TÉRMINOS DE REFERENCIA

ASESORÍA Y/O CONSULTORÍA DE CERTIFICACIÓN DEL SGSI

1. DENOMINACIÓN DE LA CONTRATACIÓN

Asesoría y/o Consultoría de Certificación del Sistema de Gestión de Seguridad de la Información

2. ÁREA USUARIA QUE REQUIERE EL SERVICIO

Departamento de Tecnologías de Información.

3. ANTECEDENTES

a) Mediante Resolución Directoral N° 022-2022-INACAL/DN, se aprueba la Norma Técnica Peruana "NTP-ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 3ª Edición."

b) Mediante Resolución N° 080-2022-2023-OM-CR, se actualizó y aprobó la Política General de Seguridad de la Información del Congreso de la República.

4. FINALIDAD PÚBLICA DE LA CONTRATACIÓN

Estando vigente la Política de Seguridad de la Información mediante el cual: "El Congreso de la República del Perú, en representación de todos los peruanos, legisla y ejerce el control político, además de cumplir con las funciones esenciales establecidas en la Constitución Política del Perú, de manera eficaz y transparente, en procura del bienestar general y la consolidación del sistema democrático. Para el ejercicio de dichas funciones valoramos la importancia y necesidad de proteger los activos de información, en cumplimiento con la normativa vigente y con los objetivos estratégicos de la institución. El Oficial Mayor, en nombre de todo el personal, se compromete a cumplir los objetivos de seguridad de la información."

En ese sentido, es necesario asegurar el cumplimiento de la Norma Técnica Peruana NTP ISO/IEC 27001:2022, de implementación obligatoria para las instituciones públicas, mediante la obtención de la Certificación ISO/IEC 27001:2022 del Sistema de Gestión de Seguridad de la Información (SGSI) del Congreso de la República, dentro de un alcance definido.

Por lo tanto, el objetivo es contratar los servicios de un organismo certificador externo (en adelante, organismo certificador), independiente y acreditado para llevar a cabo la preauditoría y la auditoría de certificación, con el fin de acreditar el cumplimiento de los requisitos establecidos por el estándar internacional ISO/IEC 27001:2022 y su equivalente NTP-ISO/IEC 27001:2022 en el Perú.

Este proceso permitirá al Congreso de la República obtener la certificación de su Sistema de Gestión de Seguridad de la Información (SGSI), en el alcance definido para dicho sistema.

5. VINCULACIÓN CON EL PLAN OPERATIVO INSTITUCIONAL

CÓDIGO	ACTIVIDAD OPERATIVA
202504025160002	Operación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información

6. CARACTERÍSTICAS DEL SERVICIO A REALIZAR

6.1 ESTADO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En el año 2008, el Congreso de la República realizó el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), con la finalidad de asegurar el cumplimiento de los objetivos específicos de seguridad de la información, de acuerdo a lo establecido en la ISO 27001:2005-SGSI y a las recomendaciones establecidas en la "NTP-ISO/EC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información".

En los años 2010 y 2011, el Congreso de la República realizó la actualización y pruebas del Plan de Continuidad de Operaciones con la finalidad de afrontar organizadamente cualquier evento o desastre mayor que ponga en riesgo la continuidad operacional de TI del Congreso.

En el año 2012, mediante Resolución N° 060-2011-2012-OM/CR, se aprueba la Directiva N° 02-2012- DGA/CR "Política General de Seguridad de la Información" y en el año 2015, el Congreso actualizó su Sistema de Gestión de Seguridad de la Información conforme a la nueva versión de la norma NTP ISONEC 27001:2014.

En el año 2016, se actualizó y aprobó la Directiva N° 07-2016-DGA/CR "Política General de Seguridad de la Información" del Congreso de la República, mediante resolución de Oficialía Mayor N° 088-2015- 2016-OM-CR, y la Dirección General de Administración (DGA) aprobó los documentos de operación del SGSI del Congreso de la República, de acuerdo a los requisitos de la Norma NTP ISONEC 27001:2014.

En el año 2020, se ejecutó el "Servicio de Formulación del Plan de Continuidad Operativa de TI" el cual concluyó en una propuesta del Plan de Continuidad Operativa de TI.

