Requerimiento de contrataciones menores

Términos de Referencia

Órgano y/o Unidad Orgánica:	Departamento de Calidad y Fiscalización/SIG
Actividad del POI:	OEI 9. Fortalecer los sistemas de gestión (Gobernanza)
Denominación de la Contratación:	Contratación del servicio de consultoría para Auditorías de Diagnóstico y Preparación para la Certificación de Sistemas de Gestión en Seguridad de la Información basada en la norma ISO 27001:2022 en Electronoroeste S.A.
Número de CNM	**CN-0012-2023-ENOSA**

I. FINALIDAD PÚBLICA

Se, requiere certificar el Sistema de Gestión de la Seguridad de la Información basado en la Norma ISO 27001:2022 con el objetivo de resguardar la confidencialidad, integridad y disponibilidad de la Información en Electronoroeste S.A., a fin de mitigar el riesgo de exposición de información sensible a nuestros grupos de interés gestionadas al interior de nuestra empresa.

II. OBJETIVO DE LA CONTRATACIÓN

Contratar los servicios de consultoría especializado para Auditorías de Diagnóstico y Preparación para la Certificación de Sistemas de Gestión en Seguridad de la Información basada en la norma ISO 27001:2022 en Electronoroeste S.A., con el objetivo de garantizar que LA EMPRESA cumpla con los requisitos de la norma y esté preparada para obtener la certificación.

III. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

3.1 Descripción del servicio a contratar

Ítem	Cantidad	Descripción del servicio
1	01	Contratación del servicio de consultoría para Auditorías de Diagnóstico y Preparación para la Certificación de Sistemas de Gestión en Seguridad de la Información basada en la norma ISO 27001:2022 en Electronoroeste S.A.

El alcance del servicio comprende la revisión, actualización y adecuación del Sistema de Gestión de Seguridad de la Información (SGSI) según la Norma ISO 27001:2022 en los procesos de Electronoroeste S.A.

El alcance de este servicio está definido para: El Sistema de Gestión de Seguridad de Información de ELECTRONOROESTE S.A. que abarcará los procesos de Comercialización de Energía Eléctrica, Gestión de la Operación y Mantenimiento en Distribución, Generación, Transmisión y Generación Hidráulica de Energía Eléctrica, y Desarrollo y Gestión de Proyectos de Energía Eléctrica, así como sus procesos transversales o necesarios, según la Norma ISO 27001:2022.

Se adjunta el Mapa de Procesos en el Anexo 01.

El servicio debe ser consistente con lo expresado en la Norma ISO 27001:2022 y los Códigos de Buenas Prácticas para la Gestión de la Seguridad de la Información. Así mismo se debe considerar las etapas para los procedimientos y actividades de gestión de riesgos vinculados a la implementación del ISO 27001:2022 para la Seguridad de la Información.

El contratista deberá revisar, adecuar y actualizar la documentación, operación y mantenimiento del SGSI, basada en la Norma ISO 27001:2022 de acuerdo a la necesidad de Electronoroeste S. A. Así también, revisar y actualizar la Estructura del SGSI, conformado por las políticas, procedimientos y base documental asociada dentro del alcance definido por ELECTRONOROESTE S.A., así como con los registros necesarios para asegurar el cumplimiento de los objetivos específicos de Seguridad de la Información.

3.2 Actividades

Etapa 1 :

- ✓ Entendimiento de la organización y de los procesos del alcance, revisar documentación existente con el objetivo de elaborar el Plan de Auditoría de Diagnóstico, el mismo que deberá considerar los siguientes ítem:
  - Objetivos.
  - Alcance.
  - Descripción de actividades.
  - Cronograma de ejecución de actividades (Incluyendo actividades de capacitación).
  - Identificación de los auditados.
  - Cronograma de entrevistas.
  - Programa de auditoría con procedimientos a ejecutar.
- ✓ Ejecutar el programa de auditoría con la finalidad de realizar el Diagnóstico de brechas, lo que permitirá identificar la brecha existente, entre la realidad de LA EMPRESA en temas de seguridad de la información (estado actual) y lo recomendado en la ISO 27001:2022 SGSI (estado deseado) y determinar las mejoras posibles a las prácticas de seguridad, así como su inclusión en la implementación bajo contratación.
- ✓ Elaboración y presentación del Informe Final de Diagnóstico de Brechas que deberá considerar lo siguiente:
  - Antecedentes.
  - Objetivos.
  - Alcance.
  - Metodología y personal entrevistado.
  - Actividades desarrolladas.
  - Estado situacional del nivel de implementación del Sistema de Gestión Antisoborno, teniendo como base el nivel del cumplimiento de requisitos establecidos en la ISO 27001:2022
  - Conclusiones.
  - Recomendaciones.
  - Planes de acción, estableciendo los ajustes y adecuaciones necesarias, identificando los responsables para la implementación del cierre de brechas respecto al cumplimiento de los requisitos establecidos en la ISO 27001:2022.

