ANEXO N.º 1

PLIEGO DE PRESCRIPCIONES TÉCNICAS

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA PRESTACIÓN DE SERVICIOS DE AUDITORÍA DE CERTIFICACIÓN EXTERNA

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA PRESTACIÓN DE SERVICIOS DE AUDITORÍA DE CERTIFICACIÓN EXTERNA

00 | INTRODUCCIÓN

El objeto del presente procedimiento es LA "CONTRATACIÓN DE SERVICIO DE AUDITORÍA DE CERTIFICACIÓN EXTERNA".

La información contenida en estas prescripciones técnicas no es exhaustiva. El licitador deberá analizarla y solicitar cuantas aclaraciones considere necesarias en aras de poder confeccionar su mejor oferta.

La información complementaria que se genere como consecuencia de las aclaraciones solicitadas y facilitadas por LogiRAIL se pondrá en conocimiento de todos los participantes en esta licitación.

La oferta técnica presentada por los licitadores formará parte integrante del contrato que ampare la ejecución de este suministro licitado.

Las empresas licitadoras realizarán su oferta económica para el conjunto de los suministros objeto de la licitación. Serán desestimadas las ofertas que superen el precio máximo de la licitación.

01 | OBJETO DE LA LICITACIÓN

Con el objetivo de mantener la excelencia requerida, LogiRAIL identifica la necesidad de que sus centros de trabajo operen siguiendo los más altos estándares de calidad. Por este motivo LogiRAIL desea contratar los servicios con la finalidad de obtener las Certificaciones correspondientes, por áreas de la Sociedad, y que se citan en la presente Especificación.

El objeto del presente Pliego, junto con el pliego de cláusulas administrativas particulares, tiene por objeto fijar las condiciones de carácter técnico y de ejecución del contrato del servicio de auditoría, certificación y renovación de los siguientes estándares. Se hace constar que, en paralelo, LogiRAIL publicará el procedimiento de Servicios de consultoría, que se llevará en paralelo al proceso de Certificación.

La/s entidad/es adjudicatarias, deberán tener en cuenta este ejercicio paralelo, siendo conscientes de que deberán mantener la correspondiente interlocución, no solo con las personas encargadas del proceso en LogiRAIL, sino con aquellos que resulten adjudicatarios en cada proceso para los servicios de Consultoría.

- Lote 1: Servicios de auditoría externa en el ámbito de Servicios Tecnológicos
  - ISO 18295
  - ISO 20000-1
  - ISO 22301
  - ISO 33001
  - ISO 270001
  - ENS

- Lote 2: Servicios de auditoría externa por parte de entidad certificadora en el ámbito de Asistencia Jurídica y Compliance.
  - ISO 37301

  ➢ Con relación al Lote 2, se aporta como ANEXO, documento descriptivo del Contexto de la organización (Parte 1 y 2), sin perjuicio de poner a disposición del Licitador documentación adicional que pudiera precisar, en el curso del presente procedimiento de contratación, en plazo para preguntas. El alcance de la Certificación podría variar si así se viera necesario en los trabajos de Consultoría.

02 | ALCANCE

El objetivo es obtener la certificación que pruebe la adopción de las normas anteriores a través de las entidades certificadoras competentes.

- ISO 18295:
  La norma ISO 18295 es un estándar internacional de calidad para la industria de centros de llamadas, reemplazando a la norma europea EN 15838. Su objetivo es ayudar a las organizaciones a demostrar su compromiso con la profesionalidad y la mejora continua en el servicio al cliente.

  Se compone de dos partes: ISO 18295-1 e ISO 18295-2. La primera establece requisitos para los centros de llamadas, mientras que la segunda describe los requisitos para las organizaciones clientes que utilizan estos centros. Ambas partes se aplican tanto a centros internos como externalizados, sin importar su tamaño o sector, y cubren diversos aspectos como la relación con el cliente, enfoque centrado en el cliente, recursos humanos, datos operativos e infraestructura de servicios.

