TÉRMINOS DE REFERENCIA

CONSULTORÍA PARA EL II CICLO DE OPERACIÓN, MANTENIMIENTO Y MEJORA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. DEPENDENCIA QUE REQUIERE EL SERVICIO

Departamento de Tecnologías de Información.

2. ANTECEDENTES

a) El Congreso de la República, con el objetivo de establecer una adecuada gestión de seguridad de la información implementó en el año 2016 un Sistema de Gestión de Seguridad de la Información (SGSI) tomando como base normativa la NTP ISO/IEC 27001:2013.

b) Mediante Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, se establece un marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno.

c) Asimismo, el artículo 33 del referido Decreto Legislativo, establece que la Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno.

d) Mediante Resolución Ministerial N° 119-2018-PCM modificado por Resolución Ministerial Nº 087-2019-PCM, de fecha 19 de marzo de 2019, se dispone la creación de un Comité de Gobierno Digital en cada entidad de la administración pública, a fin de contar con un mecanismo de gobierno para la dirección, evaluación y supervisión del proceso de transformación digital y Gobierno Digital en las entidades de la Administración Pública a fin de contribuir con el cumplimiento de sus objetivos y planes institucionales.

e) Asimismo, mediante Decreto Supremo N°029-2021-PCM, “Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo”, se precisa, en el artículo 105, inciso a), que las entidades públicas tienen, como mínimo, la obligación de “Implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI)”.

f) 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.”

g) 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.

Firmado digitalmente por: MOSCAIZA MONCADA Omar Israel FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 11/05/2026 15:41:04-0500

Firmado digitalmente por: SUEYRAS LOSTAUNAU Luis Alberto FAU 20161749126 soft
Motivo: Doy V° B°
Fecha: 11/05/2026 16:57:40-0500

3. OBJETIVO DEL SERVICIO

Contratar el servicio de consultoría para el II ciclo de operación, mantenimiento y mejora Sistema de Gestión de Seguridad de la Información del Congreso de la República, alineado a 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", considerando las actualizaciones y cambios que se requieren implementar para la alineación a la normatividad vigente.

4. FINALIDAD PÚBLICA

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, conforme a la norma NTP ISO/IEC 27001:2022 es necesario asegurar su alineamiento, sostenibilidad y cumplimiento normativo, mediante su operación, mantenimiento y mejora continua.

5. VINCULACIÓN CON EL PLAN OPERATIO INSTITUCIONAL

CÓDIGO	ACTIVIDAD OPERATIVA
202604025160001	Operación, Mantenimiento y Mejora del Sistema de Gestión de Seguridad de la Información

6. CONDICIONES DE CONTRATACIÓN

6.1 Modalidad de pago

El contrato se rige por la modalidad de suma alzada, de conformidad con el artículo 130 del Reglamento.

6.2 Sistema de entrega

No aplica

6.3 Plazo de prestación del servicio

El plazo para la prestación del servicio materia de la presente convocatoria es de doscientos cuarenta (240) días calendario, contados a partir del día siguiente de la suscripción del contrato, según detalle:

ENTREGABLES	PLAZO (Contados a partir del día siguiente de firmado el contrato)
Entregable N° 1. Fase 1: Planificación del Proyecto y Cronograma de actividades	5 días calendario
Entregable N° 2. Fase 2: Diagnóstico y revisión del SGSI.	30 días calendario
Entregable N° 3. Fase 3: Elaboración y/o actualización de documentos del SGSI	60 días calendario
Entregable N° 4. Fase 4: Gestión de Riesgos	120 días calendario
Entregable N° 5. Fase 5: Operación del SGSI	180 días calendario

Entregable N° 6. Fase 6: Auditoría Interna e Informe del Cierre de Servicio	240 días calendario

6.4 Lugar de prestación de 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.

6.5 Adelantos

No corresponde

6.6 Penalidades

6.6.1 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 Reglamento.

6.6.2 Otras penalidades

Adicionalmente a la penalidad por mora, se aplican las siguientes penalidades:

N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
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 la entrega del Entregable N°1: Fase 1: Planificación del Proyecto y Cronograma de actividades	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.