- ✓ Elaboración del Plan de Trabajo para la Implementación y/o adecuación del Sistema de Gestión de la Seguridad de la Información de LA EMPRESA, que deberá contener lo siguiente:
    - Responsables.
    - Tareas a ejecutar.
    - Fechas de inicio y término.
    - Documentación a elaborar y/o actualizar (políticas, directivas, manuales, procedimientos, otros).
    - Necesidades de capacitación y sensibilización para la alta dirección y personal en general.
    - Riesgos asociados con la implementación del Sistema de Gestión de la Seguridad de la Información.

Etapa 2 :

- ✓ Identificar los activos que son necesarios proteger. Se define como activo a la información, entre otros: documentos físicos o digitales, software, equipos de tecnología e infraestructura asociada y recursos humanos. Asimismo, determinar la clasificación y valorización de activos de información
- ✓ Realizar la gestión de riesgos que permita (identificar, analizar y evaluar), los requisitos de seguridad en LA EMPRESA, definiendo las potenciales amenazas asociados a los procesos estratégicos definidos en el SIG y a la información administrada o custodiada por las Áreas Usuarias, su vulnerabilidad, la probabilidad de ocurrencia, su posible impacto y los controles que serán necesarios incorporar. Para ello se debe tener en cuenta lo siguientes parámetros para la gestión de riesgos:
    - Liderar la revisión, adecuación y actualización de la gestión de riesgos, activos de información hasta su aprobación por parte de los propietarios.
    - Actualizar las matrices de riesgos del SGSI
    - Revisar, adecuar y actualizar el plan de tratamiento de riegos y apoyar en su establecimiento.
    - Revisar, diseñar y documentar los controles de seguridad de la información establecidos en el plan de tratamiento de riesgos. Los controles pueden ser políticas, procedimientos, instructivos, manuales, y/o lo que corresponda
    - Desarrollar los talleres y entrenamiento necesarios, al personal designado de los procesos que forman parte del alcance para la revisión, actualización y mejoras para la identificación de activos y riesgos de seguridad de la información y ejecución de los controles implementados y/o a implementar.

Etapa 3 :

- ✓ Revisar, adecuar y documentar el Manual del SGSI
- ✓ Revisar, adecuar y actualizar la declaración de aplicabilidad (SoA) en base a la versión 27001:2022.
- ✓ Elaborar el Plan de Seguridad de la Información detallado, tomando en consideración tanto los riesgos y niveles de servicio, así como las brechas existentes en temas de seguridad. En base a este plan se definirán e implementarán los controles necesarios que aseguren la reducción de los riesgos identificados, según lo definido en el plan de tratamiento de riesgos.
- ✓ Elaborar las políticas, prácticas, estándares, procedimientos y toda información complementaria, que conformen las actividades a corto plazo del Plan de Seguridad de la Información, que conduzcan a la implementación del SGSI.

- ✓ Revisar, elaborar y/o actualizar los procedimientos y controles que correspondan en cumplimiento del Anexo A de la norma ISO 27001:2022.
- ✓ Definir los controles y políticas para la seguridad de la información en la gestión de continuidad de negocio, que incluyan:
    - Planificación de continuidad de seguridad de la información.
    - Implementación de continuidad de seguridad de la información.
    - Verificación, revisión y evaluación de continuidad de la seguridad de la información.
    - Definir Controles
- ✓ Ejecución de las Capacitaciones de Sensibilización y concientización en Sistema de Gestión Seguridad de la información para todo el personal de LA EMPRESA
- ✓ Implementar el Sistema de Gestión de Seguridad de la Información, asesorando y controlando la implementación en base al Plan de Seguridad de la Información siguiendo el modelo de mejora continua PDCA (Planificar, Hacer, Verificar, Actuar).

Etapa 4 :

- ✓ Ejecución de una Auditoria Interna a fin de dejar a LA EMPRESA en condiciones adecuadas para recibir la auditoría de certificación. Para la auditoría interna el Consultor estará acompañado a modo de entrenamiento del equipo de auditores internos y/u personal que designe LA EMPRESA y realizará las siguientes actividades:
    - Revision del cumplimiento de la información documentada versus los requerimientos del estandar ISO 27001:2022
    - Revisión del funcionamiento del sistema a través de los registros generados en base a muestreos aleatorios y/o pruebas Ad-Hoc.