- ISO 20000-1:
  La norma ISO 20000-1 es un estándar internacional de gestión de servicios de tecnologías de la información (TI). Su objetivo principal es establecer los requisitos para implementar un sistema de gestión de servicios de TI efectivo y eficiente. La norma se centra en garantizar la entrega de servicios de calidad, alineados con las necesidades y expectativas del cliente.

  ISO 20000-1 se basa en un enfoque de procesos y especifica los requisitos para la planificación, diseño, transición, entrega y mejora continua de los servicios de TI. Esto incluye aspectos como la gestión de la disponibilidad, la gestión de la capacidad, la gestión del nivel de servicio, la gestión de la continuidad del servicio y la gestión de proveedores.

- ISO 22301:
  La norma ISO 22301 es un estándar internacional de gestión de continuidad del negocio. Su objetivo es ayudar a las organizaciones a establecer, implementar, mantener y mejorar sistemas de gestión de la continuidad del negocio (BCM por sus siglas en inglés) para garantizar que puedan seguir operando durante situaciones de crisis o interrupciones inesperadas.

  La norma ISO 22301 se divide en varias secciones que abordan diferentes aspectos del BCM, como la comprensión del contexto organizacional, el liderazgo y el compromiso, la planificación y el apoyo operacional, la evaluación de riesgos y oportunidades, y la monitorización y mejora continua.

- ISO 33001:
  La norma ISO 33001, también conocida como SPICE (Proceso de Evaluación de Sistemas de Información), es un estándar internacional que proporciona un marco para la evaluación de la capacidad y la mejora de los procesos de desarrollo y mantenimiento de sistemas de información. SPICE se centra en evaluar la capacidad de los procesos utilizados en el ciclo de vida del desarrollo de software y sistemas de información, desde la gestión de requisitos hasta el mantenimiento y la mejora continua.

  Esta norma se divide en diferentes partes, cada una de las cuales se centra en aspectos específicos del proceso de desarrollo de software y sistemas de información. Al utilizar SPICE, las organizaciones pueden evaluar y mejorar sus procesos, lo que les permite desarrollar productos de software de alta calidad de manera más eficiente y eficaz.

  En resumen, ISO 33001 (SPICE) proporciona un enfoque sistemático para evaluar y mejorar los procesos de desarrollo de software y sistemas de información, lo que ayuda a las organizaciones a aumentar su capacidad para producir productos de software de alta calidad de manera consistente.

- ISO 27001:
  La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. La norma

proporciona un marco para la seguridad de la información que ayuda a las organizaciones a identificar y gestionar sus riesgos de seguridad de la información de manera efectiva.

- ENS:
  El Esquema Nacional de Seguridad, de aplicación a todo el Sector Público, así como a los proveedores que colaboran con la Administración, ofrece un marco común de principios básicos, requisitos y medidas de seguridad para una protección adecuada de la información tratada y los servicios prestados, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

- ISO 9001
  La norma ISO 9001 es un estándar internacional que establece los requisitos para un Sistema de Gestión de Calidad y provee orientación y herramientas para asegurar el cumplimiento de los requerimientos legales y de los clientes.

- ISO 14001
  La norma ISO 14001 es un estándar internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión Medioambiental eficaz, para promover la estandarización de formas de producir y prestar servicios protegidos al medio ambiente, minimizando los efectos dañinos de las actividades organizacionales.

- ISO 45001
  La norma ISO 45001 es un estándar internacional que especifica los requisitos para el sistema de gestión de la seguridad y salud ocupacional, para la mejora continua y la gestión más eficaz y eficiente de los riesgos para la Seguridad y Salud en el Trabajo.

- Sistema de Gestión de Seguridad Operacional Ferroviaria
  En base a la recomendación técnica 8/2019 de la Agencia Estatal de Seguridad Ferroviaria y normativa aplicable, teniendo en cuenta el Reglamento Delegado (UE) 2018/762 por el que se establecen Métodos Comunes de Seguridad (MCS) sobre los requisitos del sistema de gestión de la seguridad, se establece un Sistema de Gestión de Seguridad Operacional Ferroviaria basado en el ciclo de la mejora contínua y en la evaluación de riesgos.