En el año 2022, mediante Resolución N° 080-2022-2023-OM-CR, se actualizó y aprobó la Política General de Seguridad de la Información del Congreso de la República.

6.2 ALCANCE Y DESCRIPCION DEL SERVICIO

El Congreso de la República requiere asegurar su SGSI basado en la norma NTP ISO/IEC 27001:2022.

El sistema de gestión comprende un proceso que se encuentra dentro del cercado de Lima, siendo este el siguiente:

Proceso	Servicios de información que dan soporte al proceso de gestión del centro de datos.
Descripción	El proceso de servicios de información que dan soporte al proceso de gestión del centro de datos busca garantizar que este funcione sin interrupciones, asegurando que no se tengan periodos de indisponibilidad que impida el acceso a la información inherente a las funciones de la entidad.
Sedes	Jirón Huallaga 358, Cercado de Lima Plaza Bolívar Avenida Abancay S/N, Cercado de Lima

Exclusión	El Congreso reconoce que la implementación solo alcanza al proceso de "servicios de información que dan soporte al proceso de gestión del centro de datos".

6.3 Actividades

6.3.1 Fase 1: Preauditoría de Certificación

Esta actividad tiene como principal objetivo la evaluación integral y detallada del SGSI del Congreso de la República (en el alcance descrito en el numeral 6.2), para identificar, analizar y confirmar aquellos aspectos y requisitos que aún no se han cubierto, contemplado o solventado de manera satisfactoria en la implementación, respecto de los requisitos de la norma ISO/IEC 27001:2022.

Se requiere un plan de preauditoria de certificación que contenga como mínimo:

i) Introducción

- Objetivo de la pre-auditoría.
- Descripción del alcance del sistema de gestión a evaluar.
- Referencia a la norma ISO/IEC 27001:2022 y su equivalente NTP.

ii) Alcance

- Procesos y áreas de la institución que serán evaluados.
- Inclusiones y exclusiones específicas (si las hay).
- Sedes y ubicaciones donde se realizará la evaluación.

iii) Metodología

- Descripción de las etapas de la pre-auditoría (Etapa 1 y Etapa 2).
- Herramientas y técnicas que se utilizarán (revisión documental, entrevistas, observaciones, etc.).

iv) Cronograma

- Duración de cada etapa de la pre-auditoría.
- Fechas previstas para las actividades principales.
- Plazos para la entrega de los informes.

v) Equipo auditor

- Identificación de los auditores responsables.
- Roles y responsabilidades de cada miembro del equipo.
- Participación de auditores internos de la institución como observadores (si corresponde).

vi) Áreas y temas a evaluar

- Validación del diseño y documentación del SGSI (Etapa 1).
- Evaluación de la implementación efectiva del SGSI en sitio (Etapa 2).

vii) Resultados esperados

- Lista de entregables (informes, reportes de hallazgos, recomendaciones).

viii) Requisitos Logísticos

- Recursos requeridos (acceso a documentación, entrevistas con personal clave, espacios físicos o virtuales para reuniones).

ix) Criterios de Evaluación

- Indicadores de conformidad y no conformidad.
- Normas y lineamientos aplicables (ISO 19011, ISO/IEC 27001:2022).

La fase 1 Preauditoría de Certificación comprende dos etapas:

a) Etapa 1- Preauditoría:

- Evaluación de la documentación del sistema de gestión, para validar el alcance de certificación previsto.
- Revisión de la idoneidad del diseño del sistema de gestión con respecto a las operaciones y riesgos de la institución, verificando su conformidad con los requerimientos de la norma ISO/IEC 27001:2022, así como la confirmación del alcance de la certificación.

b) Etapa 2 - **Preauditoría**

- Evaluación in situ (presencial) del grado de implementación efectiva en la institución respecto de los requisitos de la norma ISO/IEC 27001:2022.
- Al finalizar esta etapa, el Organismo Certificador deberá proporcionar un informe detallado con los resultados de la evaluación.
- Si se identifican no conformidades mayores, observaciones o recomendaciones que imposibiliten la certificación, el Organismo Certificador otorgará a la entidad un plazo, según la naturaleza del hallazgo, para su subsanación, la cual será verificada en una etapa posterior.