  La auditoría Interna deberá ser ejecutada por profesional(es) distinto(s) al o los integrantes del equipo consultor que tuvo a cargo el diagnóstico y acompañamiento en la implementación.
- ✓ Elaborar un plan de acción que atiendan las no conformidades y acciones correctivas producto de la auditoria interna.
- ✓ Indentificar causa raiz de las no conformidades y observaciones
- ✓ Elaborar propuesta del informe para la revisión por parte de la Dirección
- ✓ Informe Final, Cierre del Proyecto. El Proveedor informará a LA EMPRESA acerca del resultado final del trabajo realizado, para ello, el equipo consultor presentará un Resumen Ejecutivo de las actividades realizadas y su resultado. Este deberá contener recomendaciones generales que, a criterio del consultor, LA EMPRESA debería considerar en este proceso de implementación

3.3 Seguros

El Consultar es responsable de la ejecución del servicio requerido por LA EMPRESA, quedando obligado a tomar todas las medidas de prevención y de seguridad necesarias para evitar los peligros y riesgos contra la integridad psicofísica, la salud y la vida de las personas; para lo cual debe considerar como prioridad básica que su personal deba contar con el Seguro Complementario de Trabajo de Riesgo (SCTR). Por lo tanto, deberá cumplir con la presentación del SCTR, antes de ingresar a las instalaciones de LA EMPRESA.

3.4 Normas técnicas

a. Norma ISO 27001:2022 Sistemas de Gestión de la Seguridad de la Información (SGSI).
b. Norma ISO 27001:2013 Sistemas de Gestión de la Seguridad de la Información (SGSI).

c. Norma NTP ISO/IEC 27001:2014 “EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos”
d. Norma ISO 9001:2015 Sistema de Gestión de la Calidad
e. Norma ISO/IEC 31001 Gestión del Riesgos.
f. D.S. 009-2005-TR Reglamento de Seguridad y Salud en el Trabajo.
g. R.M. 111-2013-MEM/DM Reglamento de Seguridad y Salud en el Trabajo con Electricidad.
h. Norma ISO 37001 Sistema de Gestión Antisoborno.
i. Norma ISO 22301:2019 Gestión de Continuidad de Negocio.
j. Decreto Legislativo N° 1412 - Aprueba la Ley de Gobierno Digital
k. Decreto Supremo N°118-2018-PCM: Declaran de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial
l. Decreto de Urgencia N° 006-2020 Sistema Nacional de Transformación Digital
m. Decreto de Urgencia N° 007-2020 Marco de Confianza Digital y medidas para su fortalecimiento.
n. DS 029-2021-PCM Reglamento Ley de Gobierno Digital.
o. Norma Técnica Peruana ISO/IEC 27001:2022
p. Norma Técnica Peruana ISO/IEC 27002:2022
q. Art. 1° de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD

3.5 Prestaciones accesorias a la prestación principal

3.5.1 Capacitación y/o entrenamiento

Los talleres, charlas y concientización deberán realizarse en la sede de la Entidad o mediante una plataforma virtual, previa coordinación con el consultor.

El Consultor deberá llevar el control de la asistencia de cada capacitación y presentarlos en el formato alcanzado por la empresa. Así también al finalizar cada taller, charla y/o concientización, deberá realizar mediciones de efectividad mediante cuestionarios de calificación y aplicar encuestas de satisfacción, conforme al formato presentado por la Empresa.

El Consultor deberá remitir, el Informe de capacitaciones (considerando fotografías y evidencia del taller, relación de asistencia en el formato presentado por la empresa, notas del examen, resultados de la encuesta de satisfacción) y entregar el certificado de asistencia y/o aprobación a cada participante.

Las charlas y/o talleres serán los siguientes:

TEMA	PÚBLICO OBJETIVO	N°
Charla de sensibilización y concientización del SGSI	Todo el Personal de Enosa	2
Taller de gestión de riegos riesgos y controles de Seguridad de la información	Dueños de Procesos	1
Taller de identificación de activos de seguridad de la información	Dueños de Procesos	1
Estructura del Anexo ISO 27002:2022	Dueños de Procesos	1
Simulacro de Auditoria SGSI	Dueños de Procesos	1

3.5.2 Recursos a ser provistos por el Consultor

Para el caso de la Auditoría Interna y en el caso en que la necesidad del servicio lo requiera y en coordinación con ambas partes, el Consultor debe estar presente en la sede principal regional Piura por lo cual deberá asumir todos los costos de traslado (pasajes aéreos o terrestres), viáticos, alimentación, hospedaje, traslados internos o movilidades y otros que se incurran para el cumplimiento del servicio.

3.6 Entregables

Se espera el cumplimiento, ejecución de las actividades para la Implementación del SGSI en base a la Norma ISO 27001:2022.