- ISO 37301

  La Norma ISO 37301 es un estándar internacional que marca los requisitos y proporciona directrices para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión de compliance eficaz dentro de una organización. El Alcance inicial previsto, sin perjuicio de modificación posterior, según resulte de la Consultoría es el siguiente:

ALCANCE - ÁREAS DE OBLIGACIONES PARA DETERMINACIÓN DE RIESGOS Y CONTROLES
▪ Gestión contra el fraude, la corrupción y los conflictos de interés.
▪ Protección de datos / Privacidad.
▪ Prevención del delito corporativo.
▪ Prevención del soborno.
▪ Prevención del blanqueo de capitales y de la financiación del terrorismo.
▪ Gestión de los canales del sistema interno de información.

03 | METODOLOGÍA DE TRABAJO

La prestación del servicio objeto de la contratación contemplará la ejecución de las siguientes actividades a detallar en su propuesta:

- Servicios de Auditoría (Lote I y II):
  - Elaboración de programa y plan de auditorías
  - Auditoría de certificación

- Elaboración de informes de auditorías
  A la finalización de las auditorías, se realizará la reunión final de las auditorías donde se expondrán las "No Conformidades" y "observaciones" detectadas y se aclararán todas las dudas e información adicional que se demande para la comprensión del incumplimiento detectado.
  El informe de auditoría deberá entregarse a la finalización de la reunión final y deberá contener toda la información indicada en las normas de certificación y para las no conformidades y observaciones detectadas:
  - Proceso / Procedimiento que incumple
  - Requisito de la norma incumplido

04 | LUGAR DE PRESTACIÓN DEL SERVICIO

Todo el territorio peninsular, centrándose la coordinación en oficinas de LogiRAIL en Calle Maestro Ángel Llorca nº6, 2ª planta (28003), Madrid.

Se permitirá las auditorías en remoto, si bien el licitador deberá adoptar las garantías suficientes para su validez.

05 | PROGRAMACIÓN Y PLANIFICACIÓN DEL SERVICIO

A continuación, se incluye un cronograma con la estimación temporal de ejecución del servicio a seguir por el adjudicatario. Este calendario se ha definido en base a los ciclos de validez de los certificados y terminará de concretarse conjuntamente junto a la entidad certificadora que aplique y LogiRAIL, para fijar las sesiones concretas dentro de los periodos estimados. En todo caso, el adjudicatario y LogiRAIL podrán acordar la modificación de este cronograma, si fuera conveniente para el buen fin de la ejecución del Contrato.

	2024		2025				2026				2027			
	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
ENS						Consultoría								
							Renovación							
ISO 27001		Consultoría 1.1	Consultoría 1.2			Consultoría 2.1	Consultoría 2.2			Consultoría 3.1	Consultoría 3.2			
				Seguimiento 1				Seguimiento 2				Renovación		
ISO 18295	Consultoría 1				Consultoría 2				Consultoría 3					
		Auditoría				Seguimiento 1				Seguimiento 2				
ISO 200000-1				Consultoría 1				Consultoría 2				Consultoría 3		
					Auditoría				Seguimiento 1				Seguimiento 2	
ISO 22301				Consultoría 1				Consultoría 2				Consultoría 3		
					Auditoría				Seguimiento 1				Seguimiento 2	
ISO 33001				Consultoría 1				Consultoría 2				Consultoría 3		
					Auditoría				Seguimiento 1				Seguimiento 2	
ISO 37301	Auditoría Interna 1				Auditoría Interna 2				Auditoría Interna 3				Auditoría Interna 4	
	Consultoría 1 a y b				Consultoría 2 a y b				Consultoría 3 a y b				Consultoría 4 a y b	
		Auditoría				Seguimiento 1				Seguimiento 2				Renovación
ISO 9001	Consultoría 1				Consultoría 2				Consultoría 3				Consultoría 4	
ISO 14001	Consultoría 1				Consultoría 2				Consultoría 3				Consultoría 4	
ISO 45001	Consultoría contínua (conforme al plan y programa establecido)													
Seguridad Operacional	Consultoría contínua (conforme al plan y programa establecido)													

