# ANEXO N.º 1

## PLIEGO DE PRESCRIPCIONES TÉCNICAS

### PLIEGO DE ESPECIFICACIONES TÉCNICAS PARA LA PRESTACIÓN DEL SERVICIO DE EVOLUCIÓN DE LA PLATAFORMA DE GESTIÓN DE IDENTIDADES DE RENFE

## 00 | INTRODUCCIÓN

El objeto del presente procedimiento es la realización de un evolutivo sobre la plataforma de gestión de identidades de la que dispone RENFE para integrar al colectivo de usuarios designados por LogiRAIL y otras adaptaciones a cambios o necesidades que surjan a este respecto.

El licitador deberá analizar y solicitar cuantas aclaraciones considere necesarias a lo especificado en estas prescripciones técnicas en aras de poder confeccionar su mejor oferta, con una propuesta de solución que responda a los requisitos aquí detallados.

La información complementaria que se genere como consecuencia de las aclaraciones solicitadas y facilitadas por la Dirección de Innovación, Transformación Digital y Servicios Tecnológicos de 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 | INTRODUCCION Y OBJETIVOS

LogiRAIL, SME, S.A. es el medio propio del Grupo Renfe. Se trata de una sociedad mercantil estatal cuyo capital es en su totalidad de titularidad pública, dividido de la siguiente forma:

- RENFE MERCANCÍAS SOCIEDAD MERCANTIL ESTATAL, S.A., 34 %
- RENFE VIAJEROS SOCIEDAD MERCANTIL ESTATAL, S.A., 33 %
- RENFE INGENIERÍA Y MANTENIMIENTO SOCIEDAD MERCANTIL ESTATAL, S.A., 33 %

La infraestructura informática de LogiRAIL, específicamente en lo que respecta al directorio activo y la administración de usuarios y permisos, está intrínsecamente ligada a la arquitectura perteneciente a RENFE. La gestión de usuarios se lleva a cabo por el equipo técnico de RENFE, que opera en la infraestructura local (On-Premise), la cual se encuentra sincronizada con su contraparte en la nube (Cloud), administrada por el equipo de Soporte TI de LogiRAIL.

La sincronización de los datos entre la infraestructura local y la nube se realiza a través del software Syncronization Service Manager, alojado en un servidor de RENFE. Este proceso asegura que los datos que constituyen el perfil del usuario en el entorno Cloud sea un reflejo exacto de la parte física. Como resultado, el equipo de Soporte de LogiRAIL no puede modificar los datos, ya que cualquier cambio se sobrescribiría durante los ciclos de sincronización programados por RENFE.

Además, el procedimiento de incorporación de usuarios mediante el formulario estándar de RENFE impide la adición de información adicional a las propiedades del usuario. Esta limitación restringe significativamente la capacidad de crear grupos dinámicos, generar informes de Power BI, entre otros, incrementando la necesidad de intervención manual en la gestión del Tenant y sus componentes, y reduciendo la posibilidad de automatización.

La posibilidad de introducir datos adicionales mejoraría sustancialmente la administración de permisos, licencias e identidades, optimizando los procesos operativos y reduciendo la necesidad de pasos intermedios y personal dedicado a la recopilación de información.

En base a lo anterior, el objetivo de la presente licitación es el desarrollo de evolutivos sobre la solución de gestión de identidades y accesos de RENFE para que permita la integración de este nuevo colectivo de usuarios en la plataforma y otras necesidades de cambio que puedan surgir al respecto.

Esta especificación recoge los servicios profesionales requeridos para la integración de una nueva fuente autoritativa de gestión de identidades de RENFE basada en tecnología OpenIAM y la ejecución de evolutivos sobre la plataforma GID para poder adaptarla a las necesidades de LogiRAIL.

Objetivos que lograr:

- Integración del nuevo colectivo de LogiRAIL
    - Integración de LogiRAIL como fuente autoritativa.
    - Integración con RDA.