6.3.2 Fase 2: Auditoría de Certificación

Se requiere un plan de auditoría de certificación que contenga, como mínimo:

i) Introducción

- Propósito de la auditoría de certificación.
- Importancia de la certificación para la institución.
- Referencia a la norma ISO/IEC 27001:2022 y su equivalente NTP.

ii) Alcance de la auditoría

- Definición del sistema, procesos y áreas incluidos.
- Exclusiones justificadas (si las hay).

- Sedes involucradas en la auditoría.

iii) Metodología

- Detalle de las etapas de la auditoría (Etapa 1 y Etapa 2).
- Técnicas de evaluación: entrevistas, observación directa, revisión de registros.

iv) Cronograma

- Fechas clave para cada etapa.
- Duración estimada de cada actividad de auditoría.
- Plazo para la entrega del informe final.

v) Equipo auditor

- Nombres y credenciales de los auditores.
- Roles y responsabilidades específicas.
- Observadores designados por la institución.

vi) Áreas y temas a evaluar

- Evaluación de documentación y diseño del SGSI (Etapa 1).
- Implementación y eficacia del SGSI en sitio (Etapa 2).

vii) Criterios de Evaluación

- Normas aplicables y directrices específicas.
- Indicadores de conformidad y no conformidad.

viii) Resultados esperados

- Informe de Auditoría Etapa 1.
- Informe de Auditoría Etapa 2.
- Recomendación de certificación (si corresponde).
- Certificado ISO/IEC 27001:2022 con validez de tres años.

ix) Requisitos logísticos

- Espacios físicos o virtuales para reuniones.
- Acceso a documentación, registros y personal clave.

x) Consideraciones finales

- Proceso de resolución de no conformidades mayores y menores.
- Plan de seguimiento para recomendaciones de mejora.

La fase 2 Auditoría de Certificación comprende dos etapas:

a) Auditoría Etapa 1:

- Evaluación de la documentación subsanada del sistema de gestión, de ser el caso, u otros aspectos que el Organismo Certificador considere pertinentes.
- Revisión de la idoneidad de las mejoras en el diseño del sistema de gestión respecto a las operaciones y riesgos de la institución, para verificar la conformidad con los requerimientos de la norma ISO/IEC 27001:2022.

b) Auditoría Etapa 2:

- Evaluación in situ (presencial) del grado de implementación efectiva en la institución respecto de los requisitos de la norma ISO/IEC 27001:2022.
- El Organismo Certificador entregará un informe detallado con los resultados de la evaluación.
- En caso de identificarse no conformidades mayores, el Organismo Certificador otorgará un plazo no menor a 90 días calendario para su subsanación, verificable en una visita posterior cuya duración dependerá de la naturaleza del hallazgo.

6.3.3 Características del servicio

a) Se espera que las auditorías efectuadas por el Organismo Certificador, independiente y acreditado para llevar a cabo la preauditoría y la auditoría de certificación, sean provechosas y aporten valor para la entidad, mediante un proceso de evaluación enfocado en las áreas y temas importantes. Esto permitirá identificar oportunidades de mejora que contribuyan a que las sedes del Congreso de la República, ubicadas en Jirón Huallaga 358, Cercado de Lima, y Plaza Bolívar, Avenida Abancay S/N, Cercado de Lima, ofrezcan servicios comprometidos con el concepto de mejora continua.

b) El proceso de evaluación debe ajustarse a las características de la institución y al alcance de la certificación. Los procesos de auditoría deben cumplir con los lineamientos establecidos en la Norma ISO 19011. La entidad designará auditores internos en calidad de observadores para presenciar las actividades comprendidas en el presente servicio.

6.3.4 PROCEDIMIENTO Y METODOLOGIA

Metodología de Trabajo: Se llevarán a cabo reuniones de trabajo con las distintas áreas de la Institución involucradas dentro del alcance del SGSI, en coordinación con el Oficial de Seguridad y Confianza Digital.

