TÉRMINOS DE REFERENCIA

Pedido de Servicio Nº 00020 - 2023

1. Denominación de la contratación

Servicio de implementación de la Norma Técnica Peruana ISO/IEC 27001.

2. Finalidad Pública

El presente servicio tiene por finalidad contratar los servicios para concluir con la implementación de un sistema de gestión de seguridad de la información, bajo el estándar de la Norma Técnica Peruana ISO/IEC 27001:2014 con el cual la Agencia Espacial del Perú – CONIDA alcanzará altos niveles de confidencialidad, integridad y disponibilidad de la información generada por el Activo Crítico Nacional "Sistema Satelital Peruano" y gestionar los riesgos asociados a sus actividades, para establecer un gobierno de seguridad de la información.

3. Actividad del POI

Gestión del programa - Mantenimiento de los Sistemas de Gestión.

4. Descripción y cantidad del servicio

- Concluir con la Implementación del Sistema de Gestión de Seguridad de la Información bajo la Norma Técnica Peruana ISO/IEC 27001:2014, integrado al Sistema de Gestión de la Calidad de la Agencia Espacial del Perú – CONIDA bajo la Norma ISO 9001:2015.
- La implementación del Sistema de Gestión de Seguridad de la información tendrá como alcance a los procesos "Suministro de imágenes", a cargo de la Dirección del Centro Nacional de Operaciones de Imágenes Satelitales – CNOIS y "Estudios Espaciales", a cargo de la Dirección de Estudios Espaciales.
- El presente servicio debe desarrollarse bajo una metodología de gestión de proyectos para realizar la última etapa de la implementación, correspondiente a la Evaluación del Sistema de Gestión de Seguridad de la Información, integrado al Sistema de Gestión de la Calidad de la Organización.

5. Actividades

Evaluación del Sistema de Gestión de Seguridad de la Información, integrado al Sistema de Gestión de la Calidad de la Organización.

El objetivo de esta etapa es verificar que el diseño e implementación del Sistema de Gestión de Seguridad de la Información esté de acuerdo a los requisitos de las Normas Técnica Peruana ISO/IEC 27001:2014.

A. Auditoría Interna.
   Este procedimiento será realizado por un equipo auditor conformado por un auditor Líder y un auditor interno que no hayan tenido ningún tipo de intervención en las etapas anteriores del proyecto de implementación del Sistema de Gestión de Seguridad de la Información, a fin de ser imparciales en los resultados, de acuerdo a un plan de auditoria que será presentado al Jefe de la Oficina de Gestión de la Calidad para su aceptación.
   En la presente auditoría, participarán como auditores en entrenamiento, los auditores internos de la CONIDA, designados por el Jefe de la Oficina de Gestión de la Calidad.
   Al finalizar la auditoría presentarán un informe que muestre el nivel de implementación y madures del Sistema de Gestión de Seguridad de la Información y las constancias que evidencien la participación de los auditores en entrenamiento.
B. Revisión por la Dirección
   Conducirán como moderadores la primera Revisión por la Dirección del Sistema de Gestión de Seguridad de la Información, cumpliendo con los requisitos de la NTP ISO/IEC 27001:2014 párrafo 9.3, donde se verificará la conveniencia, adecuación, se definirán las oportunidades de mejora y cualquier necesidad de cambio al Sistema de Gestión de Seguridad de la Información. Se confeccionará un acta con el resultado de la Revisión por la Dirección, de acuerdo al detalle antes descrito y el o los planes de acción que correspondiesen.
C. Auditoría Interna a la Alta Dirección, cumpliendo con los requisitos indicados en el párrafo A del presente documento.
D. Levantamiento de hallazgos de auditoría
   Se brindará el soporte para realizar el análisis a los hallazgos identificados en el informe de auditoría interna y definir el o los planes de acción correspondientes.

6. Plan de trabajo

El plan de trabajo será presentado máximo a los siete (07) días calendarios de recibida la orden de servicio y debe guardar relación con el plazo de ejecución del servicio.

7. Requisitos según leyes, reglamentos técnicos, normas metrológicas y/o sanitarias, reglamentos y demás normas

De acuerdo a la Norma Técnica Peruana ISO/IEC 27001:2014, requisitos para un Sistema de Gestión de Seguridad de la Información, Norma ISO 31000 lineamientos guía para administración y gestión de riesgos y Guía ISO 27002:2022 para los controles de seguridad de la información.

8. Impacto ambiental

No corresponde.

9. Seguros

No corresponde.

10. Prestaciones accesorias a la prestación principal

- Garantía del Servicio
  No aplica para la presente contratación.

- Mantenimiento preventivo
  No aplica para la presente contratación.

- Soporte Técnico
  No aplica para la presente contratación.

- Capacitación y/o entrenamiento
  No aplica para la presente contratación.

11. Lugar de prestación del servicio

El servicio se ejecutará en las instalaciones de la Agencia Espacial del Perú - CONIDA en sus sedes según corresponda la ubicación de los procesos a auditar.

- Sede de San Isidro (CONIDA), sito en Luis Felipe Villarán 1069-San Isidro-Lima.
- Sede de Pucusana (CNOIS), sito en el Km. 5.5 de la carretera de acceso a Pucusana – Lima.

12. Plazo de ejecución del servicio

El servicio tendrá un plazo máximo de ejecución de dos (02) meses y quince (15) días, contados a partir de la recepción de la orden de servicio.