La entidad contratante considera las particularidades de las otras penalidades y señala el plazo y forma en que se notifica al contratista el supuesto incurrido para que remita sus descargos, de corresponder. En dicho caso, también se debe precisar el plazo en que la entidad contratante evalúa dicho descargo y emite una decisión.

6.7 Subcontratación

Se encuentra prohibida la subcontratación de las prestaciones objeto del contrato.

6.8 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:

Nº	INSTITUCIONES ARBITRALES	RUC
1	Cámara de Comercio de Lima	20101266819
2	Pontificia Universidad Católica del Perú	20155945860
3	Universidad de San Martin de Porres	20138149022

6.9 Plazo para respuestas entre las partes

Para los plazos de respuesta de las partes sobre aspectos vinculados con la ejecución contractual que no han sido específicamente previstos en el Reglamento, aplica el plazo máximo de respuesta del siguiente cuadro:

Plazo máximo de respuesta:	Siete (07) días calendario

Antes del vencimiento de este plazo máximo, las partes pueden acordar su prórroga para cada situación específica considerando la cláusula de notificaciones del contrato.

7. TÉRMINOS DE REFERENCIA

7.1. CARACTERÍSTICAS DEL SERVICIO A REALIZAR

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 con 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.

En el año 2026 se llevará a cabo el servicio de auditoría del Sistema de Gestión de Seguridad de la información, el mismo que, como producto de la preauditoria, contará con aspectos a subsanar a nivel documental.

7.2. ALCANCE Y DESCRIPCION DEL SERVICIO

El Congreso de la República requiere asegurar la planificación, operación, mantenimiento y mejora continua de su SGSI basado en la norma NTP ISO/IEC

27001:2022. Para ello se deberán ejecutar los siguientes procesos mínimos durante la prestación del servicio.

7.2.1. Fase 1: Planificación del Proyecto

Llevar a cabo la planificación del proyecto, el mismo que deberá encontrarse alineado a la NTP-ISO/IEC 2022 y a cada actividad de cada fase, para lo cual se detallará mediante un cronograma.

7.2.2. Fase 2: Diagnóstico y revisión del SGSI

a) Llevar a cabo una evaluación preliminar, conjuntamente con un análisis de brechas, respecto a los cambios que demanda la NTP-ISO/IEC 27001:2022 frente a su predecesora NTP-ISO/IEC 27001:2014, a efectos de poder identificar las desviaciones en materia de seguridad de la Información, ciberseguridad y protección de la privacidad respecto a los 93 controles reflejados en la nueva normativa y sus cláusulas. En tal sentido, se deberá determinar y proponer la actualización y mejoras que deban realizarse sobre todo el acervo documental del SGSI.

b) Realizar un diagnóstico de la metodología de gestión de riesgos y oportunidades, a efectos de alinearla a la 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” mediante enfoque en activos y eventos, así como la metodología de medición, análisis y evaluación de indicadores.

c) Realizar un diagnóstico del procedimiento de gestión de incidentes de seguridad digital y/o seguridad de la información, con el objetivo de identificar las desviaciones que tenga frente a la ISO/IEC 27035:2023.

d) Añadir al plan de trabajo la ejecución de actividades que se demande, como producto de la evaluación y el análisis de brechas realizado que lleven a la entidad a un estado deseado, para lo cual, además, se debe considerar los documentos de gestión, políticas, manuales, procedimientos, metodologías, formularios, instructivos y/o formatos del SGSI.

e) Elaborar y presentar un informe con un resumen ejecutivo de gestión, el mismo que se expondrá mediante un Dashboard propuesto por el proveedor del servicio. Esta herramienta servirá para la evaluación del comportamiento y evolución del SGSI durante el plazo del servicio. Adicionalmente el informe deberá contener un resumen ejecutivo de las actividades que se llevarán a cabo como producto del diagnóstico ejecutado, el cual se expondrá ante la Jefatura del Departamento de Tecnologías de la Información, el Oficial de Seguridad y Confianza Digital y el Coordinador/Gestor de Incidentes previo a su aprobación.