Normas: Las actividades y entregables, deberán desarrollarse conforme a los lineamientos y requisitos exigidos por la Norma:

- ISO 19011:2018 - Directrices para la auditoría de sistemas de gestión.
- NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición

- NTP-ISO/IEC 27002:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición
- NTP-ISO/IEC 27003:2019 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Orientación. 2ª Edición
- NTP-ISO/IEC 27004:2018 Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Seguimiento, medición, análisis y evaluación. 2ª Edición
- NTP-ISO/IEC 27005:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición
- NTP-ISO/IEC 27006:2009 (revisada el 2021) Tecnología de la información. Técnicas de seguridad. Requisitos para los organismos que realizan auditorías y certificaciones de los sistemas de gestión de la seguridad de la información.
- NTP-ISO/IEC 27007:2020 Seguridad de la información, ciberseguridad y protección de la privacidad. Directrices para la auditoría de sistemas de gestión de seguridad de la información
- NTP-ISO/IEC 27017:2018 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de la seguridad de la información basado en la ISO/IEC 27002 para los servicios de nube. 1ª Edición
- ISO/IEC 27035-1:2023, ISO/IEC 27035-2:2023 e ISO/IEC 27035-3:2020. Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información
- ISO/IEC 27036-1:2021, ISOIEC 27036-2:2022 e ISO/IEC 27036-3:2023. Ciberseguridad. Relación con proveedores

7 PRODUCTOS A OBTENER

7.1. Entregables de la Fase 1

a) Planificación del Proyecto, cronograma de actividades y Plan de preauditoría de certificación

A los cinco (05) días calendario contados a partir del día siguiente de la firma del contrato, se deberá presentar:

- Plan de proyecto, cronograma de actividades y plan de preauditoría de certificación.

La entidad tendrá el pazo de un (01) día calendario para la aprobación del mencionado plan de proyecto y cronograma de actividades.

b) Informe de preauditoría de certificación (Etapa 1)

A los cuarenta (40) días calendario contados a partir del día siguiente de la firma del contrato. Dicho informe detalla la evaluación de la documentación del sistema de gestión, incluyendo la validación del alcance de certificación previsto y el análisis de la idoneidad del diseño del sistema en relación con los riesgos y

operaciones de la institución, así como las recomendaciones preliminares para solventar hallazgos relacionados con la documentación y el diseño del SGSI.

c) Informe de preauditoría de certificación (Etapa 2)

A los sesenta (60) días calendario contados a partir del día siguiente de la firma del contrato. Dicho informe detalla los resultados de la evaluación in situ (presencial), incluyendo el nivel de implementación efectiva del SGSI según los requisitos de la norma ISO/IEC 27001:2022, así como la identificación de no conformidades, observaciones y recomendaciones, con plazos sugeridos para su subsanación.

7.2. Entregables de la Fase 2

a) Plan de auditoría de certificación

A los setenta (70) días calendario contados partir del día siguiente de la firma del contrato. Dicho informe detalla los resultados de la evaluación in situ (presencial), incluyendo el nivel de implementación efectiva del SGSI según los requisitos de la norma ISO/IEC 27001:2022, así como la identificación de no conformidades, observaciones y recomendaciones, con plazos sugeridos para su subsanación.

b) Informe de auditoría de certificación (Etapa 1)

A los doscientos cuarenta (240) días calendario contados a partir del día siguiente de la firma del contrato. Dicho informe analiza la documentación subsanada, las mejoras realizadas en el diseño del sistema de gestión, y la evaluación de conformidad con los requisitos de la norma ISO/IEC 27001:2022.

c) Informe de auditoría de certificación (Etapa 2)

A los doscientos sesenta (260) días calendario contados a partir del día siguiente de la firma del contrato. Dicho informe detalla los resultados de la evaluación in situ (presencial), indicando el grado de implementación efectiva y cualquier hallazgo adicional, así como la recomendación de certificación, de ser el caso.250+6

d) Entrega de certificados originales de certificación

A los trescientos diez (310) días calendario contados a partir del día siguiente de la firma del contrato. Entrega de tres (3) Certificados originales como documento físico, que acrediten que el Sistema de Gestión de Seguridad de la Información, cumple con los requisitos de la Norma ISO 27001:2022 con una validez de tres (3) años (de recomendarse la certificación)

8. PLAZO DE EJECUCIÓN DEL SERVICIO

La prestación del servicio tendrá una duración de doscientos cuarenta (310) días calendario contados a partir del día siguiente de firmado el contrato.

