TÉRMINOS DE REFERENCIA

Unidad Orgánica:	Oficina de Infraestructura Tecnológica y Seguridad Informática
Meta Presupuestaria:	0228 - Desarrollo y Mantenimiento de los Sistemas Informativos
Actividad del POI:	AO100107200151 – Gestión de la Infraestructura Tecnológica y de Seguridad Informática.

1. DENOMINACION DE LA CONTRATACIÓN

Contratación del Servicio de Auditoria de Certificación en la Norma ISO/IEC 27001:2022 Sistema de Gestión de Seguridad de la Información.

2. OBJETIVO

Contratar a una persona jurídica especializada que brinde el servicio de auditoría de certificación del Sistema de Gestión de Seguridad de la Información (SGSI) del Ministerio de Transportes y Comunicaciones, conforme a los requisitos establecidos en la Norma ISO/IEC 27001:2022, con la finalidad de evaluar la conformidad y eficacia de los controles implementados dentro del alcance definido por la entidad, verificando el cumplimiento de los requisitos aplicables y permitiendo la obtención de la certificación correspondiente, sobre la base del grado de madurez y estado situacional del SGSI evidenciado mediante las evaluaciones y auditorías internas realizadas por la entidad.

3. FINALIDAD PUBLICA

Contribuir al fortalecimiento de la gestión de la seguridad de la información del Ministerio de Transportes y Comunicaciones, mediante la obtención de la certificación del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a los requisitos de la Norma ISO/IEC 27001:2022, para el alcance definido por la entidad. Esta certificación permitirá evidenciar la implementación y mantenimiento de controles y buenas prácticas orientadas a proteger la confidencialidad, integridad y disponibilidad de la información que soporta los servicios digitales, sistemas de información, plataformas tecnológicas e infraestructura tecnológica institucional, fortaleciendo la continuidad de las operaciones, la gestión de riesgos de seguridad de la información y la confianza de los ciudadanos, usuarios y demás partes interesadas en los servicios brindados por el Ministerio.

4. ALCANCE

CONCEPTO	CANTIDAD	UNIDAD DE MEDIDA
Contratación del Servicio de Auditoria de Certificación en la Norma ISO/IEC 27001:2022 Sistema de Gestión de Seguridad de la Información	01	Servicio

5. ANTECEDENTES

No aplica.

6. DESCRIPCIÓN DE LAS ACTIVIDADES A REALIZAR

6.1. Descripción, características y cantidades

El servicio deberá contemplar las siguientes actividades:

- La auditoría **debe iniciar el 22 de junio de 2026**.
- La auditoría está orientada según el alcance del Sistema de Gestión de

Seguridad de la Información del Ministerio de Transportes y Comunicaciones (ver ANEXO A), cuyos procesos son parte de la Oficina General de Tecnología de la Información y de la Dirección de Circulación Vial que cuentan con 36 y 24 colaboradores aproximada y respectivamente.

- El contratista enviará el Plan de Auditoría por correo electrónico por lo menos dos (02) días calendario antes de iniciar la auditoría, en el cual se especificará los horarios, las personas que deberán ser convocadas y los accesos requeridos; el correo electrónico deberá ser enviado al Director de la Oficina de Infraestructura Tecnológica y Seguridad Informática (En adelante OITSI) y al Oficial de Seguridad y Confianza Digital (En adelante OSCD), del Ministerio de Transportes y Comunicaciones.
- El contratista realizará la apertura de la auditoria, suscribiendo la respectiva acta en el formato provisto por el OSCD.
- El contratista realizará la auditoría en las fechas y horarios previamente acordados, tanto para la verificación de los requisitos del sistema documental, así como para la verificación de la implantación del Sistema de Gestión de Seguridad de la Información conforme a ISO/IEC 27001:2022.
- La auditoría deberá ejecutarse conforme a las etapas Auditoria de Fase 1 y Auditoria Fase 2 previstas por los organismos certificadores acreditados.
- El proveedor realizará el cierre de la auditoria, suscribiendo la respectiva acta en el formato provisto por el OSCD, informando a los auditados los resultados preliminares.
- El proveedor deberá enviar al correo electrónico del Director de la OITSI y al OSCD, el informe de la auditoria de certificación con los Hallazgos, preservando la confidencialidad, dicho informe deberá ser enviado en un plazo no mayor a dos (02) días calendario posteriores a la culminación de la auditoría.
- De identificarse hallazgos, el Ministerio de Transportes y Comunicaciones elaborará el "Plan de Acción" para atender las no conformidades; dicho plan deberá ser enviado al correo electrónico del auditor líder en un plazo no mayor a cuatro (04) días calendario posteriores a la recepción del informe de la auditoria.