Entregable 1

- ✓ Plan de Auditoría de Diagnóstico.
- ✓ Informe Final Informe de Diagnóstico y de análisis de brechas que incluya un Plan detallado para cerrar las brechas entre la situación de LA EMPRESA y las recomendaciones de la Norma ISO y oportunidades de mejora.
- ✓ Plan de Trabajo para la Implementación y/o adecuación del Sistema de Gestión de la Seguridad de la Información de LA EMPRESA
- ✓ Informe detallado y sustentado del desarrollo de las actividades de lo solicitado en la etapa 1 del servicio.
- ✓ Actas visadas de reuniones correspondientes a este periodo.

Entregable 2

- ✓ Informe detallado de análisis de la gestión de riesgos que incluya:
  - Matriz de activos de información: Inventario de los activos de la información, su tasación y sus propietarios.
  - Identificación de riesgos asociados a los procesos y la Matriz de riesgos.
  - Informe de políticas y procedimientos faltantes, según análisis GAP,
  - Plan de tratamiento de riesgos.
  - Cuadro de mando para el SGSI.
  - Selección de controles y objetivos.
  - Los controles diseñados e implementados, así como la evidencia de ejecución de estos.
- ✓ Informe detallado y sustentado del desarrollo de las actividades de lo solicitado en la etapa 2 del servicio.
- ✓ Informe de Capacitación y Sensibilización para el personal (Cursos de Sensibilización y Capacitación en riesgos y sus controles asociados).
- ✓ Actas visadas de reuniones correspondientes a este periodo.

Entregable 3

- ✓ Plan de Seguridad de la Información
- ✓ Informe de Estructura del SGSI que incluya lo siguiente:
  - Manual del SGSI.
  - Políticas, procedimientos y controles de seguridad para la implementación del SGSI, dentro del alcance de aplicación de la Norma ISO 27001:2022

- Alcance del SGSI, política y objetivos de seguridad, declaración de aplicabilidad (SoA) y el procedimiento de control de documentos, el cual regula como se realizan y gestionan los documentos del SGSI.
- Políticas y Controles de la gestión de continuidad de negocios relacionados a la seguridad de la información.

✓ Informe de Capacitación y Sensibilización para el personal
✓ Informe detallado y sustentado del desarrollo de las actividades de lo solicitado en la etapa 3 del servicio.
✓ Actas visadas de reuniones correspondientes a este periodo.

Entregable 4

✓ Informe de auditoría Interna
✓ Informe para la revisión por parte de la dirección
✓ Informe final de cierre que incluya conclusiones y recomendaciones
✓ Informe detallado y sustentado del desarrollo de las actividades de los solicitado en la etapa 4 del servicio.
✓ Actas visadas de reunión correspondientes a este periodo.

Se ha previsto que la presentación de los cuatro (04) entregables, serán presentados en forma digital (formato Word, Excel, PDF, PowerPoint o Project, según sea el caso) en carpeta comprimida Zip o cualquier otra plataforma o software o aplicativo que permita la entrega no presencial al correo nolazabaly@distriluz.com.pe – Jefe de Calidad y fiscalización con copia al correo cmazaa@distriluz.com.pe – Analista SIG

En un plazo de 07 calendarios la Entidad emitirá la conformidad, de existir observaciones el contratista tendrá 05 días calendarios para subsanar.

3.7 Lugar y plazo de prestación del servicio

3.7.1 Lugar

El servicio de consultoría se realizará en forma remota o presencial a través de medios digitales, El consultor deberá contar con todos los medios de comunicación digital para la realización del presente servicio.
Para el caso de la consultoría en forma presencial, la ubicación de la prestación del servicio se desarrollará en la: Oficina principal: Calle Callao N°875-Piura.

3.7.2 Plazo

El periodo del servicio es por 120 días calendarios, contados a partir del día siguiente de firmado el contrato o recibida la orden del servicio, bajo la siguiente distribución:

DESCRIPCIÓN	PLAZO DE ENTREGA
Entregable 01	Treinta (30) días calendarios contabilizados a partir de recibida la orden del servicio
Entregable 02	Setenta (60) días calendarios contabilizados a partir de recibida la orden del servicio
Entregable 03	Noventa (90) días calendarios contabilizados a partir de recibida la orden del servicio
Entregable 04	Ciento veinte (120) días calendarios contabilizados a partir de recibida la orden del servicio

IV. REQUISITOS DEL PROVEEDOR/PERFIL DEL CONSULTOR

Deberá acreditar un monto de equivalente a S/ 50,000 (Cincuenta Mil y 00/100 Soles) por la contratación de servicios iguales o similares al objeto de la convocatoria durante 08 años anteriores a la fecha de la presentación de ofertas que se computaran desde la fecha de la conformidad o emisión del comprobante de pago según corresponda.

Acreditación: Deberá acreditarlo con contrato y su respectiva acta de conformidad o factura con su respectivo comprobante de pago.