ENTREGABLES	PLAZO (Contados a partir del día siguiente de firmado el contrato)
Planificación del Proyecto, cronograma de actividades y Plan de preauditoría de certificación	5 días calendario
Informe de preauditoría de certificación (Etapa 1)	40 días calendario

Informe de preauditoría de certificación (Etapa 2)	60 días calendario
Plan de auditoría de certificación	70 días calendario
Informe de auditoría de certificación (Etapa 1)	240 días calendario
Informe de auditoría de certificación (Etapa 2)	260 días calendario
Entrega de certificados originales de certificación	310 días calendario

9. CONFORMIDAD DE PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio será otorgada por el Oficial de Seguridad y Confianza Digital y refrendada por el/la jefe/a del Departamento de Tecnologías de la Información, luego de recibido y validado los respectivos entregables, la conformidad será realizada en un plazo de hasta siete (07) días de acuerdo a lo establecido en el numeral 144.3 del artículo 144° del Reglamento de la Ley General de Contrataciones Públicas.

10. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en pagos a cuenta, de conformidad a:

ENTREGABLES	PORCENTAJE (Monto propuesta)
Informe de preauditoría de certificación (Etapa 1)	20 %
Informe de preauditoría de certificación (Etapa 2)	20 %
Informe de auditoría de certificación (Etapa 1)	20%
Informe de auditoría de certificación (Etapa 2)	20 %
Entrega de certificados originales de certificación	20 %

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, deberá contar con la conformidad correspondiente emitida por el Oficial de Seguridad y Confianza Digital y refrendado por el/la jefe/a del Departamento de Tecnologías de la Información, ello en concordancia el numeral 67.3 del artículo 67° de la Ley General de Contrataciones Públicas.

En el caso que se haya suscrito contrato con un consorcio, el pago se realiza, a quien corresponda, de acuerdo con lo que se indique en el contrato de consorcio.

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

- Documento en el que conste la conformidad de la prestación otorgada por el Oficial de Seguridad y Confianza Digital y refrendada por el/la jefe/a del Departamento de Tecnologías de la Información.
- Comprobante de pago.

5.6 SOLUCIÓN DE CONTROVERSIAS CONTRACTUALES:

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, cuando se haya pactado y arbitraje.

Para el arbitraje, el postor ganador de la buena pro selecciona a una de las siguientes Instituciones Arbitrales para administrar el arbitraje:

- El Centro Internacional de arbitraje de la Cámara de Comercio de Lima.
- EL Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú-CARC PUCP.
- Centro de arbitraje Popular Arbitra Perú

11. LUGAR DE EJECUCION DEL SERVICIO

El servicio será ejecutado en las instalaciones del Congreso de la República. Para efectos de la prestación del servicio, se requiere que los consultores participen activamente y en forma presencial y/o remota, previa coordinación durante la ejecución del servicio. La entidad no brindará equipos de cómputo para dicho servicio.

12. MODALIDAD DE PAGO

Suma Alzada.

13. REQUISITOS MINIMOS DEL PERSONAL

La empresa deberá proveer los recursos humanos necesarios para el desarrollo de todas las actividades solicitadas en el servicio; el contratista tendrá que garantizar que todo el personal asignado cuente con equipos informáticos, computadoras personales (laptops), útiles de escritorio (lapiceros, lápiz, cuadernillos), licenciamiento de software para las labores generales de oficina (sistema operativo, software de ofimática) así como el software especializado de ser necesario, para que permita el inicio y la finalización del trabajo.

El contratista deberá garantizar la confidencialidad de la información proporcionada, y se abstendrá de comentar o dar opción a terceras personas ajenas al proyecto.

El contratista deberá presentar las copias simples de los certificados vigentes de cada miembro que forman parte del personal clave, que ejecutaran este servicio.

Para la suscripción de contrato el postor ganador deberá presentar los certificados vigentes para el Auditor Líder (1) y los Auditores (2), que conforman el Equipo, según el siguiente detalle:

a) Auditor Líder (1)
   Contar con la certificación vigente de Auditor Líder extendida por Organismo Acreditado en la norma ISO 27001.

b) Equipo Auditor (2)
   Contar con certificación vigente como Auditor en la Norma a Certificar, ISO 27001, extendida por Organismo Acreditado.