7.2.3. Fase 3: Elaboración y/o actualización de documentos del SGSI

a) Elaborar y/o actualizar, según corresponda, la documentación del SGSI identificada en la fase 2, en base a los documentos de gestión, políticas, manuales, procedimientos, metodologías, formularios, instructivos y/o formatos del SGSI identificados.

b) Elaborar la documentación necesaria para la implementación de la gestión de proveedores en seguridad de la información, en el marco de la ISO/IEC 27036-1:2021, ISOIEC 27036-2:2022 y ISO/IEC 27036-3:2023.

c) Elaborar los escenarios de respuesta para el procedimiento de gestión de incidentes de seguridad digital y/o seguridad de la información, para lo cual se debe considerar, como mínimo, los incidentes asociados a:
   - Denegación de servicio (DoS) y denegación de servicio distribuido (DDos)
   - Phishing
   - Ransomware
   - Malware
   - Violación de datos personales
   - Ataques desde dentro
   - Amenaza persistente avanzada (APT)

d) Como resultado de la ejecución de esta actividad, el proveedor elaborará y presentará el entregable solicitado, considerando el informe que contiene un resumen ejecutivo, el mismo que se expondrá ante la Jefatura del Departamento de Tecnologías de la Información, el Oficial de Seguridad y Confianza Digital y el Coordinador/Gestor de Incidentes previo a su aprobación.

7.2.4. Fase 4: Gestión de Riesgos

a) Realizar las evaluaciones de riesgos y oportunidades al proceso que se encuentra dentro del alcance del SGSI y los activos de información que formen parte de este, haciendo énfasis en los riesgos de seguridad de la información, ciberseguridad y protección de la privacidad que detalla la normativa NTP-ISO/IEC 27001:2022, NTP-ISO/IEC 27002:2022 y NTP-ISO/IEC 27005:2022.
b) Ejecutar la identificación, análisis y evaluación de riesgos para proceder con la actualización de las matrices de gestión de riesgos de seguridad de la información.
c) Presentar, evaluar y gestionar la aprobación del Plan de Tratamiento de Riesgos (PTR) con cada área involucrada al proceso del alcance. Asimismo, generar evidencias en Actas de revisión y aprobación del Plan de Tratamiento de Riesgos, firmado por el responsable del Área/Equipo.
d) Elaborar el plan de implementación, con sus respectivos procedimientos de trabajo, para el Plan de Tratamiento de Riesgos (PTR).
e) Documentar los resultados de la gestión de riesgos, incluyendo la declaración de aplicabilidad (SOA) actualizada.
f) Elaborar material de capacitación al personal responsable de ejecutar las actividades requeridas para la ejecución del plan de tratamiento de riesgos e incluir material que deberá ser entregado a la entidad.
g) Como resultado de la ejecución de esta actividad, el proveedor elaborará y presentará el entregable solicitado, considerando el informe que contiene un resumen ejecutivo, el mismo que se expondrá ante la Jefatura del Departamento de Tecnologías de la Información, el Oficial de Seguridad y Confianza Digital y el Coordinador/Gestor de Incidentes previo a su aprobación.

7.2.5. Fase 5: Operación del SGSI

a) Ejecutar el plan de implementación del Plan de Tratamiento de Riesgos, así como la ejecución del plan de trabajo, respecto al resultado del análisis de brechas del SGSI, respecto a la NTP-ISO/IEC 27001:2022. Asimismo,

monitorear y realizar el seguimiento al plan de tratamiento de riesgos y a la capacitación del personal asignado.

b) Asistir en la gestión de incidentes de seguridad digital y/o seguridad de la información que se presenten durante la ejecución del servicio, a efectos de determinar las acciones a llevar a cabo para su remediación, designándose un responsable por parte del proveedor para tal fin.

c) Revisar y evaluar que los controles declarados en el SOA (NTP ISO/IEC 27002:2022) se estén ejecutando, realizando técnicas de auditoría, revisión de muestras, entre otros.

d) Hacer seguimiento a las acciones correctivas y de mejora continua a raíz de la ejecución de auditorías internas pasadas.

e) Realizar 10 inspecciones (una por sede en Lima Metropolitana), de manera presencial, a nivel de arquitectura tecnológica, seguridad de la información, ciberseguridad y protección de la privacidad, con el objetivo de validar el cumplimiento de buenas prácticas.

f) Realizar charlas de sensibilización y concientización del SGSI, así como capacitación oficial:

- Dictado de una (01) charla de sensibilización y concientización de seguridad de la información, ciberseguridad y privacidad de datos para no menos de 200 trabajadores de manera presencial.
- Capacitación y examen de certificación en ISO/IEC 27701 Lead Implementer para tres personas por PECB, IRCA o cualquier organización internacional que se encuentre acreditada por no menos de tres organismos de certificación personal en la norma ISO/IEC 17024.

f) Como resultado de la ejecución de esta actividad, el proveedor elaborará y presentará el entregable solicitado, considerando el informe que contiene un resumen ejecutivo, el mismo que se expondrá ante la Jefatura del Departamento de Tecnologías de la Información, el Oficial de Seguridad y Confianza Digital y el Coordinador/Gestor de Incidentes previo a su aprobación

7.2.6. Fase 6: Auditoría interna del SGSI y cierre

g) Preparar y realizar una auditoría interna al SGSI, a cargo del Auditor Líder ISO 27001, teniendo como objetivos principales:

- Verificar el estado de la implementación del Sistema de Gestión de Seguridad de la Información del Congreso de la República, respecto a la NTP ISO/IEC 27001:2022, de manera que se identifiquen, analicen y confirmen aquellos aspectos y requisitos que aún no se han cubierto o contemplado de manera satisfactoria.
- Evaluar el grado de implantación y cumplimiento de las políticas, normas y procedimientos que se hayan establecido en relación a la seguridad de la información, ciberseguridad y privacidad de datos.
- Determinar la eficacia de los controles y las medidas de seguridad implementados para la protección de los activos y recursos de información (datos, tecnologías, instalaciones, personal y aplicaciones).

h) Elaborar un plan de trabajo para la solución de las no conformidades y observaciones que puedan surgir de:

- Auditorías del SGSI.
- Incidentes de seguridad de información.
- Medición y evaluación de la efectividad del SGSI y sus controles.
- Revisiones a cargo de la Alta Dirección.

- Retroalimentación de las partes interesadas.

i) Como resultado de la ejecución de esta actividad, el proveedor elaborará y presentará el entregable solicitado, considerando el informe que contiene un resumen ejecutivo, el mismo que se expondrá ante la Jefatura del Departamento de Tecnologías de la Información, el Oficial de Seguridad y Confianza Digital y el Coordinador/Gestor de Incidentes previo a su aprobación

7.3. 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:

- 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.

7.4. PRODUCTOS A OBTENER:

a) Entregables de la Fase 1: Planificación del Proyecto y Cronograma de actividades

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

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

b) Entregable de la Fase 2: Diagnóstico y revisión del SGSI.

A los treinta (30) días calendario contados partir del día siguiente de la firma del contrato, el proveedor hará entrega de:

- Informe de análisis de brecha, de acuerdo con lo indicado en el numeral 6.2.2 literal a), así como la documentación a actualizar del acervo documental del SGSI.
- Informe inherente al diagnóstico de la metodología de gestión de riesgos y oportunidades, de acuerdo a lo indicado en el numeral 6.2.2. literal b).
- Informe de diagnóstico del procedimiento de gestión de incidentes, de acuerdo a lo indicado en el numeral 6.2.2. literal c).
- Plan de trabajo, de acuerdo a las actividades a desarrollar, de acuerdo a lo señalado en el numeral 6.2.2. literal a), b), y c).
- Presentación de un resumen ejecutivo de gestión mediante dashboard y consolidar en un informe los puntos anteriores, de acuerdo a lo señalado en el numeral 6.2.2. literal e).

c) Entregable Fase 3: Elaboración y/o actualización de documentos del SGSI

A los sesenta (60) días calendario contados a partir del día siguiente de la suscripción del contrato, el proveedor hará entrega de:

- Documentación del SGSI, identificada en la fase 2, actualizada, según lo indicado en el numeral 6.2.3. literal f)
- Documentación necesaria para la implementación de la gestión de proveedores en seguridad de la información, de acuerdo a lo señalado en el numeral 6.2.3. literal g).
- Presentación de los escenarios de respuesta para la gestión de incidentes, de acuerdo a lo señalado en el numeral 6.2.3. literal h). Este material debe ser didáctico y preciso, para lo cual se prioriza el uso de diagramas de flujo y storyboard.
- Presentación de un resumen ejecutivo de gestión mediante dashboard y consolidar en un informe los puntos anteriores, de acuerdo a lo señalado en el numeral 6.2.3. literal i).