Se considera servicios similares a los siguientes:

- ✓ Adecuación de la documentación para cumplimiento de la Norma del SGSI
- ✓ Servicio de Actualización y/o Migración de Base Documental del SGSI
- ✓ Servicio de capacitación o Talleres en la Norma SGSI
- ✓ Servicios de implementación de Sistemas de Gestión de la seguridad de la información SGSI bajo la norma ISO/IEC 27001:2013 o ISO/IEC 27001:2022.
- ✓ Servicio de operación y/o mantenimiento y/o mejora continua del SGSI
- ✓ Servicio de Implementación del Sistema de Gestión de la Continuidad del Negocio- ISO 22301:2019
- ✓ Servicio de Auditoría y/o diagnóstico y/o mantenimiento y/o acompañamiento y/o consultoría y/o asesoría y/o evaluación del Sistema de Gestión de la Seguridad de la Información bajo la norma ISO/IEC 27001:2013 o ISO/IEC 27001:2022.
- ✓ Auditoría y/o diagnóstico y/o mantenimiento y/o consultoría y/o asesoría y/o evaluación de la Norma ISO 27032:2012 – Ciberseguridad

4.1 Personal

4.1.1. Personal clave

El Proveedor deberá contar con el personal profesional necesario y calificado para prestar un eficiente servicio, quienes deberán contar con un seguro complementario de trabajo de riesgo (SCTR coberturas de salud y pensiones), las cuales deben permanecer vigentes durante la prestación del servicio; además de lo señalado el postor se obliga a presentar el siguiente personal:

4.1.1.1. <u>Consultor Líder (01):</u>

a. Actividades

Será el responsable de dar las directivas y lineamientos al equipo para que se desarrolle el servicio de manera estandarizada y coordinará directamente con el Área Responsable del Servicio y Administrador del servicio, los aspectos relacionados con el presente servicio.

b. Perfil

- ❖ **Formación Académica:**
  Profesional Titulado o Bachiller en Ingeniería, Administración, Contabilidad y/o Economía.

  Acreditación: 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

- **Capacitación:**
  Curso de Certificación ISO 27001 y/o Auditor Líder en ISO 27001 con un mínimo de 40 horas lectivas.

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

- **Experiencia:**
  Experiencia mínima de tres (03) años liderando o supervisando proyectos para la implementación de Sistemas de Gestión ISO.
  Haber realizado, por lo menos, dos (02) consultorías en la implementación y/o diagnóstico y/o mantenimiento y/o acompañamiento y/o asesoría y/o evaluación de Sistemas de Gestión Sistema de Gestión de la Seguridad de la Información – ISO/IEC 27001:2013 ISO/IEC 27001:2022 para empresas o entidades públicas o privadas.

  Acreditación: La experiencia del personal 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 clave propuesto.

4.1.1.2. <u>Consultor (01):</u>

a. Actividades

Será responsable de coordinar directamente con el Administrador del Servicio, los aspectos relacionados con el presente servicio, según el programa de trabajo.

b. Perfil

- **Formación Académica**:
  Profesional Titulado o Bachiller en Ingeniería, Administración, Contabilidad y/o Economía.

  Acreditación: 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

- **Capacitación:**
  Curso de Certificación en ISO 27001 con un mínimo de 24 horas lectivas.

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

- **<u>Experiencia:</u>**
  Haber realizado, por lo menos, dos (02) consultorías en la implementación y/o diagnóstico y/o mantenimiento y/o acompañamiento y/o asesoría y/o evaluación de Sistemas de Gestión Sistema de Gestión de la Seguridad de la Información – ISO/IEC 27001:2013 ISO/IEC 27001:2022 para empresas o entidades públicas o privadas.

  Acreditación: La experiencia del personal 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 clave propuesto.

4.1.1.3. Auditor Líder (01):

a. Actividades

Será responsable de dirigir y supervisar todo el proceso de auditoría Interna, asegurando que se cumplan las normas y procedimientos, y que la auditoría sea efectiva y eficiente

b. Perfil

- **Formación Académica**:
  Profesional Titulado o Bachiller en Ingeniería, Administración, Contabilidad y/o Economía.

  Acreditación: 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

- **Capacitación:**
  Curso de Certificación ISO 27001 emitida por una empresa certificadora con acreditación internacional con un mínimo de 40 horas lectivas.

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

- **Experiencia:**
  Haber realizado por lo menos, dos (02) auditorías de Sistemas de Gestión de la Seguridad de la Información bajo la norma ISO/IEC 27001:2013 o ISO/IEC 27001:2013 para empresas o entidades públicas o privadas.

  Acreditación: La experiencia del personal 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 clave propuesto.

V. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

6.1 Otras obligaciones

6.1.1 Otras obligaciones del contratista

El Consultor es el responsable directo y absoluto de las actividades que realizará, sea directamente o a través de su personal, debiendo responder por el servicio brindado.
EL Consultor deberá informar oportunamente a la empresa las situaciones de contingencia presentadas que impidan el normal desarrollo del servicio y que se encuentren fuera de su alcance del consultor.