El alcance estimado de la Consultoría y de la Auditoría Externa-Certificación es el siguiente (Dada la actividad en paralelo, se considera necesario citar ambos servicios en esta especificación técnica para una mayor claridad de la imagen global del proceso):

CONSULTORÍA 1 a y b + AUDITORIA INTERNA 1 - AUDITORÍA EXTERNA -CERTIFICACIÓN

CONSULTORÍA 2 a y b + AUDITORIA INTERNA 2 - ISO SEGUIMIENTO AÑO 1

CONSULTORÍA 3 a y b + AUDITORIA INTERNA 3 - ISO SEGUIMIENTO AÑO 2

CONSULTORÍA 4 a y b + AUDITORIA INTERNA 4 (solo en Lote 2) - ISO RENOVACIÓN CERTIFICACIÓN

06 | EQUIPO

El proveedor deberá incluir en su oferta los perfiles profesionales detallados de las personas propuestas para la prestación de los servicios. Para cada perfil se deberá especificar al menos:

- Experiencia previa en trabajos similares (listado de proyectos realizados, funciones en cada uno de ellos, y duración).
- Certificaciones de aplicación para la ejecución de los trabajos.
- Formación.
- Rol previsto en la ejecución de los trabajos licitados y dedicación estimada.

El licitador responderá frente a LogiRAIL del equipo propuesto, tanto si es personal laboral, como si son profesionales autónomos contratados, debiendo quedar reflejada la relación contractual que se mantiene con cada perfil propuesto.

07 | FACTURACIÓN

Una vez emitido certificado, cuando procesa y así se haya solicitado o finalizados los servicios (deberá haber un acta de finalización conforme firmada por ambas partes), el licitador podrá emitir la factura correspondiente a los servicios prestados.

La oferta que se incluya por el licitador, deberá incluir todos los costes que pueda originar el proceso, incluida la emisión de los Certificados ISO originales, así como los derechos asociados a la marca de certificación.

Madrid, julio de 2024.

Jaime Gil Casas.
Director de Innovación, Transformación Digital y Servicios Tecnológicos.

Cristina Ancizu Beramendi.
Gerente de Asesoría Jurídica.

Requisitos de Seguridad en Materia de Confidencialidad de la Información y Privacidad

ANEXO I REQUISITOS DE SEGURIDAD EN MATERIA DE CONFIDENCIALIDAD DE LA INFORMACIÓN

PARTE I

El licitador cumplirá cada uno de los requisitos expuestos a continuación y desarrollados en la PARTE II del presente ANEXO. Se acreditará mediante la cumplimentación de la declaración responsable de acreditación de documentación (ANEXO II del PCP):

- El licitador asegura que en caso de resultar adjudicatario dispondrá de las siguientes figuras, estando debidamente recogidas y documentadas, y siendo personas distintas; tal y como establece el artículo 13.5 en su apartado 5 del RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) conforme a lo indicado en el punto 1.4 de la PARTE II del Anexo I de las Especificaciones Técnicas:
  - Responsable del Proyecto
  - Responsable de Seguridad
- El licitador asegura que una vez sea adjudicatario realizará un análisis de riesgos conforme al artículo 14 del ENS según la metodología conforme al ENS, que en particular LogiRAIL identifica como MAGERIT (herramienta PILAR), salvo que, por indicación contraria y expresa, del Responsable de Seguridad de los Sistemas de Información se especifique lo contrario. Este Análisis de Riesgos (realizado una vez sea adjudicatario del servicio), será compartido con la Oficina de Riesgo y Marco, conforme a lo indicado en el punto 4.1 de la PARTE II del Anexo I de las Especificaciones Técnicas.
- El licitador asegurará que, en caso de resultar adjudicatario mantendrá y pondrá a disposición de LogiRAIL, un inventario actualizado de la totalidad de equipos objeto de la presente licitación, conforme a lo indicado en el punto 6.3 de la PARTE II del Anexo I de las Especificaciones Técnicas.
- El servicio ofertado está certificado en el ENS nivel MEDIO, tal y como aparece recogido en el Documento de Seguridad “Obligaciones de los prestadores de servicios a las entidades públicas” del CCN. En caso de no estar certificado, el licitador se comprometerá a solicitar, en caso de resultar adjudicatario, dicha certificación en los primeros 6 meses de prestación del servicio. En caso de que el servicio ofertado por el licitador no esté certificado en el ENS, pero esté certificado por un tercero externo, de un Sistema de Gestión de la Seguridad de la Información (SGSI), basado en la 27001 o similar, el licitador se comprometerá a solicitar dicha certificación durante los 8 primeros meses de prestación del servicio, en caso de resultar adjudicatario. Todo ello, de acuerdo con lo indicado en el punto 8.1 de la PARTE II del Anexo I de las Especificaciones Técnicas.