En caso el Ministerio de Transportes y Comunicaciones presente un Plan de Acción, el contratista lo evaluará y emitirá la recomendación correspondiente para la decisión de certificación, de conformidad con los procedimientos de la entidad certificadora.

El servicio deberá mantener la confidencialidad de la información relacionada a los datos personales de los usuarios del servicio, limitando su uso a las necesidades propias del servicio brindado, salvo orden judicial o a solicitud del usuario, utilizando medios que garanticen el no repudio, confidencialidad e integridad de las transacciones realizadas para la firma.

NOTA: El proveedor adjudicado deberá visar los informes, actas, planes y demás documentos que genere como parte de la ejecución del servicio, en señal de conformidad y responsabilidad sobre su contenido.

6.1.1. Entregables

El Contratista debe realizar la entrega de la documentación en mesa de partes y en plazo indicado de acuerdo al siguiente detalle:

ENTREGABLE	DESCRIPCION DEL ENTREGABLE	PLAZO DE ENTREGA
ENTREGABLE N° 01	Informe de la Auditoría de Certificación ISO/IEC 27001:2022 que debe contener: - Plan de Auditoria. - "Acta de Reunión de Apertura" que deja constancia de la reunión de apertura de la auditoria. - "Acta de Reunión de Cierre" que deja constancia de la reunión de cierre de la auditoria informando los resultados. - "Informe detallado de la auditoria de certificación incluido los hallazgos y oportunidades de mejora encontrados".	**Hasta los veintiséis (26) días calendario,** contados a partir del día 22/06/2026 (inclusive ese día).
ENTREGABLE N° 02	Documento del resultado de la obtención del Certificado ISO/IEC 27001:2022 y debe contener: El Certificado ISO/IEC 27001:2022. (expedido en versión en español en formato físico y digital).	**Hasta los treinta (30) días calendario**, contados a partir del día 22/06/2026 (inclusive ese día).

Todo entregable deberá ser ingresado por Mesa de Partes de la Sede Central del Ministerio de Transportes y Comunicaciones, ubicada en el Jr. Zorritos N.º 1203, distrito del Cercado de Lima, provincia de Lima, departamento de Lima; y/o a través de la Mesa de Partes Virtual del MTC (https://mpv.mtc.gob.pe/).

6.1.2. Naturaleza y alcance del servicio

Queda establecido que el alcance del servicio requerido a través de los presentes términos de referencia, comprende aquellas actividades que apoyan, coadyuvan o fortalecen al cumplimiento regular de las funciones a cargo de la Oficina de Infraestructura Tecnológica y Seguridad Informática. Dichos servicios no reemplazan o sustituyen la responsabilidad funcional ni eximen del deber de cumplimiento de dichas funciones por parte de los funcionarios o servidores públicos de la Oficina de Infraestructura Tecnológica y Seguridad Informática.

En ese sentido, el (los) entregable(s) previsto(s) para la presente contratación, se sujetan y se circunscriben al alcance y naturaleza del servicio descrito en el párrafo precedente.

6.1.3. Consideraciones generales del servicio

El Ministerio de Transportes y Comunicaciones no se hace responsable de los eventos y/o accidentes y/o enfermedades que puedan presentarse durante el cumplimiento del contrato.

El Ministerio de Transportes y Comunicaciones no se responsabiliza de otorgar subsidios o indemnizaciones en caso ocurriese accidentes o caso fortuito en horario regular y fuera del mismo durante la ejecución del contrato.

7. PRESTACIONES ACCESORIAS

No aplica.

8. MEDIDAS DE SEGURIDAD EN LA PRESTACIÓN DEL SERVICIO

No aplica.

9. PLAZO Y LUGAR DE PRESTACION

9.1. PLAZO

El servicio se prestará conforme los plazos detallados a continuación:

9.1.1. Plazo 01

El servicio debe **iniciar el 22 de junio de 2026** y tiene una vigencia por el periodo de **treinta (30) días calendario** contados a partir del día 22/06/2026 (inclusive ese día).