    - Proceso de recertificación.
- Evolución sobre la plataforma de gestión de identidades OpenIAM

## 02 | ALCANCE

El servicio de evolución de la plataforma de gestión de identidades de RENFE se debe articular en 2 ejes o líneas de actuación:

- Integración del colectivo de LogiRAIL y proceso de recertificación.
- Evolución sobre la plataforma de gestión de identidades OpenIAM

### 02.01 | INTEGRACIÓN DE NUEVO COLECTIVO LOGIRAIL Y PROCESO DE RECERTIFICACIÓN

#### 02.01.01 | INTEGRACIÓN DE LOGIRAIL COMO FUENTE AUTORITATIVA

Para la integración de LogiRAIL como fuente autoritativa es necesario definir nuevos objetos y procesos en la actual gestión de identidades:

- Definición de nuevo tipo de usuario en OpenIAM que permita su tratamiento en los procesos de OpenIAM involucrados en la gestión de la identidad (pre/post procesos, políticas de atributo para sistemas finales, reconciliaciones, sincronizaciones, workflow).

- Creación de un nuevo proceso de sincronización en OpenIAM que genere las operaciones que deben realizarse sobre la gestión de identidades:

    - Alta de usuario (creación de usuario en OpenIAM).
    - Modificación de usuario (actualización de datos en OpenIAM).
    - Baja de usuario (desactivación de usuario en OpenIAM y bloqueo de cuentas en sistemas finales).
    - Reactivación de usuario (reactivación de cuentas del usuario en sistemas finales).

- Tratamiento de excepciones para identificar los usuarios que no deben ser tratados por el proceso de sincronización.

- Umbral de salvaguarda, que permita incrementar temporalmente el número máximo de operaciones permitidas y relanzar el proceso de sincronización (previa validación de negocio).

- Envío de notificaciones:

    - Notificación de información del proceso (a enviar a los usuarios y responsables involucrados en la revisión de la tarea de sincronización): información sobre el número de operaciones detectadas y necesidad o no de activar el umbral de salvaguarda. Aviso en caso de que se hayan detectado cambios en usuarios (a nivel de tratamiento de excepciones) y sobre cambios de responsable para usuarios colaboradores.
    - Notificación de altas y bajas de usuario (a enviar a los responsables de sistemas en los que se realicen tareas adicionales al alta de usuarios).
    - Notificación de Remedy (creación ticket en Remedy por cada baja procesada).

#### 02.01.02 | INTEGRACION CON RDA:

Integración con RDA para actualizar y ampliar el actual mapa de políticas del sistema gestionado para el tratamiento de los usuarios de LogiRAIL.

- Creación y adaptación de políticas de atributo: El listado de atributos RDA gestionados actualmente por el conector son:

| Atributo RDA | Valor usuario Renfe |
|---|---|
| AccountPassword | Password del usuario |
| Co | Atributo usuario RNF_USER_NACION |
| Company | Atributo usuario RNF_USER_EMPRESA |
| CountryCode | Atributo usuario RNF_USER_TNACION |
| departmentNumber | Atributo usuario RNF_USER_AAHCOD |
| DisplayName | Nombre completo en formato “Nombre Apellidos” |
| EmailAddress | <Valor calculado> |
| employeeType | Atributo usuario RNF_USER_POSDES |
| Enabled | <Valor calculado> |
| extensionAttribute1 | Atributo usuario RNF_USER_EMPRCOD |
| extensionAttribute10 | Atributo usuario RNF_USER_DIVCOD |
| extensionAttribute12 | <Valor calculado> |
| extensionAttribute14 | <Valor calculado> |
| extensionAttribute2 | Atributo usuario RNF_USER_AACDES |
| extensionAttribute3 | Atributo usuario RNF_USER_AACCOD |
| extensionAttribute4 | Atributo usuario RNF_USER_NEGDES |
| extensionAttribute5 | Atributo usuario RNF_USER_NEGCOD |
| extensionAttribute7 | Atributo usuario RNF_USER_CNTCON |
| GivenName | Nombre |
| Group | Grupos del usuario |
| HomePhone | <No se asigna valor> |
| l | <No se asigna valor> |
| mobile | <No se asigna valor> |
| msExchRecipientDisplayType | <Valor calculado> |
| msExchRecipientTypeDetails | <Valor calculado> |
| msExchRemoteRecipientType | <Valor calculado> |
| Name | Identificador usuario |
| otherFacsimileTelephoneNumber | <No se asigna valor> |
| otherHomePhone | <No se asigna valor> |
| otherIpPhone | <No se asigna valor> |
| otherMobile | <No se asigna valor> |
| otherPager | <No se asigna valor> |
| otherTelephone | <No se asigna valor> |
| pager | <No se asigna valor> |
| Path | <Valor calculado> |
| PostalCode | <No se asigna valor> |
| proxyAddresses | <Valor calculado> |
| SamAccountName | Identificador de usuario. |
| st | <No se asigna valor> |
| street | <No se asigna valor> |
| Surname | Apellidos |
| targetAddress | <Valor calculado> |
| telephoneNumber | <No se asigna valor> |
| Title | Atributo usuario RNF_USER_CATCOD |
| url | <No se asigna valor> |

