reglas DLP, de modo que se active un flujo de trabajo diferente, dependiendo de la cantidad de datos confidenciales que se filtran.
Gestión de Eventos, Tableros, Reportes y Auditoria
La solución debe permitir gestionar los eventos de seguridad, ya sea que se detecten/prevengan automáticamente o que los administradores/usuarios finales encuentren después de no haber sido prevenidos.
La solución debe contar con una vista detallada de todos los eventos de seguridad en tiempo real. Mediante la búsqueda y los filtros, puede ver eventos relacionados con cualquier período de tiempo, estado, nivel de gravedad y SaaS.
La solución debe contar comuna vista centrada en las amenazas con información como - Usuarios involucrados en el evento (destinatarios, remitentes, propietarios de archivos compartidos)

- Información de quien remedio la amenaza que puede ser el administrador, por la herramienta de seguridad o por el proveedor de correo en nube
La solución debe proporcionar tableros análisis de eventos maliciosos detallados para cada aplicación SaaS.
Los Tableros (Dashboards) detallados de los eventos de seguridad por cada aplicación SaaS de almacenamiento y/o colaboración. Registrando la cantidad usuarios, archivos, recursos compartidos, enlaces, inicios de sesión, y detecciones de amenazas.
La solución deberá proveer reportes ejecutivos de eventos de seguridad de los última semana, dos semanas y últimos 30 días.
La solución debe permitir a los administradores programar informes de seguridad se envíen con diferentes zonas horarias y a diferentes destinatarios.
Debe proveer capacidades de investigación que apoyen los procesos de cacería de amenazas de la organización, poder realizar consultas a toda la metadata (archivos, inicios de sesión de usuario, etc.) capturada y almacenados en el tenant
La solución debe tener la posibilidad de exportar eventos a archivos CSV, json, xlsx
La solución deberá proveer reportes de los eventos por hasta 180 días, en formato csv o xlsx.
La solución debe permitir filtrar los correos electrónicos en función de su dirección, entrante, saliente e interno.
La solución debe contar con un tablero con el número de reportes phishing de los usuarios, solicitudes de restauración y socios de riesgo, así como una indicación de si las cuentas comprometidas se bloquean automáticamente o no.
La solución debe permitir a los administradores tener visibilidad del riesgo de los socios con los que comunican utilizando un motor de IA y recibir alertas sobre los socios que pueden estar comprometidos.
La solución debe permitir a los administradores puedan desencadenar una acción específica cuando el dominio del remitente se parece mucho al dominio de un socio, o evitar ataques de socios comprometidos
La solución debe permitir a los administradores puedan ver la justificación de los usuarios finales antes de aprobar / rechazar las solicitudes antes de liberar un correo de cuarentena
La solución debe brindar el detalle del análisis de un archivo identificado como malicioso incluyendo los comportamientos riesgosos que fueron identificados y las técnicas identificadas. EL resultado de la emulación de un archivo malicioso debe incluir un video indicando el resultado de emulación.
La solución debe permitir a los administradores pueden personalizar: - cuándo y cuántas veces al día sus usuarios finales reciben el informe de cuarentena (resumen). - La dirección de respuesta del informe de cuarentena diario enviado a los usuarios finales. - Los textos en el cuerpo y el asunto del informe diario de cuarentena del usuario final (resumen). - El texto del enlace en el que los usuarios hacen clic para generar un reporte.
La solución debe permitir a los administradores puedan configurar, para cada detección de Microsoft 365, si los usuarios finales pueden solicitar una restauración, restaurar por su cuenta o no pueden restaurar los archivos en absoluto.
Todas las solicitudes de restauración enviadas por los usuarios finales estarán disponibles para los administradores en el panel Solicitudes de restauración
La solución debe permitir a los administradores puedan cargar un logotipo personalizado para agregarlo a las notificaciones por correo electrónico, las páginas del navegador y los informes.
La solución debe permitir a los administradores puedan restringir el acceso al portal de la organización a una dirección IP o CIDR específica

La solución debe permitir desde portal de gestión que los administradores se mantengan actualizados sobre las actividades de mantenimiento y el estado del servicio.
La solución debe permitir a los administradores puedan definir buzones dedicados para recibir alertas sobre el estado del servicio
Integraciones a SIEMs y API
La solución ofertada debe permitir integrarse con soluciones SIEM vía syslog vía TCP o json vía HTTP
La solución debe soportar API Rest para administrar y actuar sobre los eventos de seguridad detectados

- Configurar la plataforma de modo que quede operativa la prevención y protección contra amenazas en herramientas de colaboración de Microsoft 365.

- Entregar documento de vigencia de licenciamiento al inicio del servicio

- Entregar informe final del servicio que incluya por lo menos (activación. Configuración, recomendaciones y manuales).