9.1.2. Plazo 02

El plazo máximo para presentar el **Entregable N° 01** es de **veintiséis (26) días calendario** contados a partir del día 22/06/2026 (inclusive ese día).

9.1.3. Plazo 03

El plazo máximo para presentar el **Entregable N° 02** es de **treinta (30) días calendario** contados a partir del día 22/06/2026 (inclusive ese día).

9.2. Lugar

El servicio se brindará en la sede del Ministerio de Transportes y Comunicaciones, sito Jr. Zorritos N° 1203 – Cercado de Lima. El MTC podrá modificar el lugar de prestación de contrato, pudiendo realizar el contrato de manera presencial o no presencial, acorde a la necesidad del área usuaria.

10. REQUISITOS DEL CONTRATISTA Y PERSONAL

10.1. CONDICIONES GENERALES

- Persona jurídica con inscripción vigente en el Registro Nacional de Proveedor – RNP.
- Contar con Registro único del Contribuyente (RUC) habilitado.
- Contar con código de Cuenta Interbancario registrado (CCI).
- No estar impedido para contratar con el Estado.
- No estar inhabilitado para contratar con el Estado.
- La entidad certificadora deberá acreditar que cuenta con acreditación vigente para la certificación de Sistemas de Gestión de Seguridad de la Información ISO/IEC 27001, otorgada por un organismo de acreditación signatario del Acuerdo Multilateral de Reconocimiento (MLA) del International Accreditation Forum (IAF).

10.2. CONDICIONES PARTICULARES

10.2.1. Capacidad Legal

No aplica.

10.2.2. Personal clave

Auditor líder.

- Profesional universitario titulado nacional y/o internacional y colegiado con habilitación vigente en el respectivo colegio profesional.

Acreditación:
El personal clave será verificado por los evaluadores en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda.
El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.
En caso el profesional titulado no se encuentre inscrito en los referidos registros, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
En caso se acredite estudios en el extranjero del personal clave, debe presentarse adicionalmente copia simple del documento de la revalidación o del reconocimiento ante SUNEDU, del grado académico o título profesional otorgados en el extranjero, según corresponda.

- Deberá contar con capacitación en formación de Auditor Líder ISO 27001, con una duración mínima de cinco (05) días o cuarenta (40) horas lectivas o académicas.
  Acreditación:
  Se acreditará con copia simple de constancias, certificados, u otros documentos.

10.2.3. Experiencia del personal clave

Experiencia mínima de cinco (05) auditorías de certificación, recertificación y/o seguimiento de Sistemas de Gestión de Seguridad de la Información conforme a ISO/IEC 27001, en entidades públicas o privadas.

Acreditación:
La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.

10.2.4. Experiencia del postor en la especialidad

El postor debe acreditar un monto facturado acumulado equivalente a S/. 50,000.00 (Cincuenta Mil con 00/100 soles) por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los diez

(10) años anteriores a la fecha de la presentación de ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes:

- Servicios de implementación de Sistemas de Gestión de Seguridad de la Información.
- Auditoría en Sistemas de Gestión de Seguridad de la Información.
- Consultorías en Seguridad informática o Seguridad de la información.
- Gestión de Riesgos de TI o Continuidad de TI, cualquiera de ellos bajo el estándar de la ISO 27001.

Acreditación:
La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados, para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

10.2.5. Equipamiento estratégico
No aplica.

10.2.6. Infraestructura estratégica
No aplica.

11. RESPONSABILIDAD DEL POSTOR
Es preciso mencionar que el proveedor es el responsable directo y absoluto de las prestaciones que realizará, debiendo responder por la ejecución de la prestación del servicio.

12. RESPONSABILIDAD DEL ÁREA USUARIA
El área usuaria entregará y facilitará accesos al proveedor del servicio, de lo siguiente:

- Acceso a la información contenida en los sistemas, plataformas o aplicativos informáticos necesarios para la ejecución del contrato cuando corresponda, otorgando las instrucciones necesarias para su adecuada utilización y protección de datos que resulten aplicables.

13. FORMA Y CONDICIONES DE PAGO
El pago se realizará en una (01) armada, previa conformidad de la contratación emitida por la Oficina Infraestructura Tecnológica y Seguridad Informática de la

Oficina General de Tecnologías de la Información del MTC.