Los cambios que deben realizarse sobre las políticas de atributo actuales del sistema gestionado RDA para el mantenimiento de los atributos de los usuarios de LogiRAIL son:

| Atributo DA Usuario LogiRAIL | Tratamiento desde GID |
|---|---|
| **City (*)** | **Nueva política de atributo.** Recupera del fichero de RRHH el campo "Ciudad" |
| CN | Identificador de usuario. |
| Company | ***Modificar política de atributo*** para recuperar del fichero de RRHH el campo "Empresa". |
| **Department (*)** | **Nueva política de atributo**. Recupera del fichero de RRHH el campo "Departamento". |
| DisplayName | Nombre y apellidos del usuario |
| DistinguishedName | Identificador de usuario (Rama de DA usuarios LogiRail) |
| **Division (*)** | **Nueva política de atributo**. Recupera del fichero de RRHH el campo "Área de Negocio". |
| employeeType | ***Modificar política de atributo*** para recuperar del fichero de RRHH el campo "Tipo de contrato". |
| extensionAttribute4 | ***Modificar política de atributo*** para recuperar del fichero de RRHH el campo "Fecha Aplicación Antigüedad". |
| extensionAttribute5 | ***Modificar política de atributo*** para recuperar del fichero de RRHH el campo "Fecha Nacimiento". |
| GivenName | Nombre del usuario |
| l | Ciudad (*nueva política de atributo creada para City*). |
| **Manager (*)** | **Nueva política de atributo.** Recupera del fichero de RRHH el campo "Ciudad" |
| mobile | **Nueva política de atributo.** Recupera del fichero de RRHH el campo "Teléfono Móvil". |
| MobilePhone | **Nueva política de atributo.** Misma política que para el atributo "mobile". |
| Name | Identificador de usuario |
| **Office (*)** | **Nueva política de atributo.** Recupera del fichero de RRHH el campo "Centro de Trabajo". |
| **OfficePhone (*)** | **Nueva política de atributo.** Recupera del fichero de RRHH el campo "Teléfono Empresa". |
| otherMobile | ***Modificar política de atributo.*** Misma política que para el atributo "OfficePhone". |
| Pager | ***Modificar política de atributo.*** Misma política que para el atributo "OfficePhone". |
| **physicalDeliveryOfficeName (*)** | **Nueva política de atributo.** Misma política que para el atributo "Office". |
| SamAccountName | Identificador de usuario |
| sn | Apellidos de usuario. |
| Surname | Apellidos de usuario. |
| telephoneNumber | ***Modificar política de atributo.*** Misma política que para el atributo "OfficePhone". |
| Title | ***Modificar política de atributo*** para recuperar del fichero de RRHH el campo "Tipo de Empleado". |
| UserPrincipalName | UPN asignado para el usuario (logirail.com) |

(*) Atributos no recuperados actualmente por el conector

Debe revisarse también el comportamiento del resto de políticas de atributo usadas actualmente por el conector para el cálculo de los atributos de RDA de los usuarios de Renfe. Para los usuarios de LogiRAIL no deben informarse los siguientes atributos:

| Atributos DA no informados para usuarios de LogiRAIL | |
|---|---|
| Co | otherFacsimileTelephoneNumber |
| CountryCode | otherHomePhone |
| departmentNumber | otherIpPhone |
| EmailAddress | otherPager |
| extensionAttribute1 | otherTelephone |
| extensionAttribute10 | PostalCode |
| extensionAttribute12 | proxyAddresses |
| extensionAttribute14 | st |
| extensionAttribute2 | street |
| extensionAttribute3 | targetAddress |
| extensionAttribute7 | url |
| HomePhone | |
| msExchRecipientDisplayType | |
| msExchRecipientTypeDetails | |
| msExchRemoteRecipientType | |

- Modificación de conector del Directorio Activo para que incorpore el tratamiento de los nuevos atributos gestionados para los usuarios de LogiRAIL. Debe modificarse para que pueda gestionar los atributos: *City, Department, Division, Manager, Office, OfficePhone, physicalDeliveryOfficeName.*

### 02.01.03 | PROCESO DE RECERTIFICACIÓN

Durante el proceso de recertificación se consultará el fichero de RRHH que proporciona LogiRAIL para la toma de decisiones.