6.1.2 Otras obligaciones de la Entidad

La empresa brindará las instalaciones, ambientes necesarios para el desarrollo de las reuniones. La empresa brindará la información requerida y necesaria al consultor para el buen desarrollo del servicio

6.2 Medidas de control durante la ejecución contractual

El Jefe Calidad y Fiscalización y TI, designará al Analista SIG para supervisar de forma virtual la ejecución de las actividades y para las coordinaciones para la entrega de la información.

El analista SIG, hará seguimiento al cronograma de trabajo, revisando que la documentación de los entregables sea la requerida y que sean entregados en los plazos establecidos.

Así también podrá solicitar reuniones inopinadas, por lo menos una vez duranta cada etapa del servicio para verificar el avance de la ejecución de las actividades.

Área que coordinará con el contratista: Departamento de Calidad y Fiscalización/SIG

Área responsable de las medidas de control: Departamento de Calidad y Fiscalización/SIG.

Área que brindará la conformidad: Departamento de Calidad y Fiscalización/SIG.

6.3 Conformidad de la prestación

La conformidad de la prestación se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley 32069, Ley General de Contrataciones Públicas. La conformidad es otorgada por el Jefe del Departamento de Calidad y Fiscalización/SIG. en el plazo máximo de siete (7) calendarios días computados desde el día siguiente de producida la recepción.

6.4 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.

La entidad contratante realiza el pago de la contraprestación pactada a favor del contratista según la presentación de cada entregable:

DESCRIPCIÓN	PORCENTAJE DE PAGO
Entregable 1	20%
Entregable 2	25%
Entregable 3	25%
Entregable 4	30%

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

- Comprobante de pago.
- Documento en el que conste la conformidad del entregable, suscrita por el responsable del Departamento de Calidad y Fiscalización/SIG.
- Entregable correspondiente
- El contratista deberá presentar la Factura o Recibo por Honorarios en la plataforma electrónica para ingreso control y seguimiento de comprobantes pago de

ELECTRONOROESTE S.A.: http://aplicaciones.distriluz.com.pe/Proveedor; considerando como Administrador del Contrato al Analista SIG.

6.5 Penalidad por mora:

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 Otras penalidades aplicables

Otras penalidades			
N°	**Supuestos de aplicación de penalidad**	**Forma de cálculo**	**Procedimiento de verificación**
1	El contratista cambie al personal propuesto sin contar con la autorización previa de la Entidad.	20% de la UIT (por caso detectado)	Constatación de asistencia y/o actas de reunión con personal de la empresa
2	Comunicación inoportuna de retiros y reemplazos de personal.	20% de la UIT (por caso detectado)	Constatación de asistencia y/o actas de reunión con personal de la empresa
3	Incumplimiento del Plan de trabajo aprobado	5% de la UIT (por caso detectado)	Actas de reuniones de avance
4	Falta de probidad u honestidad, agresión, maltrato físico o moral del personal contratista a LA EMPRESA.	50% de la UIT (por caso detectado, además del retiro del trabajador)	Actas y/o informes de verificación
5	Uso indebido de la información antes, durante y/o después de la ejecución de las actividades.	50% de la UIT (por caso detectado, además del retiro del trabajador)	Actas y/o informes de verificación

6.7 Responsabilidad por vicios ocultos

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

6.8 Modalidad de pago y sistema de entrega

a. Modalidad de pago

El contrato se rige por la modalidad de pago a base de porcentajes de conformidad con el artículo 130 del Reglamento.

6.9 Cláusula de Cumplimiento

Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

El postor adjudicatario de la buena pro, presentará como requisito para el perfeccionamiento del contrato, la “Declaración Jurada sobre prohibiciones e Incompatibilidades” a que se hace referencia en la Ley N° 31564 “Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público”.

6.10 Cláusula de confidencialidad

El contratista deberá mantener a perpetuidad la confidencialidad y reserva absoluta en el manejo de cualquier información y documentación a la que se tenga acceso a consecuencia de la contratación y la ejecución de la prestación, quedando prohibida revelarla a terceros.
Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades previas a la ejecución de la prestación, durante su ejecución y la producida una vez que se haya concluido la prestación.
Dicha información puede consistir en informes, recomendaciones, cálculos, documentos y demás datos compilados o recibidos por el contratista.
Asimismo, aun cuando sea de índole pública, la información vinculada al procedimiento de contratación, incluyendo su ejecución y conclusión, no podrá ser utilizada por el contratista para fines publicitarios o de difusión por cualquier medio sin obtener la autorización correspondiente de la entidad.
Los documentos técnicos, estudios, informes, grabaciones, películas, programas informáticos y todos los demás que formen parte de su Oferta y que se deriven de las prestaciones contratadas serán de exclusiva propiedad de la entidad.
En tal sentido, queda claramente establecido que el contratista no tiene ningún derecho sobre los referidos productos, ni puede venderlos, cederlos o utilizarlos para otros fines que no sean los que se deriven de la ejecución del presente.
La Contratista deberá dar cumplimiento a todas las políticas y estándares definidos por la entidad o el Grupo Distriluz, en materia de seguridad de la información. Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido el servicio. Asimismo, debe cumplir con la Política Corporativa sobre “SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES” - PC02.03-2.