14. OTRAS CONSIDERACIONES ADICIONALES

14.1 COLEGIATURA

En caso el proveedor presente profesionales en Ingeniería, éstos deberán ser Colegiados y estar habilitados de acuerdo a lo indicado en la Ley N° 28858 y su Reglamento, dicha documentación será presentada al inicio del servicio.

15. PENALIDADES POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, 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 del Reglamento de la Ley General de Contrataciones Públicas.

La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

Penalidad diaria = (0.10 x monto)/ (F x plazo)

Donde F tiene los siguientes valores:
Para bienes y servicios: F = 0.40

Tanto el monto como el plazo se refiere, según corresponda, al monto vigente del contrato, componente o ítem que debió ejecutarse o, en caso de que estos involucren entregables cuantificables en monto y plazo, al monto y plazo del entregable que fuera materia de retraso.

16. OTRAS PENALIDADES

N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento de verificación
1	En caso el contratista incumpla con su obligación de ejecutar la prestación con el personal acreditado o debidamente sustituido.	50% de una UIT por cada día de ausencia del personal.	Mediante informe del área usuaria.
2	Por día de atraso en el entregable: Planificación del Proyecto, cronograma de actividades y Plan de preauditoría de certificación	5% de una UIT por cada día de atraso.	Mediante informe del área usuaria.
3	Por día de atraso en el entregable: Informe de preauditoría de certificación (Etapa 1)	5% de una UIT por cada día de atraso.	Mediante informe del área usuaria.
4	Por día de atraso en el entregable: Informe de preauditoría de certificación (Etapa 2)	5% de una UIT por cada día de atraso.	Mediante informe del área usuaria.
5	Por día de atraso en el entregable: Plan de auditoría de certificación	5% de una UIT por cada día de atraso.	Mediante informe del área usuaria.
6	Por día de atraso en el entregable: Informe de auditoría de certificación (Etapa 1)	5% de una UIT por cada día de atraso.	Mediante informe del área usuaria.

N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento de verificación
7	Por día de atraso en el entregable: Informe de auditoría de certificación (Etapa 2)	5% de una UIT por cada día de atraso.	Mediante informe del área usuaria.
8	Por día de atraso en el entregable: Entrega de certificados originales de certificación	5% de una UIT por cada día de atraso.	Mediante informe del área usuaria.

La suma de la aplicación de las penalidades por mora y otras penalidades no debe exceder el 10% del monto vigente del contrato o, de ser el caso, del ítem correspondiente.

17. VICIOS OCULTOS

El contratista es responsable por la calidad ofrecida y los vicios ocultos por un plazo de un (01) año contado a partir de la conformidad otorgada por la entidad.

18. ACUERDO DE CONFIDENCIALIDAD

El contratista y su personal se obligan a mantener y guardar estricta reserva y absoluta confidencialidad sobre todos los documentos e informaciones del Congreso de la República a los que tenga acceso en ejecución del presente contrato. En tal sentido, El Contratista y su personal deberán abstenerse de divulgar tales documentos e informaciones, sea en forma directa o indirecta, a personas naturales o jurídicas, salvo autorización expresa y por escrito del Congreso de la República. Asimismo, El Contratista y su personal convienen en que toda la información suministrada en virtud de este contrato es confidencial y de propiedad del Congreso de la República, no pudiendo El Contratista y su personal usar dicha información para uso propio o para dar cumplimiento a otras obligaciones ajenas a las del presente contrato.

Los datos de carácter personal entregados por el Congreso de la República a El Contratista y su personal, y obtenidos por estos durante la ejecución del servicio, única y exclusivamente podrán ser aplicados o utilizados para el cumplimiento de los fines del presente documento contractual.

El Contratista se compromete a cumplir con lo indicado en la ley N* 29733, Ley de protección de datos personales.

El Contratista deberá adoptar las medidas de índole técnica y organizativa necesarias para que sus trabajadores, directores, accionistas, proveedores y en general, cualquier persona que tenga relación con El Contratista no divulgue a ningún tercero los documentos e informaciones a los que tenga acceso, sin autorización expresa y por escrito del Congreso de la República, garantizando la seguridad de los datos de carácter personal y evitar su alteración. Asimismo, El Contratista se hace responsable por la divulgación que se pueda producir, y asumen el pago de la indemnización por daños y perjuicios que la autoridad competente determine.