Un usuario interno de LogiRAIL puede tener dos cuentas en el AD.
- usuario@logirail.com. Se encuentra en la rama de LogiRAIL.
- usuario@colaboradores.renfe.com. Se encuentra en la rama de externos de todo el grupo Renfe.

Deberá revisarse diariamente el listado de usuarios activos de LogiRAIL del fichero de RRHH que tengan una cuenta adicional en la rama de colaboradores. Estos usuarios quedarán excluidos del proceso de recertificación.

También se revisará diariamente los usuarios que se encuentran en estado de baja en el fichero de RRHH de LogiRAIL. Para estos usuarios se comprobará si disponen de una cuenta adicional en la rama de usuarios colaboradores. Si disponen de una cuenta en la rama de colaboradores, se procederá a realizar la baja.

## 02.02 | EVOLUTIVOS SOBRE LA PLATAFORMA DE GESTIÓN DE IDENTIDADES OPENIAM

Actualmente, RENFE tiene implantada una solución de gestión de identidades y accesos basada en la herramienta OpenIAM. Las tareas que se engloban en este apartado son las necesarias para el desarrollo de evolutivos sobre la plataforma GID para poder adaptarla a los cambios o nuevas necesidades que surjan en torno a la gestión de identidades del ecosistema de LogiRAIL.

# 03 | MODELO DE CAPACIDAD Y CONSUMO DEL SERVICIO ENCARGADO

El modelo para la gestión de la capacidad de recursos para la prestación de los servicios de esta licitación y su consumo se fundamenta en jornadas laborales, siendo la unidad de medida para la valoración de los servicios.

Una jornadas de trabajo corresponde a 8 horas de servicio que incluye en general cualquier tipo de actividad relacionada con la gestión y resolución de las órdenes de trabajo, por ejemplo tareas de gestión del servicio, seguimiento del servicio y reporte a la estructura de control, actividades de aseguramiento y mejora de la calidad, confección de las actas de

reunión, gestión de los equipos de trabajo propios, gestión del ANS, gestión del conocimiento y transferencia periódica de conocimiento, y las tareas propias de las actividades técnicas destinadas a la resolución de las órdenes de trabajo (análisis funcional, diseño técnico, codificación, ETLs, construcción de los modelos de datos, construcción de algoritmos, soporte, consultas, documentación, pruebas, reuniones técnicas, seguimiento operativo, corrección de excepciones, entre otras).

Los conceptos fundamentales de capacidad y consumo son los siguientes:

- La Capacidad Máxima, que corresponde al volumen máximo de jornadas de trabajo por parte del licitador para la realización de los servicios encargados.
- Jornadas de trabajo incurridas, es el monto de jornadas de trabajo que han sido destinadas para la ejecución de una orden de trabajo.
- Precio de la jornada de trabajo, es el valor económico global, correspondiente al conjunto de actividades prestadas en la ejecución de una orden de trabajo por cada jornada de servicio realizado.

El modelo para la gestión de la capacidad y el consumo es el siguiente:

- Al inicio del Servicio se establecerá la Capacidad Máxima del contrato que podrá ser revisada, y servirá de referencia.
- Esta Capacidad Máxima se consumirá en función de las órdenes de trabajo, pero en ningún caso se garantiza que se vaya a consumir totalmente dicha Capacidad.
- Si se identifica un riesgo de desviación entre las jornadas de trabajo consumidas y la Capacidad Máxima del contrato establecida, se deberán promover planes de ajuste de desviaciones y escalar la situación.
- Se irá consumiendo bajo demanda según se vayan trasladando las órdenes de trabajo al servicio encargado y estas órdenes de trabajo alcancen sus hitos de consumo.
- El consumo mínimo por petición de trabajo será de media jornada.

Mensualmente se facturará por parte del proveedor, una vez remitida el acta con el desglose de los servicios prestados, el total de las jornadas de trabajo prestadas de acuerdo con los hitos de consumo alcanzados al precio convenido de las jornadas de trabajo.

