# ANEXO I

# ESPECIFICACIONES TÉCNICAS PARA EL SUMINISTRO E INSTALACIÓN DE MÓDULOS DE MEMORIA EN EQUIPOS HPE SINERGY

# ESPECIFICACIONES TÉCNICAS PARA EL SUMINISTRO E INSTALACIÓN DE MÓDULOS DE MEMORIA EN EQUIPOS HPE SINERGY

## 1.- OBJETO Y ALCANCE

El objeto de este contrato es la adquisición de memoria para equipos HPE Synergy y su instalación con el fin de optimizar su rendimiento. Actualmente disponemos de 4 equipos HPE Synergy 480 Gen10 Plus.

Se requiere el suministro de **40 módulos de memoria HPE 64Gb DDR4 Dual Rank 3200MTs con part number P06035-B21.**

Han de ser exactamente estos módulos y con ese part number, para mantener homogeneidad y compatibilidad completa sobre el equipamiento de Blades Synergy que están actualmente en garantía.

Los módulos deberán ser nuevos, no admitiéndose equipamiento usado ni procedente de programas de demostración.

Además, el licitador deberá presentar una acreditación firmada que incluya la certificación del fabricante de los servidores actuales en el que se exponga que, tanto el suministro como la instalación que se va a realizar mantenga en su totalidad la garantía y los servicios de soporte y mantenimiento en vigor para los equipos.

## 2.-PLAZO DE SUMINISTRO E INSTALACIÓN.

El suministro del equipamiento, instalación y configuración deberá realizarse en un plazo máximo de **6 semanas**.

Los componentes deben ser instalados en los equipos con plenas garantías de funcionamiento y causando la menor disrupción posible a los servicios que presta el entorno de virtualización en términos globales. Será necesario realizar la ampliación de memoria de forma escalonada para que siempre se disponga del número adecuado de equipos prestando servicio en cada entorno.

Al concluir la instalación se comprobará que los servidores funcionan correctamente, que la nueva memoria es reconocida por el hardware y que su funcionamiento es el adecuado.

## 3.-GARANTÍA

### 3.1.- Duración de la Garantía

El período de garantía de los suministros contratados será de **3 años**.

Esta garantía incluirá los servicios de atención y reparación de averías derivados del mal funcionamiento hardware, software o configuración de los equipos suministrados por el licitador que resulte adjudicatario y que se encuentran descritos en la presente Especificación Técnica.

## 3.2 Resolución de incidencias durante el periodo de la garantía

### Descripción

Aglutina todas las actividades encaminadas a la resolución de una avería, incidente o anomalía en el comportamiento de los equipos o en los servicios ofrecidos y soportados por los mismos.
El ámbito de aplicación de este servicio incluye tanto el hardware como el software y las configuraciones de los equipos incluidos en el alcance objeto de la presente licitación.
El adjudicatario dispondrá de un servicio de monitorización remoto para una rápida respuesta en el diagnóstico y resolución de incidencias.
Los requerimientos mínimos de la garantía son:

- Resolución Incidentes y Problemas:
  - Diagnóstico, y resolución de cualquier incidencia o anomalía hardware, software, o de error de configuración de cualquiera de los elementos o servicios dentro del perímetro del alcance.
  - El diagnóstico y resolución de incidencias se realizará in-situ, incluyendo en el servicio la mano de obra, desplazamiento, reposición e instalación de componentes o equipos. Todo ello sin coste adicional para Renfe-Operadora.
  - Cuando por la magnitud de la incidencia, o cualquier otra causa, las reparaciones o resolución del incidente no pudiera realizarse de acuerdo con los estándares y procedimientos marcados en los puntos anteriores, el adjudicatario activará la puesta en marcha de soluciones alternativas provisionales (Workaround) encaminadas a restablecer el servicio en los plazos acordados.

- Gestión del Software:
  - El adjudicatario mantendrá informado a RENFE-Operadora de forma periódica, sobre la aparición de nuevas versiones/releases/parches de Software, de las nuevas características de estas, emitiendo además una recomendación sobre la conveniencia e idoneidad de su instalación en la infraestructura de RENFE-Operadora, poniendo a disposición de RENFE-Operadora todas las actualizaciones Software que el fabricante vaya liberando.
  - El adjudicatario instalará in-situ aquellas actualizaciones Software que sean necesarias para la resolución de una avería.

### Definiciones:

- Incidencias críticas: Son aquellas con un elevado impacto en las operaciones de la compañía, y que en general cumplen uno o varios de los siguientes criterios:
- El servicio que presta el equipamiento instalado, lo hace con deficiencias e incide en el buen funcionamiento de las aplicaciones críticas de RENFE, viéndose afectadas en su totalidad o en alguna de sus funcionalidades esenciales.
- Unos volúmenes importantes de usuarios se ven gravemente afectados (Toda la organización, un Centro o una parte importante del mismo).
- Unos volúmenes importantes de servicios se ven gravemente afectados (aun no siendo servicios críticos).