N° DE PAGOS	PORCENTAJE DE PAGOS
Pago único	100% del monto total de la orden de servicio, previa presentación del **entregable 01, entregable 02** y del otorgamiento de la conformidad de servicio correspondiente.

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

- Acta de conformidad
- Recibo por honorarios electrónico o comprobante de pago, según corresponda.
- Carta CCI

El pago se realiza en un plazo máximo de diez (10) días hábiles luego de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles más.

14. CONFORMIDAD

La Conformidad será emitida por la Oficina de Infraestructura Tecnológica y Seguridad Informática (OITSI) de la Oficina General de Tecnología de la Información (OGTI), quien verificará el cumplimiento de los presentes Términos de Referencia.

De existir observaciones, LA ENTIDAD CONTRATANTE las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar NO MAYOR AL 30% DEL PLAZO DEL ENTREGABLE CORRESPONDIENTE, DEPENDIENDO DE LA COMPLEJIDAD O SOFISTICACIÓN DE LAS SUBSANACIONES A REALIZAR. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, LA ENTIDAD CONTRATANTE puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar sin considerar los días en los que pudiera incurrir la entidad contratante para efectuar las revisiones y notificar las observaciones correspondientes.

Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD CONTRATANTE no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

15. CONFIDENCIALIDAD

El proveedor se obliga a mantener y guardar estricta reserva y absoluta confidencialidad todos los documentos e informaciones de la entidad a los que tenga acceso en ejecución del presente contrato. Se entiende que la obligación asumida por el consultor está referida no solo a los documentos e informaciones señalados como "confidenciales" sino a todos los documentos e informaciones que en razón del presente contrato o vinculado con la ejecución del mismo, pueda ser conocida por cualquier medio por el consultor.

16. PENALIDAD POR MORA

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las

prestaciones objeto del contrato, LA ENTIDAD CONTRATANTE le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo con la siguiente fórmula:

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

Donde:
F = 0.40

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de LA ENTIDAD CONTRATANTE no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme al numeral 120.4 del artículo 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

17. OTROS TIPOS DE PENALIDAD

No aplica.

18. RESOLUCION 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.
Cualquiera de las partes puede resolver, total o parcialmente, el contrato en los siguientes supuestos:

a) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
b) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
c) Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
d) Por incumplimiento de la cláusula anticorrupción.
e) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
f) Configuración de la condición de terminación anticipada establecida en el contrato, de acuerdo con los supuestos que se establezcan en el reglamento para su aplicación.

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.

19. ANTICORRUPCIÓN Y SOBORNO

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 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 numeral, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. 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. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

20. RESPONSABILIDAD POR VICIOS OCULTOS

El plazo de responsabilidad de vicios ocultos, materia de la presente contratación tendrá un plazo de un (01) año, contado a partir de emitida la conformidad.

21. PROPIEDAD INTELECTUAL

El Ministerio de Transportes y Comunicaciones tendrá todos los derechos de propiedad intelectual (sin limitación, patentes, derechos de autor, nombres comerciales y marcas registradas respecto a los productos u otros materiales relacionados a la contratación).

22. DECLARACION JURADA DE INTERESES

No aplica.

23. GESTION 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.

24. SOLUCION DE CONTROVERSIAS

Las controversias que surjan entre las partes sobre la validez, nulidad, interpretación, ejecución, terminación o eficacia de los contratos menores se resuelven mediante conciliación, conforme lo dispuesto en el numeral 81.3 del artículo 81 de la Ley.

25. GARANTIAS

No aplica.

26. APLICACIÓN SUPLETORIA

En todo lo no previsto en la presente contratación se aplicará de manera supletoria la Ley General de Contrataciones Públicas su Reglamento; demás normas generales y específicas que resulten aplicables y el Código Civil, siempre que no se contradiga con las disposiciones establecidas en los Términos de Referencia.

27. REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS

- Norma ISO/IEC 27001:2022– Sistema de Gestión Seguridad de la Información.
- Norma de Auditoría ISO 19011:2018 – Directrices para la auditoría de sistemas de gestión.

28. SANCIONES

La presente contratación se sujeta a lo establecido en el Título VI de la Ley General de Contrataciones Públicas Ley N° 32069 referido al régimen de infracciones y sanciones.