## 04 | MODELO DE EJECUCIÓN

Cuando exista una necesidad de realización de un evolutivo se seguirá el siguiente proceso:

- El equipo técnico responsable del servicio en LogiRAIL proporcionará por escrito una descripción de las nuevas funcionalidades o mejoras a realizar.
- El adjudicatario realizará una valoración de las mejoras solicitadas, aclarando cuantas dudas surjan una vez recibida la solicitud de LogiRAIL.
- Una vez establecidos el ámbito y el entorno de actuación, el adjudicatario preparará una propuesta de ejecución que incluya:
    - Descripción de la propuesta y mejoras a realizar, incluyendo las modificaciones y desarrollos específicos a realizar.
    - Calendario de ejecución y plan de proyecto de los desarrollos a realizar (si procede).
    - Jornadas estimadas para la realización de los trabajos.
    - Inicio de los trabajos tras la aprobación de la propuesta por parte de LogiRAIL.

## 04 | PERFILES

Dada la criticidad y especificidad de las necesidades detalladas en la presente licitación, LogiRAIL considera que, para garantizar el correcto desarrollo del servicio objeto, los perfiles deberán contar con la certificación OpenIAM Specialist.

Los requisitos indicados en este punto de la especificación Técnica se exigen con carácter de mínimo imprescindible, de modo que el equipo ofertado deberá cumplir las condiciones incluidas en este punto.

## 05 | ESTIMACION DE ESFUERZOS MÍNIMOS POR SERVICIO

La dedicación mínima estimada podrá sufrir variaciones durante el contrato, pudiendo balancear las horas de un servicio a otro en función de las necesidades del proyecto.

| Concepto | Unidades de Medida | Unidades estimadas |
|---|---|---|
| Integración nuevo colectivo LogiRAIL y proceso de recertificación | Jornada de Trabajo | 25 |
| Evolutivos sobre la plataforma de gestión de identidades OpenIAM | Jornada de Trabajo | 20 |

LogiRAIL se reserva el derecho de no alcanzar el importe total de la adjudicación, de forma que el importe final resultante quedará vinculado al servicio efectivamente prestado en función de las necesidades reales de LogiRAIL.

## 06 | DURACIÓN

La duración del presente contrato es de 4 meses.

## 07 | HORARIOS

El horario diario de los trabajos será de 8 horas, de lunes a viernes laborables, pudiéndose adaptar a las necesidades de LogiRAIL por necesidades del proyecto o por incidencias puntuales y urgentes en el servicio.

El proyecto se realizará en instalaciones del adjudicatario, teniendo en cuenta que en el caso de ser necesaria su presencia deberán desplazarse a las oficinas de LogiRAIL en Madrid o de Renfe en Madrid sin coste alguno para LogiRAIL. No obstante, la ubicación del equipo podrá variarse durante la ejecución del contrato para ajustarse a las necesidades del proyecto.

## 08 | FACTURACIÓN

El adjudicatario elaborará un acta con el desglose del servicio prestado en el mes, una vez que sea validado por parte de LogiRAIL, se podrá emitir la factura correspondiente.

Pablo Alarcón Minchillo
Responsable de Innovación, Transformación Digital y Servicios Tecnológicos

# ANEXO Nº 1

## REQUISITOS DE SEGURIDAD EN MATERIA DE CONFIDENCIALIDAD DE LA INFORMACIÓN Y PRIVACIDAD

## ANEXO 1 - 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 según la metodología conforme al artículo 14 del ENS conforme al ENS, que en particular LogiRAIL identifica como MAGERIT (herramienta PILAR), salvo que, por indicación contraria y expresa, del Área de Ciberseguridad y Privacidad del Grupo Renfe 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, conforme a lo indicado en el punto 6.9 y 7.3 de la PARTE II del Anexo I de las Especificaciones Técnicas.
- La solución ofertada está certificada 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 certificada, 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 la solución ofertada por el licitador no esté certificada en el ENS, pero este certificada 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 a lo indicado en el punto 9.1 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 del Grupo Renfe, 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, 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 en su apartado 5 del ENS.
     - 1.4.1. Responsable del Proyecto.
     - 1.4.2. Responsable de Seguridad.
   - 1.5. En caso de que el alcance del contrato requiera de desarrollo de mantenimiento de software o bien de desarrollos de software, el adjudicatario deberá disponer y seguir una metodología de Desarrollo Seguro. Los desarrollos y las pruebas realizadas deberán estar alineados con dicha metodología.
   - 1.6. 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.
   - 1.7. 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.
   - 1.8. 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. El adjudicatario deberá alinearse con el proceso interno de Gestión de Incidentes de Seguridad, siguiendo las directrices de notificación recogidas en la IT-02.NS-11.PE.GRS.TIC *Actuación proveedor ciberincidente con afectación a Renfe.*
   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 pueda informar 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.
   3.5. Adicionalmente el adjudicatario dispondrá de herramientas de análisis de vulnerabilidades, en base a las comunicaciones de amenazas que se reciban por parte del CERT del Grupo RENFE, CCN-CERT, así como de otros canales procedentes de organismos de difusión de amenazas.