4.3 Lugar y plazo de prestación del servicio

4.3.1 Lugar

Por la naturaleza del servicio, la ejecución de este se realizará de manera remota desde las instalaciones del contratista.

4.3.2 Plazo

El plazo de activación de la suscripción y configuración será máximo de siete (7) días calendario contabilizados desde el día siguiente a la notificación del pedido de compra.

La vigencia de la licencia será de 365 días contados a partir de la activación de esta.

V. RECURSOS A SER PROVISTOS POR EL CONTRATISTA

5.1 Personal

A. Personal clave

a. Jefe de Proyecto

i. Actividades

- Desarrollar el plan de trabajo para el servicio.
- Facilitar recursos para la ejecución de actividades
- Supervisar al ingeniero que realice la implementación
- Presentación de los entregables del servicio
- Cerrar el proyecto

b. Especialista implementador

i. Actividades

- Realizar la activación de la suscripción.
- Configurar los accesos, reglas y controles en la plataforma.
- Desarrollar el documento de vigencia de suscripción de licencia.
- Desarrollar el informe final del servicio.

VI. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

6.1 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.

6.2 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 Tecnologías de información y Comunicaciones en el plazo máximo de siete (7) días computados desde el día siguiente de producida la recepción.

6.3 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 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 la configuración de plataforma)
- Documento de vigencia de licencia.

6.4 Modalidad de Pago

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

6.5 Penalidades

6.5.1 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.

6.6 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 1 año(s) contado a partir de la conformidad otorgada por LA ENTIDAD CONTRATANTE.

6.7 Requisitos de Seguridad, Salud Ocupacional y Medio Ambiente

SALAS BELLO Julio Miguel FAU 20216293593 hard

Firmado digitalmente por SALAS BELLO Julio Miguel FAU 20216293593 hard
Motivo: NO APLICA
Fecha: 2025.12.04 15:48:35 -05'00'

No aplica

6.8 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.

[1] Artículo 9 de la Ley N°32069, Ley General de Contrataciones Públicas.

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].

6.9 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 con 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.

[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.

6.10 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.

6.11 Gestión de riesgos.

No aplica.

6.12 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 03/12/2025

VII. REQUISITOS DE CALIFICACIÓN

7.1 Experiencia del Personal Clave.

Requisitos:

a. Jefe de Proyecto
El Jefe de Proyecto deberá tener experiencia mínima de tres (03) años asumiendo roles de Jefe de Tecnologías de Información y/o Jefe de Proyectos y/o Jefe de Infraestructura y Comunicaciones y/o Asistente de sistemas y/o Redes y/o Bases de Datos.

b. Especialista implementador
El especialista implementador de la plataforma deberá tener experiencia mínima de un (01) año en actividades relacionadas a implementación y/o instalación de equipos de seguridad de redes, y/o instalación y/o soporte de servidores windows y/o soluciones de correo electrónico y/o ciberseguridad.

Acreditación:

La experiencia profesional 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.

7.2 Formación académica.

Requisitos:

a. Jefe de Proyecto
Contar con bachiller o Título profesional en Ingeniería en Informática y/o Ingeniería de Sistemas y/o Ingeniería Electrónica.

b. Especialista implementador
Como mínimo contar con Bachiller en ingeniería de sistemas y/o título técnico en sistemas y/o computación y/o informática y/o administración de redes y/o comunicaciones.

Acreditación:

El titulo técnico y/o bachiller será verificado por los evaluadores en el Registro Nacional de Grados Académicos y Titulo 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: https://titulosinstitutos.minedu.gob.pe/, según corresponda.

En caso de que el título profesional no se encuentre inscrito en los referidos registros, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

7.3 Capacitación del personal clave

Requisitos:

a. Jefe de Proyecto
Contar con las siguientes certificaciones:
- 50 horas lectivas y/o académicas de Seguridad en Redes.

Acreditación:

Se acreditará con copia simple de constancias, certificados, u otros documentos, según corresponda.

7.4 Experiencia del postor en la especialidad

Requisitos:

El postor debe acreditar una experiencia mínima de S/. 80,000.00 (ochenta Mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto del presente requerimiento.

Se consideran servicios similares a los siguientes: Venta y/o Licenciamiento y/o Renovación de hardware y/o software de ciberseguridad, y/o licenciamiento de Firewalls y/o solución de seguridad perimetral y/o software de ciberseguridad.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de: copias simples (i) contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia en servicios iguales o similares a los solicitados.

Firmado digitalmente por QUIROZ GOMEZ Jorge Luis FAU 20216293593 hard
Fecha: 2025.12.04 14:39:57 -05'00'

Firmado digitalmente por CHIRINOS VELA Maryluz Concepcion FAU 20216293593 hard
Motivo: DEC
Fecha: 2025.12.12 11:29:58 -05'00'