ESPECIFICACIONES TÉCNICAS PARA LA CONTRATACIÓN DE LICENCIAS Y SUSCRIPCIONES DE LA PLATAFORMA DE APIFICACIÓN E INTEGRACIÓN DE MULESOFT

ÍNDICE

1. ANTECEDENTES

La Entidad Pública Empresarial RENFE-Operadora (en adelante RENFE) cuenta actualmente con una implantación de MuleSoft, que incluye toda la funcionalidad de la plataforma y la línea base para el despliegue de las APIs necesarias para los proyectos que actualmente se encuentran desplegados.

En 2023 se realizó una adquisición de suscripciones para dar cobertura a las necesidades identificadas, tras esa implantación inicial, el objetivo de la licitación es la adquisición de las licencias necesarias y la contratación de una capacidad variable en modelo suscripción.

2. ALCANCE: SUMINISTRO DE SUSCRIPCIONES DE MULESOFT

El adjudicatario será responsable de suministrar las suscripciones de los productos de MuleSoft que Renfe solicite a lo largo del contrato a través del procedimiento que ambas partes acuerden al inicio del contrato.

Renfe se compromete a una adquisición inicial de licencias que será la línea base que se mantenga a lo largo de todo el contrato y se adjudicará una capacidad variable sin compromiso de consumo en modos suscripción. Los licitadores deben ofertar un precio unitario de compra y dichos precios serán fijos durante toda la vigencia del contrato.

En el cuadro siguiente se indica el número estimado de licencias y suscripciones estimadas para toda la vigencia del contrato:

- Previsión inicial: capacidad necesaria al inicio del contrato. Este dato se ha calculado con la demanda existente y proporciona el volumen de capacidad necesario al inicio del proyecto.

MULESOFT BLOQUE DE LICENCIAS

Producto	Ud
MuleSoft - Anypoint Platform Base Subscription - Platinum Edition	1
MuleSoft - Load Balancer - Platinum Edition	2
MuleSoft - Anypoint API Manager Production - Platinum Edition	100
MuleSoft - Anypoint API Manager Pre-Production - Platinum Edition	120
MuleSoft - Additional vCore Production - Platinum Edition	6
MuleSoft - Additional vCore Pre-Production - Platinum Edition	6
MuleSoft - Anypoint Flex Gateway (100M API Calls) - Platinum Edition	10
MuleSoft - Anypoint VPC/VPN - Platinum Edition	2
MuleSoft - Additional Core Production - Platinum Edition (No Flex)	1
MuleSoft - Additional Core Pre-Production - Platinum Edition (No Flex)	1

- Variable: capacidad adicional que se ha identificado en base a los proyectos que se van a abordar a lo largo de los próximos 5 años y que se solicitará de forma progresiva durante la vigencia del contrato.

Producto	Ud
MuleSoft - Anypoint API Manager Production - Platinum Edition	30
MuleSoft - Anypoint API Manager Pre-Production - Platinum Edition	30
MuleSoft - Additional Core Production - Platinum Edition (No Flex)	1
MuleSoft - Additional Core Pre-Production - Platinum Edition (No Flex)	1
MuleSoft - Additional vCore Production - Platinum Edition	1
MuleSoft - Additional vCore Production - Pre- Production - Platinum Edition	1
MuleSoft - Anypoint Flex Gateway (100M API Calls) - Platinum Edition	30

Renfe podrá decidir de forma mensual qué capacidad variable de computación (cores/APIs flex) se activa, siempre y cuando no se supere el importe máximo adjudicado.

Las suscripciones se contabilizarán por meses enteros desde el mismo día de su activación en la suscripción de Renfe.

La facturación de cada capacidad tendrá en cuenta los meses transcurridos desde el día en el que ésta esté activada hasta el último día del contrato siendo el importe mes, la doceava parte del importe ofertado por el licitador como importe anual de la suscripción.

De forma mensual, el proveedor deberá emitir un informe en el que se detallen las activaciones de nuevos cores en la plataforma Mulesoft para soportar nuevos casos de uso (cores en uso). Estas activaciones se pagarán desde el mes en que son activados hasta el final de contrato. Una vez validado el informe, se aprobará la facturación de la capacidad activa a mes vencido.