6.11 Cláusula de verificación de cumplimiento de obligaciones

LA CONTRATISTA brindara las facilidades a LA ENTIDAD a fin de que esta última pueda efectuar auditorías y/o supervisiones específicas para la verificación del cumplimiento de obligaciones contraídas en el presente contrato, estando obligada LA CONTRATISTA a alcanzar la documentación e información que resulte necesaria para dicho propósito, conforme al requerimiento formulado por LA EMPRESA.
De detectarse algún incumplimiento, LA ENTIDAD aplicará la penalidad o actuará con arreglo a la normativa de contratación estatal que corresponda, conforme a las obligaciones asumidas y detalladas en los Términos de Referencia que forman parte integrante del presente contrato.

6.12 Cláusula – Protección de datos personales

EL CONTRATISTA autoriza a LA EMPRESA, para que realice el tratamiento de todos los datos personales que suministre o se generen como consecuencia de su relación contractual a favor de LA EMPRESA, de manera indefinida o hasta que revoque dicha autorización. Sus datos personales serán almacenados en la base de datos denominada “Relación de Proveedores” de titularidad de LA EMPRESA.

Estos datos personales consisten en nombre y apellido, número de documento de identidad, número de pasaporte, dirección de domicilio, teléfono, dirección de correo electrónico, imagen, firma, teléfono de referencia, carné de extranjería, libreta militar, estado civil, fecha de nacimiento, nacionalidad, sexo, profesión, edad, lugar de nacimiento, historial educativo, especialización, idioma, historial profesional, datos de derechohabientes, datos bancarios, información tributaria, seguros, planes de pensiones, jubilaciones, beneficios, código ESSALUD, CUSPP, información relativa a la salud física o mental, alergias, grupo sanguíneo, otro que pudiera ser considerado datos personales o sensibles que se pongan en conocimiento de LA EMPRESA durante el desarrollo de la relación contractual. El tratamiento podrá ser realizado directamente por LA EMPRESA o a través de un tercer agente designado por LA EMPRESA, exclusivamente para las finalidades que describimos en el siguiente párrafo. En cualquier caso, LA EMPRESA garantiza la seguridad y confidencialidad del tratamiento de sus datos personales.

La finalidad del tratamiento es una adecuada ejecución de la relación contractual de la que usted es parte y cumplir las obligaciones legales que nos corresponden. Entre dichas finalidades tenemos: i) gestión de recursos humanos; ii) administración de beneficios laborales y sociales para los colaboradores y sus derechohabientes; iii) evaluación de desempeño; iv) registros de ingresos y salidas; v) gestión de programas corporativos, vi) manejo de acciones correctivas; vii) procesamiento y gestión de atenciones y reclamos de seguros, entidades prestadoras de servicios de salud y sistemas de pensiones; viii) evaluaciones de ingreso, salida y controles periódicos de salud; ix) análisis de perfiles; y x) cualquier otra que sea necesaria para el cumplimiento de la relación contractual. Por tal razón, la autorización para el tratamiento de sus datos personales resulta obligatoria para la ejecución de dichas actividades, y en caso de negativa, ellas no se podrán realizar.

Por su parte, EL CONTRATISTA se compromete a: (i) utilizar los datos personales que pudiera recibir directa o indirectamente únicamente para los fines vinculados a la relación de prestación de servicios que mantiene a favor de LA EMPRESA; (ii) guardar confidencialidad en el tratamiento de los datos personales que maneje durante su función, inclusive con posterioridad a la culminación de su relación de prestación de servicios a favor de LA EMPRESA; y, (iii) devolver o destruir la información referida a datos personales que hubiera recibido en atención a su relación de servicios con LA EMPRESA, según se le disponga.

El CONTRATISTA se obliga a cumplir con estos compromisos y, en general, con las disposiciones de la Ley de Protección de Datos Personales, Ley N°29733 y su Reglamento, que le resulten aplicables en el marco de la relación de prestación de servicios que mantiene con LA EMPRESA. En caso de incumplimiento, LA EMPRESA podrá tomar las acciones disciplinarias correspondientes, sin perjuicio de iniciar las acciones legales necesarias para resarcir cualquier daño que pueda sufrir como consecuencia del incumplimiento.