- Incidencias graves: Son aquellos Incidentes en los que aun estando disponibles los servicios, estos se prestan con alguna deficiencia importante. También se consideran incidentes graves aquellos en el que se vean afectada la disponibilidad o funcionalidades de los servicios, y cuyo impacto sin llegar a afectar a un volumen muy importante de usuarios, sí impacta en un grupo de ellos (más de un usuario).
- Incidencias leves: Son aquellas que, prestando el servicio con normalidad, hay algún elemento o elementos que no funcionan adecuadamente.
- Tiempo de Intervención (TI): Tiempo transcurrido desde que se abre un incidente al adjudicatario hasta que el técnico asignado se pone en contacto con RENFE.
- Tiempo de Resolución (TR): Tiempo transcurrido entre la apertura de un incidente y su resolución.
- Ventana de acceso a la garantía: Calendario y horario en que el adjudicatario debe proveer las coberturas descritas en las condiciones marcadas en estas Especificaciones Técnicas.

**Ventana de acceso a la garantía:** 24 horas, 365 días al año (24X7X365)

**Asistencia y cobertura durante la garantía:**
El adjudicatario pondrá a disposición de Renfe Operadora como mínimo:

- Servicio telefónico 24X7 en español.
- Sistema Centralizado de apertura, seguimiento, consultas, escalado y cierre de las incidencias.
- Tratamiento de Incidentes y resolución in-situ y en horario 24X7.

A continuación, se describe en detalle el tipo de cobertura asociado a la garantía:

| Tipo de Incidencia | Ventana | Tiempo De Intervención | Tiempo de Resolución |
|---|---|---|---|
| Crítica | 24x7 | 2 horas | 4 horas |
| Grave | 24x7 | 4 horas | 8 horas |
| Leve | 24x7 | 24 horas | NBD (Next Business Day) |

# 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 asegurará que, en caso de resultar adjudicatario mantendrá y pondrá a disposición del Grupo Renfe, un inventario actualizado de la totalidad de equipos objeto de la presente licitación, conforme a lo indicado en el punto 5.9 y 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 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 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 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.
   1.7. 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 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. 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. El Grupo Renfe pueda informar al adjudicatario sobre eventos de seguridad que ha detectado.

3.4.2. El adjudicatario informe 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.

4. 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:

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

4.2. 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.

4.3. 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.

4.4. 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 del Grupo de 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.

4.5. 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 Renfe). Deberán implantarse procesos o procedimientos formales y documentados para garantizar la realización de copias de seguridad y para la recuperación de la Información.

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

5. En relación con los **equipos** objeto de la licitación, el adjudicatario deberá:

5.1. El adjudicatario deberá proporcionar la documentación detallada sobre los protocolos, puertos necesarios, requisitos de alimentación, frecuencias y pruebas de funcionamiento de cada equipo.

5.2. Deberá existir documentación formal detallando las medidas necesarias para la configuración segura de los dispositivos de red y los equipos. 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.

5.3. El adjudicatario deberá documentar la configuración de los elementos de información y observar específicamente cualquier medida de seguridad asociada con el sistema (incluidos los dispositivos de cifrado y la protección por contraseña, así como los protocolos o versiones de protocolos a utilizar).

5.4. Los equipos deberán estar provistos 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.

5.5. El adjudicatario deberá mantener los equipos actualizados a la última versión de software y firmware 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.

5.5.1. En caso de que el adjudicatario sea conocedor de que uno de los equipos se encuentre en obsolescencia tecnológica, es decir, cuando no puedan instalarse nuevos parches de seguridad o no estén disponibles a pesar de existir vulnerabilidades que le afecten, ya sea por causa del fabricante, sistema

operativo u otra causa relacionada con el equipo, deberá notificárselo al Grupo Renfe.

5.6. Deberá colaborar en la elaboración por parte del Grupo Renfe, y cuando este lo requiera, de una política de bastionado de los equipos una vez sea el adjudicatario del proyecto.

5.6.1. El adjudicatario eliminará o inhabilitará en todos los equipos, el software que no sea necesario para la operación y el mantenimiento de dicho equipo antes de ponerlo a disposición del Grupo Renfe.

5.6.2. Todos los nombres de usuario, contraseñas u otros códigos de seguridad configurados por el adjudicatario o por defecto, se cambiarán o eliminarán en el momento de la entrega a Renfe Viajeros.

5.7. 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.

5.8. Deberá colaborar con el Grupo Renfe en lo que este le requiera para la remediación de infecciones que se produzcan en los equipos y responsabilizándose de la efectiva remediación de dichas infecciones. 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.

5.9. Deberá mantener y poner a disposición del Grupo Renfe de un inventario actualizado de la totalidad de equipos objeto de la presente licitación. 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.

5.10. El adjudicatario deberá proteger la información de los equipos eléctricos y electrónicos frente a amenazas de tipo TEMPEST, que pueden llevare a la obtención de información por cauces no previstos.

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

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:

h. Dirección IP del equipo.
i. Nombre del equipo (hostname).
j. Dirección MAC del equipo
k. Inventario actualizado del Software instalado en cada equipo.
l. Modelo del equipo.
m. Versión del sistema operativo instalado.
n. 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 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 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 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 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.
d) Fecha destrucción material.