PARTE II

1. Relacionados con las **Políticas de Seguridad**, se deberá cumplir con los siguientes requisitos:
   - 1.1. El adjudicatario, deberá conocer y cumplir las medidas de Seguridad incluidas en la Política de Seguridad de los Sistemas de Información de LogiRAIL, recogidas y especificadas en el resto de Requisitos que se detallan a continuación.
   - 1.2. El adjudicatario, deberá tener establecidas Políticas de Seguridad de los Sistemas de Información en su empresa.
   - 1.3. El adjudicatario, deberá disponer de un programa sobre Seguridad de la Información para supervisar el establecimiento y mantenimiento de las políticas, estándares e iniciativas sobre seguridad de la Información.
   - 1.4. El licitador deberá asegurar que dispondrá de las siguientes figuras en caso de resultar adjudicatario, estando debidamente recogidas y documentadas, y siendo personas distintas; tal y como establece el artículo 13 en su apartado 5 del ENS:
     - 1.4.1. Responsable del Proyecto.
     - 1.4.2. Responsable de Seguridad.
   - 1.5. La gestión de la Seguridad de la Información se abordará desde un enfoque basado en el riesgo. Por lo tanto, el adjudicatario deberá implementar procesos, procedimientos o metodologías formales y documentadas para la evaluación del Riesgo de Seguridad de la Información.
   - 1.6. En su caso, las empresas subcontratadas por el adjudicatario que sean o puedan llegar a ser procesadores de información de LogiRAIL o bien tengan acceso a la red o sistemas de LogiRAIL, deberán adoptar las mismas políticas y estándares sobre seguridad de la información que mantiene con LogiRAIL.
   - 1.7. El personal del adjudicatario y el personal de las empresas subcontratadas por el adjudicatario (en caso de que aplique) deberá firmar un Acuerdo de Confidencialidad con LogiRAIL, así como cumplir los procedimientos de seguridad establecidos para los adjudicatarios.

2. El adjudicatario deberá cumplir con los siguientes requisitos de seguridad relativos a la **Clasificación de Seguridad, confidencialidad y propiedad intelectual de la Información**:
   - 2.1. Deberá realizar un tratamiento de la Información teniendo en cuenta la clasificación de la Información que haya realizado el Responsable de la Información interno de LogiRAIL.
   - 2.2. Deberá contar con controles asociados a la información clasificada en virtud de esa confidencialidad.
   - 2.3. El adjudicatario no divulgará información de proyecto (naturaleza, herramientas de desarrollo, arquitectura, etc.) a terceros no autorizados, con especial atención a otro personal del adjudicatario no autorizado en el proyecto adjudicado, así como la fuga por divulgación en redes sociales de la empresa o en los perfiles profesionales de sus trabajadores.
   - 2.4. Deberá respetar la propiedad intelectual de LogiRAIL sobre los requisitos, códigos, ejecutables y documentación.
   - 2.5. Relativo al acceso a la Información, el adjudicatario deberá disponer de documentación formal en la que se detallen los requisitos necesarios para garantizar una gestión eficaz del acceso a la información, incluyendo su otorgamiento, aprobación, revisión y retirada.
   - 2.6. El adjudicatario sólo podrá disponer de la información de LogiRAIL que el mismo le autorice o esté recogida dentro del alcance del servicio.