6.13 Gobierno e integridad corporativa

EL CONTRATISTA declara que ha sido debidamente informado de los compromisos adoptados por ENOSA S.A., en el ámbito de la ética, la anticorrupción, el manejo de los conflictos de intereses, establecidos en el Código de Ética y Conducta, la Política

Anticorrupción, la Política de Prevención y Tratamiento del Conflicto de Intereses (Documentos se encuentran disponibles en la siguiente página Web de https://www.distriluz.com.pe/index.php/etica-y-cumplimiento).

Las Partes declaran y garantizan que cumplen y cumplirán con las normas del derecho internacional y las leyes aplicables y en especial con:

(i) Los derechos humanos fundamentales y en particular la prohibición del uso trabajo infantil y cualquier forma de trabajo forzoso u obligatorio; y, la organización de cualquier tipo de discriminación en la ejecución de sus actividades.

(ii) La normativa sobre prevención de delitos de lavado de activos y del financiamiento del terrorismo, delitos financieros, en particular la corrupción o cohecho, el fraude, y/o delitos similares o relacionados.

De igual forma, las Partes declaran que ni ellas, ni sus accionistas, socios o participacionistas o empresas vinculadas, ni cualquiera de sus respectivos directores, funcionarios, apoderados, empleados, ni ninguno de sus asesores, representantes o agentes, directa o indirectamente; han pagado, ofrecido, negociado, ni intentado pagar u ofrecer; ni intentarán pagar u ofrecer en el futuro ningún pago o comisión ilegal o cualquier beneficio o incentivo ilegal, para la celebración del presente contrato o durante la ejecución de este.

Asimismo, las Partes se obligan a conducirse durante la ejecución del Contrato, con honestidad, probidad, veracidad e integridad; y se obliga a no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus accionistas, integrantes de sus órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a sus empresas. Además, las Partes se comprometen a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

De igual forma, durante la vigencia del Contrato, Las Partes se obligan a adoptar medidas razonables para asegurarse de que sus agentes u otros terceros sujetos a su control o a su influencia determinante, también cumplan con las obligaciones señaladas en el párrafo precedente.

Las Partes declaran que sus recursos no provienen de actividad ilícita, por lo que no vulnera o contravine la normativa penal, ni utiliza tales recursos para desarrollar o financiar actividades ilícitas, lavado de activos, corrupción, terrorismo, entre otros.

Queda expresamente establecido que el Contrato quedará resuelto de pleno derecho en caso se verifique que alguna de las personas naturales o jurídicas mencionadas en los párrafos anteriores, hubiesen sido condenadas mediante sentencia consentida o ejecutoriada o hubiesen admitido y/o reconocido, la comisión de cualquiera de los delitos tipificados en la Sección IV del Capítulo II del Título XVIII del Código Penal (corrupción de funcionarios) o los previstos en la Ley N° 30424 - Ley que regula la responsabilidad administrativa de las personas jurídicas por el delito de cohecho activo transnacional.

EL CONTRATISTA manifiesta, con carácter de Declaración Jurada, lo siguiente:

a. Brindará la información que le sea requerida, en cumplimiento de las exigencias sobre el sistema de prevención de lavado de activos y financiamiento del terrorismo. Esta obligación, incluye también a la atención de los requerimientos de información que se le formulen, para la actualización de la información.

b. Que no tiene registros negativos en la lista Office of Foreign Assets Control - OFAC o en la Lista consolidada del Consejo de Seguridad de las Naciones Unidad – ONU.
c. Se compromete a cumplir y atender los requisitos establecidos en el modelo de cumplimiento de LA ENTIDAD; estando obligado a presentar la información y documentación institucional, comercial y/o financiera, en la oportunidad en que tal información y documentación le sea solicitada

Tener conocimiento que la información y documentación institucional, comercial y/o financiera que proporcione podrá ser entregada a los organismos o entidades competentes, para el cumplimiento de sus fines y atribuciones de investigación, supervisión, etc. (ejemplo, el Ministerio Público).

VI. RESOLUCIÓN DE CONTRATO POR INCUMPLIMIENTO

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

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES proceden de acuerdo a lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

VII. SOLUCIÓN DE CONTROVERSIAS:

Cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 82 de la Ley N° 32069, Ley General de Contrataciones Públicas.

VIII. GESTIÓN DE RIESGOS

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

IX. CLÁUSULA ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción del 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 contratación1 y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

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

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

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

X. GARANTÍAS

De conformidad con el artículo 139° del Reglamento de la Ley General de Contrataciones Públicas, NO se otorga garantía de fiel cumplimiento del contrato ni garantía de fiel cumplimiento por prestaciones accesorias en contratos de servicios cuyo monto es menor o igual a 50 UIT.

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

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

[4] Numeral 122.6 del artículo 122 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.

ANEXO 01

MAPA DE PROCESOS