RAFAEL VICTOR PORTA DE LA CRUZ
DIRECTOR DE LA OFICINA DE INFRAESTRUCTURA TECNOLOGICA Y SEGURIDAD INFORMATICA

ANEXO A[1]

ALCANCE DEL SGSI

Considerando el análisis del contexto interno y externo de la organización, así como las necesidades y expectativas de las partes interesadas pertinentes, el Ministerio de Transportes y Comunicaciones establece el siguiente alcance del Sistema de Gestión de Seguridad de la Información (SGSI):

El SGSI aplica a la prestación de los servicios digitales asociados al Sistema Nacional de Conductores (SNC) y a la infraestructura tecnológica que los soporta, bajo responsabilidad del Ministerio de Transportes y Comunicaciones, a través de la Oficina General de Tecnología de la Información y las unidades organizacionales responsables de su operación.

El alcance comprende la aplicación de controles organizacionales, de personas, físicos y tecnológicos establecidos en el Anexo A de la NTP ISO/IEC 27001:2022, sobre los siguientes elementos:

1. **Infraestructura tecnológica del Centro de Datos institucional del MTC, incluyendo:**
   - Servidores físicos y virtuales.
   - Redes de comunicaciones y equipos de interconexión.
   - Sistemas de almacenamiento de información.
   - Plataformas de respaldo, contingencia y recuperación.
   - Plataformas de monitoreo, trazabilidad y auditoría de eventos de seguridad.
   - Sistemas de energía, climatización y soporte físico del centro de datos que alojan infraestructura crítica del SNC.

2. **Activo de información crítico asociado al Sistema Nacional de Conductores (SNC)**

   El activo crítico protegido en el marco del SGSI corresponde a la información gestionada por el Sistema Nacional de Conductores, incluyendo los datos personales y biométricos asociados a los registros de conductores, cuya

[1] No forman parte del alcance de certificación los procesos, servicios, sistemas y activos no descritos expresamente en el presente Anexo

confidencialidad, integridad y disponibilidad deben ser garantizadas conforme a la normativa vigente y a los controles establecidos en el SGSI.

Para efectos de su gestión tecnológica, dicho activo se encuentra soportado por el Sistema Nacional de Conductores (SNC), el cual comprende:

- Plataforma de gestión de licencias y registros de conductores.
- Bases de datos asociadas, sistemas operativos y componentes de software que soportan la operación del SNC, incluyendo sus mecanismos de seguridad.
- Interfaces de interoperabilidad con otras entidades del Estado y actores autorizados, en lo que respecta a los componentes bajo control y administración del MTC.
- Módulos de atención al ciudadano y mecanismos de validación biométrica, cuando corresponda.

3. **Sistemas y componentes tecnológicos que interactúan o dependen funcional o tecnológicamente del SNC**
   - Servicios web y APIs de intercambio de información.
   - Sistemas de autenticación, autorización y control de acceso.
   - Componentes de seguridad perimetral y protección de la información.

El presente alcance comprende los procesos, personas, instalaciones físicas, recursos tecnológicos y activos de información asociados al Centro de Datos institucional y al Sistema Nacional de Conductores, en la sede central del Ministerio de Transportes y Comunicaciones, así como los entornos tecnológicos directamente vinculados a su operación.

El alcance incluye exclusivamente los componentes tecnológicos, procesos y activos de información bajo control y administración del MTC, no extendiéndose a la infraestructura, sistemas o controles de seguridad de terceros con los cuales se mantengan relaciones de interoperabilidad o intercambio de información. Dichas dependencias externas son gestionadas mediante mecanismos contractuales, acuerdos de nivel de servicio, controles de seguridad aplicables y evaluaciones de riesgos correspondientes.

El Comité de Gobierno y Transformación Digital reconoce la necesidad de implementar y mantener el SGSI conforme a la NTP ISO/IEC 27001:2022 bajo un enfoque basado en riesgos y mejora continua, asegurando la confidencialidad, integridad y disponibilidad de la información gestionada.

Quedan fuera del alcance del SGSI los demás sistemas, procesos y servicios institucionales que no interactúan ni dependen funcional o tecnológicamente del Centro de Datos institucional o del Sistema Nacional de Conductores, sin perjuicio de su futura incorporación conforme al proceso de mejora continua del SGSI.

El presente alcance se encuentra documentado y aprobado por el Comité de Gobierno y Transformación Digital y será revisado periódicamente conforme al proceso de mejora continua del SGSI.