2.7. Toda información que sea entregada por LogiRAIL al adjudicatario para que salga de las instalaciones de LogiRAIL, se realizará a través de un dispositivo cifrado proporcionado por el adjudicatario.

3. En relación con la **Notificación de Incidentes de Seguridad**, el adjudicatario deberá cumplir con los siguientes requisitos:
   3.1. El adjudicatario, debe conocer y cumplir las obligaciones, que, en relación con los incidentes de seguridad, LogiRAIL tiene con las diferentes autoridades de control y de las que por proveer el servicio asume como encargado del tratamiento y bajo el alcance del contrato.
   3.2. Se han de implantar procesos o procedimiento formal y documentado para la notificación, escalado, investigación y resolución de incidentes relativos a la seguridad de la información.
   3.3. En el tratamiento de los incidentes de seguridad de la información, deberá contactarse con el Responsable de Seguridad de LogiRAIL.
   3.4. Deberá ofrecer mecanismos para que:
      3.4.1. LogiRAIL pueda informar al adjudicatario sobre eventos de seguridad que ha detectado.
      3.4.2. El adjudicatario informe a LogiRAIL sobre eventos de seguridad que ha detectado.
      3.4.3. LogiRAIL pueda realizar un seguimiento de la situación de un evento de seguridad del que haya sido informado.

4. En relación con los **Análisis de Riesgos,** el adjudicatario deberá cumplir con los siguientes requisitos:
   4.1. El licitador que resulte adjudicatario deberá llevar a cabo un análisis de riesgos conforme al artículo 14 del ENS según la metodología conforme al ENS, que en particular LogiRAIL identifica como MAGERIT (herramienta Pilar), salvo que, por indicación contraria y expresa, del Responsable de Seguridad de los Sistemas de Información se especifique lo contrario. El análisis de riesgos deberá incluir:
      - Identificación de los activos que forman parte del proyecto (comunicaciones, hardware, software, personal, etc).
      - Valoración del servicio.
      - Riesgo Inicial acorde a Magerit (Alto, Medio o Bajo).
      - Amenazas de seguridad.
      - Controles de seguridad que mitiguen las amenazas.
      - Riesgo Residual obtenido tras aplicar los controles de seguridad, también acorde a Magerit (Alto, Medio o Bajo).

      Este Análisis de Riesgos cumple con un doble objetivo: por un lado, el adjudicatario es consciente de los riesgos de ciberseguridad que debe tener en cuenta, y, por otro lado, debe ser consciente que la calidad del Análisis de Riesgos realizado, le permitirá responder más adecuadamente las salvaguardas que le sean de aplicación, una vez gestionado y evaluado el riesgo por el Responsable de Seguridad de los Sistemas de Información.
      El Análisis (realizado una vez sea adjudicatario del servicio), será compartido con la Oficina de Riesgo y Marco, ya que formará parte de la evaluación del Riesgo que realiza el Responsable de Seguridad de los Sistemas de Información. El adjudicatario deberá colaborar e implementar bajo el alcance del contrato, aquello que le sea de aplicación.