Por tanto, los datos de volumen de la capacidad no establecen una fecha de inicio y la facturación se realizará en base al momento de activación a lo largo del contrato y precio unitario aportado por el adjudicatario.

No existirá compromiso por parte de Renfe de emitir peticiones ni por todos los conceptos, ni por cantidades determinadas, de forma que sólo se abonarán la capacidad que sea efectivamente activada durante la vida del contrato.

3. NIVELES DE SERVICIO

- **Horario de atención del servicio de soporte:** de 8:00 am y 5:00 pm de lunes a viernes, excepto los días festivos locales.
- **Error:** se refiere a cualquier error de nivel de gravedad S1, error de nivel de gravedad S2, error de nivel de gravedad S3 o error de nivel de gravedad S4, cada uno según se define en la Tabla de definición de gravedad de error a continuación.

Nivel de severidad	Descripción
S1	**Interrupción del sistema** Interrupción del sistema de producción Esto incluye los siguientes escenarios: • El producto en el entorno de producción no se puede utilizar y está afectando gravemente a otras funciones comerciales críticas, y no hay una solución alternativa disponible. • La interrupción en la nube de MuleSoft está provocando interrupciones en el servicio de las versiones de producción de las API expuestas en la plataforma.
S2	**Funcionalidad clave deteriorada; Sin solución** El problema informado afecta a la funcionalidad clave y/o causa una degradación del rendimiento, y no hay una solución disponible. Otras características del producto siguen siendo funcionales.
S3	**Impacto moderado con solución alternativa** El problema tiene un impacto moderado o menor en el uso y el producto sigue funcionando. Esta categoría puede incluir solicitudes de administración de cambios/aprovisionamiento, solicitudes de mejora, preguntas prácticas comunes y cualquier problema de producto con una solución alternativa viable.
S4	**Impacto menor** Incluye problemas menores, estéticos o relacionados con la documentación, y solicitudes de mejora que no son sensibles al

	tiempo. No hay impacto en las características existentes del producto.

Durante el Plazo de Suscripción, MuleSoft proporcionará a RENFE-Operadora Niveles de Servicio que consisten en lo siguiente: (i) soporte en línea, por correo electrónico o por teléfono con respecto al uso y la implementación del Producto de acuerdo con la tabla a continuación; (ii) Versiones principales y secundarias de los mismos Productos licenciados por RENFE-Operadora durante la suscripción ("Mantenimiento") y soporte con respecto a Errores como se establece a continuación. Para acceder al soporte, RENFE-Operadora debe poder acceder al Portal de Soporte ubicado en: https://www.mulesoft.com/support-login.

Número de contactos e incidencias anuales

Núcleos/VCore	Incidentes
1-7	Ilimitado
8-63	Ilimitado
64-255	Ilimitado
256-511	Ilimitado
512-1,023	Ilimitado
1,024+	Ilimitado

Horario de soporte de MuleSoft

Apoyo técnico	Platino
Horas de soporte	S1 - 24x7x365 S2-S4 - 8x5 Horario comercial

Tiempo de respuesta de error

	Platino
productos	S1 - 2 horas S2 - 4 horas laborales S3-S4 - 8 horas laborales

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

ADQUISICIÓN DE LICENCIAS Y SUSCRIPCIONES DE LA PLATAFORMA DE APIFICACIÓN E INTEGRACIÓN DE MULESOFT

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 (anexos del PCP regulador):

- 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 indiciado en el punto 1.4 de la PARTE II del presente anexo:
    - Responsable del Proyecto
    - Responsable de Seguridad
- El licitador asegurará que, en caso de resultar adjudicatario mantendrá y pondrá a disposición del Grupo Renfe, un inventario actualizado de la totalidad de equipos de la presente licitación, conforme a lo indicado en el punto 6.3 de la PARTE II del presente anexo.
- 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 a lo indicado en el punto 8.1 de la PARTE II del presente anexo.

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 del Grupo RENFE o bien tengan acceso a la red o sistemas del Grupo RENFE, deberán adoptar las mismas políticas y estándares sobre seguridad de la información que mantiene con el Grupo RENFE.
   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 el Grupo Renfe, 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 Renfe.
   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 del Grupo Renfe 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 del Grupo Renfe que el mismo le autorice o esté recogida dentro del alcance del servicio.

2.7. Toda información que sea entregada por el Grupo Renfe al adjudicatario para que salga de las instalaciones del Grupo, 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, el Grupo RENFE 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 del Grupo Renfe.