d) Entregable de la Fase 4: Gestión de Riesgos

A los ciento veinte (120) días calendario contados a partir del día siguiente de la suscripción del contrato, el proveedor deberá presentar:

- Documentación de acuerdo al proceso del alcance como producto de la Gestión de Riesgos y Oportunidades del SGSI, con un enfoque activos y eventos, de acuerdo detallado en el numeral 6.2.4. literal j), k) y l), la cual incluye, pero no se limita a:
  i. Matriz de inventario de activos
  ii. Informe de inventario de activos
  iii. Informe de enfoque en eventos (escenarios)
  iv. Matriz de evaluación de riesgos
  v. Plan de tratamiento de Riesgos
  vi. Plan de gestión de oportunidades
  vii. Informe de Gestión de riesgos y oportunidades

- Documentos actualizados de acuerdo con la gestión de riesgos y oportunidades realizada con la versión de la NTP-ISO/IEC 27001:2022 y NTP-ISO/IEC 27002:2022 de acuerdo con lo indicado en el numeral 6.2.4 literal m), la cual incluye, pero no se limita a:

  i. Manual del SGSI del Congreso de la República
  ii. Declaración de aplicabilidad (SOA) – 93 controles
  iii. Requisitos de seguridad de la información, ciberseguridad y privacidad de datos.

iv. Análisis del Contexto y Requerimiento de partes interesadas
v. Alcance del proceso
vi. Roles y Responsabilidades
vii. Objetivos de seguridad de la información, ciberseguridad y privacidad de datos
viii. Métricas de seguridad de la información, ciberseguridad y privacidad de datos.

- Plan de implementación para el Plan de Tratamiento de Riesgos, de acuerdo con lo señalado en el numeral 6.2.4. literal n).
- Documentación de material de capacitación, la misma que debe ser entregada a la entidad y tener relación a las mejores prácticas de seguridad de la información, ciberseguridad y privacidad de datos, de acuerdo al numeral 6.2.4. literal o).
- Presentación de un resumen ejecutivo de gestión mediante dashboard y consolidar en un informe los puntos anteriores, de acuerdo a lo señalado en el numeral 6.2.4. literal p).

e) Entregable Fase 5: Operación del SGSI

A los ciento ochenta (180) días calendario contados a partir del día siguiente de la suscripción del contrato, el proveedor hará entrega de:

- Informe del desarrollo de la implementación del Plan de Tratamiento de Riesgos y el Plan de Trabajo del análisis de brechas, de acuerdo a lo señalado en el numeral 6.2.5. literal q).
- Informe de seguimiento a incidentes de seguridad digital y/o seguridad de la información, en donde se debe brindar propuestas de soluciones, de acuerdo a lo señalado en el numeral 6.2.5. literal r).
- Informe de revisión de los controles declarados en el SOA, de acuerdo a lo señalado en el numeral 6.2.5. literal s).
- Informe de seguimiento a las acciones correctivas y de mejora continua, de acuerdo a lo señalado en el numeral 6.2.5. literal t).
- Informe de las inspecciones realizadas a nivel de arquitectura tecnológica, seguridad de la información, ciberseguridad y protección de la privacidad que incluya estadísticas, evidencias y recomendaciones, de acuerdo a lo señalado en el numeral 6.2.5. literal u).
- Lista de asistencia a la charla de sensibilización y concientización de seguridad de la información, ciberseguridad y privacidad de datos, asi como a la capacitación en ISO/IEC 27701 Lead Implementer, de acuerdo al numeral 6.2.5. literal v).
- Presentación de un resumen ejecutivo de gestión mediante dashboard y consolidar en un informe los puntos anteriores, de acuerdo a lo señalado en el numeral 6.2.5. literal w).

f) Entregable Fase 6: Auditoría Interna e Informe del Cierre de Servicio

A los doscientos cuarenta (240) días calendario contados a partir del día siguiente de la suscripción del contrato, el proveedor deberá presentar el Informe de Cierre de Servicio, el cual debe contener las actividades de cierre, evaluando y verificando el cumplimiento general de la planificación, considerando como mínimo lo siguiente:

- Presentación de los siguientes documentos, de acuerdo a lo señalado en el numeral 6.2.6. literal x), la cual incluye, pero no se limita a:
  Plan Anual de Auditoría Interna del SGSI
  Informe de Auditoría Interna del SGSI

- Presentación de los siguientes documentos, de acuerdo a lo señalado en el numeral 6.2.6. literal y), en donde se incluya un informe de solución de no conformidades y observaciones, con su respectivo plan de trabajo.
- Presentación de un resumen ejecutivo de gestión mediante dashboard y consolidar en un informe los puntos anteriores, de acuerdo a lo señalado en el numeral 6.2.6. literal z). que incluya las conclusiones y recomendaciones del Servicio.

Todos los entregables serán proporcionados en medio impreso y anillado (1 original y 1 copia en sobre cerrado), incluyendo archivos encriptados en los formatos digitales (PDF y archivos editables, word, Excel, entre otros) con capacidad de búsqueda (con idéntico contenido que el original impreso) en medio magnético (USB) que adicionalmente contendrá los documentos en formato fuente original y editable (Word, Excel, PowerPoint, Project, Visio, entre otros). Todas las reuniones deberán contener un Acta que evidencie la asistencia y acuerdos.

6. 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 máximo de siete días, de acuerdo con lo establecido en el numeral 144.3 del artículo 144° del Reglamento de la Ley N° 32069, Ley General de Contrataciones del Públicas.

7. FORMA DE PAGO

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.
La entidad contratante paga las contraprestaciones pactadas a favor del contratista dentro de los diez días hábiles siguientes de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles.

ENTREGABLES	PORCENTAJE (Monto propuesta)
Entregable N° 2. Fase 2: Diagnóstico y revisión del SGSI.	10 %
Entregable N° 3. Fase 3: Elaboración y/o actualización de documentos del SGSI	20 %
Entregable N° 4. Fase 4: Gestión de Riesgos	30 %
Entregable N° 5. Fase 5: Operación del SGSI	20 %
Entregable N° 6. Fase 6: Auditoría Interna e Informe del Cierre de Servicio	20%

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 efectuada suscrita por el servidor responsable del Oficial de Seguridad y Confianza Digital y refrendada por el/la jefe/a del Departamento de Tecnologías de la Información.
- Comprobante de pago.
- Productos descritos en el numeral 7.4

Salvo los documentos que emite la entidad contratante, es decir, de recepción y verificación, así como de conformidad, debe presentar la documentación restante en mesa de partes del Congreso de la República de manera física o virtual (https://wb2server.congreso.gob.pe/mpv/#/).

8. REQUISITOS MINIMOS DEL PROVEEDOR

Registro Único de Contribuyentes (RUC) activo y habido
Registro Nacional de Proveedores (RNP) vigente
No encontrarse impedido ni inhabilitado para contratar con el Estado.

9. 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.
A continuación, se detallan los certificados vigentes que se deberán presentar por cada uno de los miembros del **personal clave**:

a) Un (01) Líder del Proyecto
- Certificado en gestión de proyectos PMP o Certificación ISO 21500 o Certificación ISO 21502.
- Contar con al menos dos (2) de las siguientes certificaciones vigentes:
  - ISO/IEC 27001 Lead Implementer
  - Certified Information Security Manager (CISM).
  - ISO/IEC 27001 Lead Auditor
  - Certified Information Systems Auditor (CISA)
  - Certified Information System Security Professional (CISSP)
  - ISO/IEC 31000 o ISO 27005 Risk Manager

b) Un (01) Consultor Senior en Seguridad de la Información
- Contar con al menos dos (2) de las siguientes certificaciones vigentes:
  - ISO/IEC 27001 Lead Implementer
  - ISO/IEC 27001 Lead Auditor
  - ISO/IEC 31000 o ISO 27005 Risk Manager
  - ISO 22301 Lead Implementer
  - Certified Information Security Manager (CISM)
  - Certified Information Systems Auditor (CISA)

c) Un (01) Especialista en Ciberseguridad
- Contar con al menos tres (3) de las siguientes certificaciones vigentes:
  - Certified Information Security Manager (CISM).
  - Certified Information Systems Auditor (CISA)
  - Certified Information System Security Professional (CISSP)
  - Certified Ethical Hacker (CEH)
  - Certified Penetration Testing Engineer (CPTE)
  - Certified Professional Ethical Hakcer (CPEH)
  - eLearnSecurity Junior Penetration Tester (eJPT)
  - ISO/IEC 27032 Lead Cybersecurity Manager
  - Certified Secure Web Application Engineer (CSWAE)
  - Certified Ethical Hacker Practical (CEH PRACTICAL)

d) Un (01) Auditor ISO 27001
- Contar con la certificación vigente como Lead Auditor ISO 27001 (IRCA o PECB)