13. Entregables

- Plan de trabajo para el desarrollo del presente servicio entregado máximo a los siete (07) días calendarios de recibida la orden de servicio.
- Plan de Auditoría Interna entregado máximo a los siete (07) días calendarios de recibida la orden de servicio.
- Informe de Auditoría Interna entregado máximo a los tres (03) días hábiles, contados a partir del día siguiente de terminada la auditoría interna.
- Acta de Revisión por la Dirección entregado máximo a los tres (03) días hábiles, contados a partir del día siguiente de terminada la Revisión por la Dirección.
- Informe de Auditoría Interna de la Alta Dirección entregado máximo a los dos (02) días hábiles, contados a partir del día siguiente de terminada la auditoría.
- Planes de acción de los hallazgos de la auditoría interna y de las acciones definidas en la Revisión por la Dirección entregado a más tardar a cinco (05) días hábiles de que concluya el servicio.

14. Requisitos del proveedor

Ser una empresa con experiencia mínima de cinco (05) años en, implementación de sistemas de gestión de seguridad de la información, en gestión de riesgos tecnológicos y operacionales, en auditoría y capacitación en los mencionados sistemas.

Se requerirá de dos equipos, uno implementador y otro auditor.

El equipo implementador, será el encargado de conducir el presente proyecto, y estará conformado por los siguientes profesionales:

A. Un (01) Director de Proyecto, con las siguientes características:

   a. Profesional titulado en Ingeniería Industrial, Sistemas o carreras afines.
   b. Con especialización en Gerencia de Proyectos y una experiencia comprobada mínimo tres (03) años.
   c. Con especialización en Sistemas de Gestión de Seguridad de la Información y Sistemas de Gestión de la Calidad.

B. Un (01) Especialista de proyecto, con las siguientes características:

   a. Profesional titulado en Ingeniería Industrial, Sistemas o carreras afines.
   b. Con especialización en Sistemas de Gestión de Seguridad de la Información y Sistemas de Gestión de la Calidad.
   c. Experiencia comprobada en trabajos de consultoría referentes al servicio solicitado, como mínimo tres (03) años de experiencia.

El equipo auditor, será el encargado de conducir las auditorías internas necesarias para confirmar la implementación del Sistema de Gestión de Seguridad de la Información, así como el tratamiento de los hallazgos de las indicadas auditorías, y estará conformado por los siguientes profesionales:

A. Un (01) Auditor líder, con las siguientes características:

   a. Curso de Auditor líder en la Norma ISO/IEC 27001 (actualización a la versión internacional 2013 o versión NTP 2014) e ISO 9001 (actualización a la versión 2015).
   b. Con experiencia en auditorías como Auditor Líder mínimo tres (03) años.

B. Un (01) Auditor interno, con las siguientes características:

   a. Curso de Auditor interno en la Norma ISO/IEC 27001 (actualización a la versión internacional 2013 o versión NTP 2014) e ISO 9001 (actualización a la versión 2015).

b. Con experiencia en auditorías como Auditor interno mínimo dos (02) años.

Se debe alcanzar Currículo Vitae documentado de cada una de las personas que conforman el equipo implementador y auditor.

Contar con el Registro Nacional de Proveedores. Capítulo de Servicios.

15. Recursos y facilidades a ser provistos por la entidad

- Personal integrante de los Procesos a ser auditados.
- Documentación pertinente a la implementación del Sistema de Gestión de Seguridad de la información.

16. Adelantos

No corresponde.

17. Confidencialidad

La compañía y sus empleados deben garantizar durante y después de concluido el servicio, la confidencialidad de la información entregada y revisada de la Agencia Espacial del Perú - CONIDA y de los hechos ocurridos durante el servicio, propios del mismo.

18. Propiedad intelectual

No corresponde.

19. Medidas de control durante la ejecución contractual

La oficina de Gestión de la Calidad realizará el seguimiento sobre el cumplimiento de los plazos y condiciones del contrato.

20. Conformidad de la prestación

La conformidad la otorgará el Jefe de la Oficina de Gestión de la Calidad.

21. Forma de pago

Al final del servicio contratado.

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

- Informe de conformidad brindada por la Oficina de Gestión de la Calidad.
- Comprobante de pago (Factura)
- Acta de conformidad.

22. Penalidades

22.1. Penalidad por mora

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto de la contratación, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso.

Cálculo de la penalidad diaria:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo de vigencia}}.$$

Monto: monto de la entrega no atendida.
Plazo de vigencia: en días, plazo ofertado.
F = 0.25, para plazos mayores a los 60 días calendario.

Cálculo de la penalidad a aplicar:
Penalidad a aplicar = Penalidad diaria x días de retraso

22.2. Consideraciones generales

- El monto máximo de la penalidad por mora no superará el diez por ciento (10%) del monto de la orden de servicio.
- Esta penalidad se deduce de los pagos a cuenta o del pago final.
- Superado el monto máximo de la penalidad, la Entidad puede resolver la contratación.

23. Responsabilidad por vicios ocultos

El plazo de responsabilidad por vicios ocultos es de un (01) año, contabilizados a partir de su recepción conforme.

24. ANEXOS

No se han generado.

Licenciado
ALFREDO ROBLES HIDALGO
Jefe de la Oficina de Gestión de la Calidad
AGENCIA ESPACIAL DEL PERÚ - CONIDA

AGENCIA ESPACIAL DEL PERU CONIDA
Firmado digitalmente por: ROBLES HIDALGO Alfredo Antonio FAU 20131371889 soft
Motivo: Soy el autor del documento
Fecha: 06/02/2023 10:56:10-0500