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 según la metodología conforme al artículo 14 del ENS, que en particular LogiRAIL identifica como MAGERIT (herramienta Pilar), salvo que, por indicación contraria y expresa, del Área de Ciberseguridad y Privacidad del Grupo Renfe 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 realizará 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. En relación con la **seguridad de las aplicaciones**, el adjudicatario deberá cumplir con los siguientes requisitos de seguridad en los desarrollos, los cuales son de aplicación sea cual sea el lenguaje utilizado, o el sistema final, lo que incluye los desarrollos para las tabletas y móviles inteligentes o cualquier otro entorno o sistema anfitrión del desarrollo:
   - 5.1. El adjudicatario debe incluir controles y medidas de seguridad en los diferentes análisis funcionales, de manera que los desarrollos respeten el principio de "security and privacy by design".
   - 5.2. El adjudicatario debe contar con una metodología y prácticas en el desarrollo seguro, conforme a buenas prácticas y estándares reconocidos.
     Para las tareas de mantenimiento, el adjudicatario deberá igualmente disponer y seguir una metodología de Desarrollo Seguro. Los desarrollos y las pruebas realizadas deberán estar alineados con dicha metodología.
     - 5.2.1. Si, como consecuencia de las labores de soporte y mantenimiento, fuera imprescindible acceder a datos de entornos de Producción, estos solo se podrán utilizar con la única finalidad de dar solución a la incidencia y durante el mínimo tiempo necesario para su resolución.
     - 5.2.2. Si, debido a labores de mantenimiento evolutivo, se modificasen o adaptasen aplicativos, deberán ser realizadas atendiendo a los principios de privacidad y seguridad desde el diseño y por defecto. En caso de duda y a modo de referencia, el adjudicatario puede consultar las guías publicadas por la Agencia Española de Protección de Datos sobre ambas materias.
   - 5.3. En base al análisis de riesgos realizado, el adjudicatario debe incluir controles y medidas de seguridad y privacidad adecuadas al nivel de riesgo aprobado.
   - 5.4. El adjudicatario, expondrá las metodologías que se plantea aplicar, en qué puntos del desarrollo y por qué se consideran idóneas estas opciones para un desarrollo de esta naturaleza.
   - 5.5. El adjudicatario debe contar, y detallar, con una práctica adecuada para integrar el desarrollo seguro en las herramientas de elaboración de código.
   - 5.6. El adjudicatario debe exponer cómo abordará el análisis del código fuente de la aplicación en busca de condiciones de diseño y/o desarrollo que pudieran conllevar vulnerabilidades o superficies atacables.
   - 5.7. El adjudicatario, expondrá las metodologías y herramientas/soluciones que plantea utilizar, con qué frecuencia, en qué momentos y por qué se consideran idóneas estas opciones para una plataforma de este tipo.
   - 5.8. El adjudicatario deberá establecer procesos y mecanismos específicos de aceptación del código, preservando las trazas necesarias para posibilitar a LogiRAIL auditorías del código generado.
   - 5.9. Los resultados de las pruebas estáticas y dinámicas (caja negra y blanca) del código que pase a producción deben ser notificados a la Gerencia de Área de Ciberseguridad y Privacidad de LogiRAIL.
   - 5.10. El adjudicatario debe dotar a la plataforma de protección frente ataques de denegación de servicio a nivel de red y de aplicación.
   - 5.11. El adjudicatario describirá los elementos de seguridad que implementará, operará y administrará para la protección de la aplicación. El adjudicatario, además, debe describir la solución propuesta y por qué considera adecuada la misma para la naturaleza de esta plataforma.
   - 5.12. El adjudicatario, en el caso que sea necesario, para desarrollar las tareas de desarrollo en remoto, deberá tener el tráfico segregado y seguro en su compañía. Además, si dichas tareas de desarrollo se realizan por parte del adjudicatario con sus propios equipos, éstos deberán estar bastionados, disponiendo de antivirus (preferiblemente del tipo EDR) y el sistema operativo actualizado con las últimas revisiones de seguridad.
   - 5.13. El adjudicatario deberá proporcionar un registro formal y estructurado (SBOM) que detalle tanto los componentes del software como su relación con la cadena de suministro. Este registro deberá incluir al menos los siguientes campos:
     - Nombre del proveedor: Individuo u organización que crea o fabrica el componente software.