Los certificados vigentes, es decir, los que se encuentran dentro de su periodo de validez y con cumplimiento de los requisitos de mantenimiento establecidos por la entidad certificadora, deberán ser presentados para el perfeccionamiento del contrato.

10. OTRAS CONSIDERACIONES ADICIONALES

15.1. CUMPLIMIENTO DEL PROTOCOLO SANITARIO DEL CONGRESO

En aspectos relacionados a la seguridad e higiene ocupacional, para los trabajos dentro de las instalaciones de la Entidad, el Contratista deberá cumplir con los lineamientos establecidos en el "Plan para la Vigilancia, Prevención y Control de COVID – 19 en el Congreso de la República- 7.5.3 Medidas para el público visitante" el cual será entregado al Contratista luego de suscrito el contrato.

El personal propuesto por el Contratista para la ejecución del servicio deberá contar en forma permanente con la indumentaria y equipos de protección personal (EPP) relacionados con las actividades a desarrollar y deberán portar en forma obligatoria un carné de identificación visible. Así como también deberá contar con el Seguro Complementario de Trabajo de Riesgo (SCTR) vigente, durante la prestación del servicio.

15.2. COLEGIATURA

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

16. VICIOS OCULTOS

La recepción conforme de la prestación por parte del Congreso de la República 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 el artículo 144 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de un (01) año contado a partir de la conformidad otorgada por LA ENTIDAD CONTRATANTE.

17. 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.

18. CLAUSULA ANTICORRUPCIÓN

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

11. REQUISITOS DE CALIFICACIÓN

11.1 Requisitos de calificación obligatorios

A. Experiencia del postor en la especialidad

Requisitos:
El postor debe acreditar un monto facturado acumulado equivalente a S/. 190,000.00 (Ciento noventa mil con 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.

En el caso de postores que declaren en el Anexo tener la condición de micro y pequeña empresa, se acredita una experiencia de S/. 20,000.00 (Veinte mil con 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. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.

Se consideran servicios de consultoría similares a los siguientes: Se consideran servicios similares a los siguientes: Servicios de Consultoría para la Implementación de Norma Técnica Peruana NTP ISO/IEC 27001 y/o Servicios de consultoría para la implementación de Sistemas de Gestión de Seguridad de la Información (SGS]) y/o Servicio mantenimiento y mejora continua del sistema de seguridad de la información (SGSI) y/o Servicio de Consultoría para la Adecuación al Nuevo Reglamento de la Gestión de la Seguridad de la Información y la Ciberseguridad y/o Servicio de Consultoría ISO/IEC 27001 y/o Servicios de Consultoría para mejoras de Procesos de Seguridad de la Información

Acreditación:
La experiencia del postor en la especialidad se acredita 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 o cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[4] o comprobante de retención electrónico emitido por SUNAT por la retención del IGV[5], correspondientes a un máximo de veinte contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados[6], 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 servicios 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

[4] El solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación fehaciente de su cancelación. Es válido el sello colocado por el cliente del postor (sea utilizando el término “cancelado” o “pagado”).

[5] De acuerdo con el Régimen de Retenciones del Impuesto General a las Ventas (IGV).

[6] Se entiende “privados” como aquellos que no son entidades contratantes.

contrario, se asume 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 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.