3.4. Deberá ofrecer mecanismos para que:

3.4.1. El Grupo Renfe pueda informar al adjudicatario sobre eventos de seguridad que ha detectado.

3.4.2. El adjudicatario pueda informar al Grupo Renfe sobre eventos de seguridad que ha detectado.

3.4.3. El Grupo Renfe 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 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:

4.1. 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”.

4.2. 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.

4.2.1. 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.

4.2.2. 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.

4.3. El adjudicatario debe contar, y detallar, con una práctica adecuada para integrar el desarrollo seguro en las herramientas de elaboración de código.

4.4. 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 Renfe.

4.5. El adjudicatario debe dotar a la plataforma de protección frente ataques de denegación de servicio a nivel de red y de aplicación.

4.6. 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. 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. 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 Grupo RENFE estén debidamente autorizados, adquiridos o creados.

5.2. Deberá disponer de documentación formal detallando las medidas necesarias para proteger los sistemas de Información frente a los actos maliciosos o malintencionados.

5.3. 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.

5.4. 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.

5.5. Tanto el software como las aplicaciones utilizadas como soporte de las actividades empresariales de Renfe deben estar configurados para solucionar factores de vulnerabilidad y amenazas conocidas y nuevas en un plazo aceptable.

5.6. 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 del Grupo RENFE 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.

5.7. A la hora de realizar una copia de seguridad (backup) de los equipos que contengan datos del Grupo RENFE, 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 del Grupo RENFE, el adjudicatario deberá tomar las medidas necesarias en virtud de la clasificación de seguridad de la información.

5.8. 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 del Grupo de Renfe o bien en los que se trate información del Grupo Renfe, deberán estar correctamente protegidos y configurados para que no representen una amenaza a la confidencialidad, disponibilidad e integridad de la información de Renfe. Entre otras cuestiones de configuración de los mismos, NO deben generar tráficos no autorizados desde las redes del Grupo Renfe hacia recursos externos o internos de la red del adjudicatario.

5.9. 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

5.10. El adjudicatario, en caso de alojar información del Grupo Renfe en Bases de Datos ajenas al mismo; deberá seguir las recomendaciones de seguridad establecidas en la Guía “CCN-CERT BP/24 Recomendaciones de seguridad en bases de datos”.

5.10.1. Si la tecnología de las Bases de Datos es DB2, deberá seguir adicionalmente las recomendaciones de seguridad establecidas en la Guía “CCN-CERT BP/23 Recomendaciones de seguridad para bases de datos DB2”.

5.10.2. Si la tecnología de las Bases de Datos es Oracle, deberá seguir adicionalmente las recomendaciones de seguridad establecidas en la Guía “CCN-CERT BP/22 Recomendaciones de seguridad para Oracle Database 19C”.

5.11. En el caso de que la solución requiera el envío de correos electrónicos, se deberán llevar a cabo conforme a las medidas de seguridad indicadas propuestas por Grupo Renfe. Todos los correos electrónicos enviados y recibidos deben configurarse para que empleen los sistemas de Grupo Renfe que dispone para ello, y asegurar la autenticidad del dominio de Renfe.

6. En relación con los **equipos** que vayan a conectarse a las redes o sistemas de información del Grupo Renfe, o vayan a tratar información del Grupo Renfe, 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 del Grupo Renfe 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 Renfe, en los que se vaya a tratar información del Grupo Renfe o se vayan a conectar a la red o sistemas de información del Grupo Renfe, 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 Renfe.

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 Grupo RENFE.

7.4. Todos los usuarios del adjudicatario que vayan a acceder a las redes o sistemas de información del Grupo Renfe, o vayan a acceder a información de Renfe, deben estar dados de alta en la gestión de identidad del Grupo Renfe, 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 de 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 del Grupo Renfe) de la información confidencial recabada durante la ejecución del servicio.

8.2.1. Si por la naturaleza del proyecto, Grupo Renfe 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.

8.2.2. Asimismo, para cada borrado/destrucción realizado, el adjudicatario deberá entregar a Grupo Renfe 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.

Madrid, 1 de Marzo de 2024

Firmado por SEGADE BLANCO SONIA - ***4034** el día 01/03/2024 con un certificado

Sonia Segade Blanco