- Nombre del componente: Nombre asignado al software según lo definido por el proveedor o fabricante original.
- Versión del componente: Número de versión especificado por el proveedor o fabricante.
- Otros identificadores únicos: Identificadores adicionales además del nombre y la versión del componente.
- Relación de dependencia: Relación entre los componentes software utilizados dentro del software objeto de la licitación y sus componentes ascendentes.
- Autor de datos SBOM: Individuo o grupo que crea los datos de SBOM.
- Timestamp: Registro de la fecha y hora del ensamblaje de datos SBOM.

6. 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:
   6.1. Deberán disponer de procesos documentados, incluyendo criterios y evaluación, para garantizar que el software y las aplicaciones utilizadas como soporte de las actividades empresariales de LogiRAIL estén debidamente autorizados, adquiridos o creados.
   6.2. Deberá disponer de documentación formal detallando las medidas necesarias para proteger los sistemas de Información frente a los actos maliciosos o malintencionados.
   6.3. Siempre que sea de aplicación conforme al objeto del proyecto, deberá existir documentación formal detallando las medidas necesarias para la configuración segura de los dispositivos de red, aplicaciones y desarrollos. Se deben evitar entre otras malas prácticas las configuraciones "de caja", las credenciales por defecto, los permisos no ajustados a las necesidades, el uso de credenciales no unipersonales, entre otras.
   6.4. 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.
   6.5. 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.
   6.6. El adjudicatario debe colaborar en la medida de lo posible con la Gerencia de Área de Ciberseguridad y Privacidad para realizar un escaneo de vulnerabilidades de la solución ofertada.
   6.7. 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, sino también aquellos procesos internos del adjudicatario que incorporan copia de información de LogiRAIL como parte de sus datos. Deberán implantarse procesos o procedimientos formales y documentados para garantizar la realización de copias de seguridad y para la recuperación de la información.
   6.8. 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.
   6.9. Se implementarán controles de seguridad a nivel de aplicación para asegurar que la información intercambiada con las diferentes interfaces de la plataforma está convenientemente protegida.
   6.10. 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 o bien en los que se trate información 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.

6.11. Las autenticaciones se realizarán contra del Directorio Activo de LogiRAIL. Las autorizaciones deberán ser realizadas acorde al principio de mínimo privilegio (incluida la figura del Administrador del Sistema). Del mismo modo, deberá cumplir con la política de seguridad de contraseñas de LogiRAIL.

6.12. El adjudicatario deberá asegurar que la solución genera unos logs, que recojan al menos los siguientes campos:

a. Actividad
b. Acceso
c. IP origen
d. IP destino
e. Usuario

7. 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:

7.1. 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.

7.2. 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. Además, no debe ser próxima la fecha de finalización del soporte el software instalado en dichos equipos.

7.3. 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.

7.4. 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.

7.5. 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:

7.5.1. 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.

7.5.2. 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 (7.5.1) de todos los equipos bajo alcance del proyecto.

8. En relación con la Seguridad relativa a terceras partes y a recursos humanos, el adjudicatario deberá cumplir los siguientes requisitos:
   8.1. 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.
   8.2. 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.
   8.3. 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 de LogiRAIL.
   8.4. Todos los usuarios del adjudicatario que vayan a acceder a las redes o sistemas de información de 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.

9. Relativo a los aspectos de Cumplimiento Normativo de Seguridad:
   9.1. La solución ofertada por el licitador debe estar certificada 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 certificada 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 la solución no esté certificada en el ENS, pero este certificada 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.
   9.2. Debe contemplarse el compromiso de devolución/destrucción (a elección de LogiRAIL) de la información confidencial recabada durante la ejecución del servicio.
      9.2.1. Si por la naturaleza del proyecto, LogiRAIL requiere del borrado y destrucción de cualquier soporte de información 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.
      9.2.2. 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.