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

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

PARTE I

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

- El licitador asegura que en caso de resultar adjudicatario dispondrá de las siguientes figuras, estando debidamente recogidas y documentadas, y siendo personas distintas; tal y como establece el artículo 13.5 en su apartado 5 del RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) conforme a lo indicado en el punto 1.4 de la PARTE II del Anexo I de las Especificaciones Técnicas:
  - Responsable del Proyecto
  - Responsable de Seguridad
- El licitador asegura que una vez sea adjudicatario realizará un análisis de riesgos conforme al artículo 14 del ENS según la metodología conforme al ENS, que en particular el Grupo Renfe identifica como MAGERIT (herramienta PILAR), salvo que, por indicación contraria y expresa, del Área de Seguridad TIC del Grupo Renfe se especifique lo contrario. Este Análisis de Riesgos (realizado una vez sea adjudicatario del servicio), será compartido con el Área de Seguridad TIC del Grupo Renfe, conforme a lo indicado en el punto 6.1 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 del Grupo Renfe, un inventario actualizado de la totalidad de equipos conforme a lo indicado en el punto 5.3 de la PARTE II del Anexo I de las Especificaciones Técnicas.
- El licitador asegura que los servicios prestados, en caso de resultar adjudicatario, así como los sistemas de información que los sustentan, se prestarán de conformidad a los requisitos de seguridad establecidos en el Esquema Nacional de Seguridad, conforme a lo indicado en el punto 8.1 de la PARTE II del Anexo I de las Especificaciones Técnicas.

PARTE II

1. Relacionados con las **Políticas de Seguridad**, se deberá cumplir con los siguientes requisitos:
   1.1. El adjudicatario, deberá conocer y cumplir las medidas de Seguridad incluidas en la Política de Seguridad de los Sistemas de Información 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.

4.7. 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".*

4.7.1. 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".*

4.7.2. 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. 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:

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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.

5.5. 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:

5.5.1. 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.

5.5.2. 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. En relación con la **seguridad del software** necesario para la prestación del servicio (la herramienta gestión de los datos asociados al contrato o cualquier otra que vaya a suponer soporte del servicio), en adelante aplicaciones, el adjudicatario deberá cumplir con los siguientes requisitos de seguridad:

6.1. El adjudicatario deberá realizar un Análisis de Riesgos de la/s aplicación/es desde el punto de vista de la Seguridad de la Información conforme a lo indicado en el ENS (Esquema Nacional de Seguridad) (la metodología MAGERIT, salvo indicación contraria y expresa, del Departamento de Seguridad de la información del Grupo RENFE), al inicio del proyecto y mantenerlo durante todo el ciclo de vida de este.

6.2. Como resultado del Análisis de Riesgo, el adjudicatario deberá especificar los controles de seguridad que se deberán implementar y además deberá tener en consideración aquellos indicados desde el Grupo RENFE, para disponer de un adecuado nivel de seguridad y acorde a la gestión del riesgo.

6.3. El adjudicatario deberá contar con un proceso formal de Gestión de vulnerabilidades y parcheado de elementos, plataformas e infraestructuras involucrados en la prestación del servicio que garantice la correcta configuración y actualización de los mismos.

6.1. El adjudicatario describirá los elementos de seguridad que implementará, operará y administrará para la protección de las aplicaciones. El adjudicatario, además, debe

describir la solución propuesta y por qué considera adecuada la misma para la naturaleza de esta plataforma.

6.1.1. En particular, el adjudicatario debe dotar a la plataforma de protección frente ataques de denegación de servicio a nivel de red y de aplicación

6.2. Se implementarán controles de seguridad a nivel de aplicación para asegurar que la información intercambiada con las diferentes interfaces de la plataforma o aplicaciones, está convenientemente protegida.

6.2.1. Uso de mecanismos de firmas digitales para la autenticación de los equipos/ servidores que intercambien información.

6.2.2. Uso de mecanismos de cifrado de información en tránsito (comunicaciones), en uso y almacenada que, según el caso, sean de aplicación, considerando cualquier información sensible que pueda ser intercambiada dentro del contexto de la plataforma o aplicaciones.

6.3. Las aplicaciones serán objeto de escaneos de vulnerabilidades, tanto por parte del adjudicatario como por parte de la Gerencia de Ciberseguridad y Privacidad, ya que ésta aplica actualmente un proceso continuo de gestión de vulnerabilidades de su infraestructura IT. Para ello, el adjudicatario deberá habilitar en las políticas de red los correspondientes accesos para los escaneos periódicos y resolver las vulnerabilidades detectadas en los plazos establecidos, de acuerdo a su criticidad.

En caso de que el adjudicatario cuente con informes/reportes de escaneo de vulnerabilidades de las aplicaciones, objeto de la licitación, realizados por un tercero, y una vez que sean analizados por el área de Ciberseguridad y Privacidad, podrán ser aceptados como equivalentes a lo indicado en el párrafo anterior, por parte del Grupo Renfe.

6.4. Las aplicaciones, objeto de la licitación, deben generar unos logs, que recojan al menos los siguientes campos:

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

6.5. En caso de ser requeridos por el área de Ciberseguridad y Privacidad, el adjudicatario deberá poner a su disposición dichos logs, o bien deberá colaborar con dicha área para la integración de los mismos en el SIEM del Grupo Renfe.

6.6. El adjudicatario debe contar con productos de seguridad que deben ser comerciales para las áreas de:

6.6.1. Defensa perimetral y perímetro virtual (FW, etc.).

6.6.2. Protección IDS e IPS.

6.6.3. Solución de Seguridad de filtrado a nivel de aplicación.

6.6.4. Cuando la naturaleza de la solución del adjudicatario incorpore servicios web, el adjudicatario deberá incorporar: Protección de aplicaciones (WAF).

6.6.5. Cuando la naturaleza de la solución del adjudicatario requiera servicios web se requerirán: Proxys de entrada (proxys inversos).

6.6.6. Segundo factor de autenticación (2FA), para aquellos servicios expuestos a Internet que lo requieran.

6.7. El adjudicatario deberá dotar a los servicios de DNS específicos para la aplicación y servicios de, al menos, los siguientes mecanismos:
6.7.1. Protección por reputación
6.7.2. Creación de Sinkhole
6.7.3. Protección de exfiltración mediante paquetes DNS.

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:
e. Nombre y apellidos.
f. DNI.
g. Correo electrónico profesional.
h. Teléfono móvil.

8. Relativo a los aspectos de **Cumplimiento Normativo de Seguridad**:
8.1. El proveedor se asegurará de que los servicios prestados, así como los sistemas de información que los sustentan, se prestan de conformidad a los requisitos de seguridad establecidos en el Esquema Nacional de Seguridad, tal y como aparece recogido en el Documento de Seguridad “Obligaciones de los prestadores de servicios a las entidades públicas” del CCN.
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.