5. Relacionados con la **Seguridad de la Red, del Software**, **de la Operación y de las tecnologías de la Información,** el adjudicatario deberá cumplir con los siguientes requisitos:
   5.1. Deberá disponer de documentación formal detallando las medidas necesarias para proteger los sistemas de Información frente a los actos maliciosos o malintencionados.
   5.2. Los sistemas del adjudicatario dentro del alcance de estos trabajos, deberán tener instaladas las últimas revisiones del software y deberá existir un programa/proceso de actualización.
   5.3. Tanto el software como las aplicaciones utilizadas como soporte de las actividades empresariales de LogiRAIL deben estar configurados para solucionar factores de vulnerabilidad y amenazas conocidas y nuevas en un plazo aceptable.
   5.4. Los sistemas de información, como equipos personales (portátiles entre otros) que sean propiedad del adjudicatario o bien de las empresas subcontratadas por el adjudicatario (en caso de que aplique) y hagan uso de las redes de usuario de LogiRAIL deberán estar correctamente protegidos y configurados para que no representen una amenaza a la confidencialidad, disponibilidad e integridad de la información de LogiRAIL. Entre otras cuestiones de configuración de los mismos, NO deben generar tráficos no autorizados desde las redes de LogiRAIL hacia recursos externos o internos de la red del adjudicatario.
   5.5. El adjudicatario deberá disponer de una política de copias de seguridad (backup) específica, la cual debe incluir la identificación no sólo de los procesos identificados como relacionados con el proyecto/servicio/desarrollo, sino también aquellos procesos internos del adjudicatario que incorporan copia de información de Renfe EPE como parte de sus datos (que incluso puede no estar identificada en los sistemas internos del adjudicatario como de LogiRAIL). Deberán implantarse procesos o procedimientos formales y documentados para garantizar la realización de copias de seguridad y para la recuperación de la Información.
   5.6. A la hora de realizar una copia de seguridad (backup) de los equipos que contengan datos de LogiRAIL, el adjudicatario deberá solicitar autorización expresa, indicando la información que contienen dichos equipos. En cualquier otro caso en el que la información deba salir del ámbito de LogiRAIL, el adjudicatario deberá tomar las medidas necesarias en virtud de la clasificación de seguridad de la información.

6. En relación con los **equipos** que vayan a conectarse a las redes o sistemas de información de LogiRAIL, o vayan a tratar información de LogiRAIL, el adjudicatario deberá:
   6.1. El adjudicatario deberá contar con un plan de acciones correctivas dentro del proceso de mantenimiento para hacer frente a cualquier incidencia software y/o hardware que se produzca en los equipos o cualquiera de sus componentes.
   6.2. El adjudicatario deberá mantener los equipos actualizados a la última versión de Software disponible por el fabricante o fabricantes, según un proceso o política de actualización que deberá ser elaborado por el adjudicatario.
   6.3. Deberá mantener y poner a disposición de LogiRAIL de un inventario actualizado de la totalidad de equipos. Este inventario deberá contener al menos los siguientes campos:
      a. Dirección IP del equipo.
      b. Nombre del equipo (hostname).
      c. Dirección MAC del equipo
      d. Inventario actualizado del Software instalado en cada equipo.
      e. Modelo del equipo.

f. Versión del sistema operativo instalado.
g. Marca, modelo y Versión de antimalware instalado.

6.4. El adjudicatario realizará la remediación de infecciones que se produzcan en los equipos y se responsabilizará de la efectividad de dicha remediación. Asimismo, y para minimizar el número de estas posibles acciones, el adjudicatario deberá realizar la instalación y el mantenimiento de actualizaciones de un producto antimalware.

6.5. El adjudicatario que haga uso de equipos de usuario (Windows 7, Windows 10 y Windows 11, Linux centOs 7 y Linux centOs 8) portátiles, sobremesa o cualquier otro tipo de dispositivo (Surface), no gestionado por LogiRAIL, en los que se vaya a tratar información de LogiRAIL o se vayan a conectar a la red o sistemas de información de LogiRAIL, deberá proporcionar a la Gerencia de Área de Ciberseguridad y Privacidad la siguiente información para cada uno de los equipos:

6.5.1. Informe individual del equipo con el detalle obtenido por el adjudicatario de la herramienta CLARA del CCN para determinar el cumplimiento con las características de seguridad técnicas definidas en el ENS para una categorización del sistema con nivel MEDIO.
La Gerencia de Área de Ciberseguridad y Privacidad considerará seguro un equipo cuando el informe indique un cumplimiento con las características de seguridad técnicas definidas en el ENS para una categorización del sistema con nivel MEDIO de un 65% o superior.

6.5.2. Informe agregado de cumplimiento elaborado por el adjudicatario, en el que se debe incluir en el nivel de cumplimiento obtenido en el informe individual, de cada uno de los equipos bajo alcance del proyecto. Este informe debe indicar el valor agregado, que será el valor medio del Informe individual (6.5.1) de todos los equipos bajo alcance del proyecto.