El Contratista se compromete a devolver todo el material que le haya proporcionado por el Congreso de la República a los dos (02) días calendarios siguientes de la culminación o resolución del contrato, sin que sea necesario un requerimiento previo. Sin embargo, El Contratista se encuentra facultado a guardar copia de los documentos producto del resultado de la prestación del servicio, siendo el Congreso de la República el único que

pueda acceder a dicha información. Dicha copia no puede ser dada a terceros, salvo autorización expresa y por escrito del Congreso de la República.

La obligación de confidencialidad establecida en la presente clausula seguirá vigente incluso luego de la culminación del presente contrato, hasta por cinco (05) años.

19. CLAUSULA ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción de este contrato, 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

[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

20. REQUISITOS DE CALIFICACIÓN

A	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 159,000.00 (Ciento noventa mil y 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince (15) años anteriores a la fecha de la presentación de ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran servicios similares a los siguientes: Servicio de certificación del Sistema de Gestión de Seguridad de la Información ISO/IEC 27001 y/o Servicio de recertificación del Sistema de Gestión de Seguridad de la Información ISO/IEC 27001 y/o Servicio de certificación y seguimiento del Sistema de Gestión de Seguridad de la Información ISO/IEC 27001. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago10, correspondientes a un máximo de veinte (20) contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados 11 , para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación. En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo correspondiente referido a la Experiencia del Postor en la Especialidad. En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los quince (15) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo correspondiente. Las personas jurídicas resultantes de un proceso de reorganización societaria no pueden acreditar como experiencia del postor en la especialidad que le hubiesen transmitido como parte de dicha reorganización las personas jurídicas sancionadas con inhabilitación vigente o definitiva. Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicio o de cancelación del comprobante de pago, según corresponda.

	Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo correspondiente referido a la Experiencia del Postor en la Especialidad.

B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.1	**EXPERIENCIA DEL PERSONAL CLAVE**

Requisitos:

a) El personal Clave Auditor Líder (Cantidad 1)
Contar con experiencia no menor a cuatro (04) años realizando auditorias de Certificación y/o Recertificación y/o Seguimiento, bajo la metodología de la norma 27001.

b) Equipo Auditor
Auditor (Cantidad 2)

Contar con experiencia no menor a tres (03) años realizando auditorias de Certificación y/o Recertificación y/o Seguimiento, bajo la metodología de la norma 27001.

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

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.

Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.
En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.
Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

Importante

- *El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores. Asimismo, los trabajos o prestaciones que se le requiera acreditar deben estar relacionados con la actividad especifica que realizará durante la ejecución contractual.*

- *Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función*

	propia del cargo o puesto requerido en las bases.
B.2	**CALIFICACIONES DEL PERSONAL CLAVE**
B.2.1	**FORMACIÓN ACADÉMICA**
	Requisitos: a) Auditor Líder (1) Título Profesional o con Grado de Bachiller en cualquiera de las siguientes formaciones académicas: Ingeniería en Sistemas de Información, Ingeniería de Redes y Comunicaciones, Ingeniería de Computación y Sistemas, Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería Industrial, Ingeniería Informática, Ingeniería de Software o Licenciado en Computación. b) Equipo Auditor (Auditores (2) Título Profesional o con Grado de Bachiller en cualquiera de las siguientes formaciones académicas: Ingeniería en Sistemas de Información, Ingeniería de Redes y Comunicaciones, Ingeniería de Computación y Sistemas, Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería Industrial, Ingeniería Informática, Ingeniería de Software o Licenciado en Computación. Acreditación: El Título Profesional o con Grado de Bachiller requerido, será verificado por los evaluadores 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: *https://titulosinstitutos.minedu.gob.pe/* , según corresponda. El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido. En caso el Título Profesional o con Grado de Bachiller requerido, 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. En caso se acredite estudios en el extranjero del personal clave, debe presentarse adicionalmente copia simple del documento de la revalidación o del reconocimiento ante SUNEDU, del grado académico o título profesional otorgados en el extranjero, según corresponda.