8.2 Requisitos de calificación adicionales

A Capacidad técnica y profesional

A.1 Experiencia del personal clave

Requisitos:

a) Un (01) Líder del Proyecto

Contar con experiencia no menor a seis (06) años gestionando proyectos de consultoría de implementación de Sistemas de Gestión de Seguridad de Información (SGSI) bajo al estándar ISO/IEC 27001.

b) Un (01) Consultor Senior en Seguridad de la Información

Contar con experiencia no menor a tres (03) años en proyectos de consultoría de implementación de Sistemas de Gestión de Seguridad de Información (SGSI) bajo al estándar ISO/IEC 27001.

c) Un (01) Especialista en Ciberseguridad

Contar con experiencia no menor a tres (02) años en servicios de consultoría en Ciberseguridad y/o Ethical Hacking y/o Análisis de Vulnerabilidades y/o implementación de controles de ciberseguridad.

d) <u>Un (01) Auditor ISO 27001</u>
Contar con experiencia no menor a tres (03) años en proyectos de consultoría de implementación y/o Auditoría de Sistemas de Gestión de Seguridad de Información (SGSI) bajo al estándar ISO/IEC 27001.

<u>Acreditación</u>:
El postor debe señalar la denominación del puesto, cargo y/o posición, y tiempo de experiencia del personal clave propuesto (años, meses y días) en el **Anexo correspondiente**, adjuntando en su oferta copia simple de cualquiera de los siguientes documentos: (i) contratos y su respectiva conformidad; (ii) constancias; (iii) certificados; o (iv) cualquier otra documentación que, de manera fehaciente, demuestre la experiencia del personal propuesto. Estos documentos deben señalar los nombres y apellidos del personal clave; el cargo desempeñado 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 está en meses sin especificar los días se debe considerar el mes completo. Se considera aquella experiencia que no tenga una antigüedad mayor a veinticinco años anteriores a la fecha de la presentación de ofertas. El inicio de plazo de la experiencia requerida debe ser desde **<u>Bachiller o desde la colegiatura, de ser el caso</u>**. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considera una vez el periodo traslapado. En ningún caso corresponde exigir que el mismo personal clave acredite experiencia en más de un cargo.

B.2 Calificaciones del personal clave

B.2.1. Formación académica

<u>Requisitos:</u>

a) <u>Un (01) Líder del Proyecto</u>
Título Profesional en cualquiera de las siguientes formaciones académicas: Ingeniería en Sistemas de Información o Ingeniería de Redes y/o Comunicaciones o Ingeniería de Computación y/o Sistemas o Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería Industrial o Ingeniería Informática o Ingeniería de Software o Licenciado en Computación o Administración.

b) <u>Un (01) Consultor Senior en Seguridad de la Información</u>
Título Profesional o con Grado de Bachiller en cualquiera de las siguientes formaciones académicas: Ingeniería en Sistemas de Información o Ingeniería de Redes y/o Comunicaciones o Ingeniería de Computación y/o Sistemas o Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería Industrial o Ingeniería Informática o Ingeniería de Software o Licenciado en Computación.

c) <u>Un (01) Especialista en Ciberseguridad</u>
Título Profesional o con Grado de Bachiller en cualquiera de las siguientes formaciones académicas: Ingeniería en Sistemas de Información o Ingeniería de

Redes y/o Comunicaciones o Ingeniería de Computación y/o Sistemas o Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería Industrial o Ingeniería Informática o Ingeniería de Software o Licenciado en Computación o Ingeniería Informática y/o de Sistemas.

d) Un (01) Auditor ISO 27001

Título Profesional o con Grado de Bachiller en cualquiera de las siguientes formaciones académicas: Ingeniería en Sistemas de Información o Ingeniería de Redes y/o Comunicaciones o Ingeniería de Computación y/o Sistemas, Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería Industrial o Ingeniería Informática o Ingeniería de Software o Licenciado en Computación.

Acreditación:

El postor debe señalar los nombres y apellidos, documento de identidad, el nombre de la universidad o institución educativa que expidió el grado de título profesional, y el grado o título profesional obtenido en el **Anexo correspondiente**, adjuntando en su oferta copia del grado de bachiller o título profesional. En caso se acredite estudios en el extranjero del personal clave, debe presentarse, adicionalmente, copia simple de la revalidación o reconocimiento del grado o título ante la SUNEDU.

Los evaluadores o la DEC, según corresponda, verifican los grados o títulos profesionales en el Registro Nacional de Grados Académicos y Títulos Profesionales 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 del Ministerio de Educación, a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/ según corresponda.