6.6. En el caso de que los equipos utilicen tecnologías de comunicación inalámbrica, el adjudicatario deberá cumplir con los siguientes requisitos:

6.6.1. El adjudicatario debe minimizar, en lo posible, el uso de redes inalámbricas frente a redes cableadas, dado que por el diseño de especificaciones son más inseguras.

6.6.2. La red inalámbrica proporcionará comunicaciones cifradas.

6.6.3. La red inalámbrica deberá estar provista de métodos de autenticación como contraseñas, u otros mecanismos seguros de autenticación (firmas digitales, entre otros), para estar protegida de modificaciones o usos no autorizados.

6.6.4. El adjudicatario debe incluir este equipamiento inalámbrico dentro de los procesos de gestión del riesgo y gestión de las vulnerabilidades.

7. En relación con la **Seguridad relativa a terceras partes y a recursos humanos**, el adjudicatario deberá cumplir los siguientes requisitos:

7.1. Deberán realizarse evaluaciones de los riesgos para la seguridad de la información de los proveedores para las terceras partes que accedan, procesen, recojan, creen o almacenen información de LogiRAIL.

7.2. Todo el personal del adjudicatario deberá conocer las políticas, estándares y procesos sobre seguridad de la información que resulten de aplicación. Además, dicho personal, deberá estar formado y concienciado en materia de seguridad de la información.

7.3. Los empleados, contratistas, agentes y otras terceras partes implicadas en el proyecto deberán, sobre sus responsabilidades, recibir formación, al menos con carácter anual o bien mediante

acciones de concienciación en aquellos momentos que el Adjudicatario considere necesario, para garantizar la seguridad y la protección de los recursos de información del LogiRAIL.

7.4. Todos los usuarios del adjudicatario que vayan a acceder a las redes o sistemas de información del LogiRAIL, o vayan a acceder a información de LogiRAIL, deben estar dados de alta en la gestión de identidad de LogiRAIL, para lo que se necesitan los siguientes datos:

a. Nombre y apellidos.
b. DNI.
c. Correo electrónico profesional.
d. Teléfono móvil.

8. Relativo a los aspectos de **Cumplimiento Normativo de Seguridad**:

8.1. El servicio ofertado por el licitador debe estar certificado en el ENS nivel MEDIO, tal y como aparece recogido en el Documento de Seguridad "Obligaciones de los prestadores de servicios a las entidades públicas" del CCN. En caso de no estar certificado, el licitador se comprometerá a solicitar dicha certificación durante los 6 primeros meses de prestación del servicio, en caso de resultar adjudicatario.

En el caso que el servicio no esté certificado en el ENS, pero esté certificado por un tercero externo, de un Sistema de Gestión de la Seguridad de la Información (SGSI), basado en la 27001 ó similar, el licitador se comprometerá a solicitar dicha certificación durante los 8 primeros meses de prestación del servicio, en caso de resultar adjudicatario. El aumento temporal de 2 meses en la solicitud de la certificación en el ENS, en este caso, se debe a que el licitador se encuentra ya en cumplimiento con un Marco de Seguridad de la Información.

8.2. Debe contemplarse el compromiso de devolución/destrucción (a elección de LogiRAIL) de la información confidencial recabada durante la ejecución del servicio.

8.2.1. Si por la naturaleza del proyecto, LogiRAIL requiere del borrado y destrucción de cualquier soporte de información o elemento hardware englobado al alcance del servicio prestado; el adjudicatario deberá aplicar un procedimiento seguro de borrado y destrucción conforme a lo indicado en el Esquema Nacional de Seguridad.

8.2.2. Asimismo, para cada borrado/destrucción realizado, el adjudicatario deberá entregar a LogiRAIL un certificado recogiendo al menos los siguientes campos:

a) Fecha recogida material.
b) Personal proveedor encargado de la recogida y transporte.
c) Procedimiento detallado empleado en el borrado/destrucción realizado.
d) Fecha destrucción material.