

ANEXO II

REQUISITOS DE SEGURIDAD A IMPLANTAR POR PARTE DEL ADJUDICATARIO EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Obligaciones genéricas del adjudicatario (encargado del tratamiento)

1. El Encargado del tratamiento deberá adoptar las medidas técnicas necesarias para la protección y salvaguarda de los activos como hardware, software y aplicaciones (enumeración a título enunciativo pero no limitativo) que proporcionan el servicio a RENFE, garantizando, en cualquier caso, la confidencialidad, disponibilidad e integridad de los datos de RENFE.
2. Deber de notificación a RENFE:
 - (i) El Encargado del tratamiento de servicio debe de notificar inmediatamente a RENFE en el caso de que se detecte o se tenga una sospecha fundada de que los sistemas y soportes utilizados en la provisión del servicio hayan sido comprometidos o utilizados sin autorización, proporcionando un informe de auditoría del incidente que identifique la causa del incidente e incluya revisiones forenses.
 - (ii) El Encargado del tratamiento de servicio deberá afrontar el coste de las investigaciones forenses necesarias realizadas en la investigación del incidente, proporcionando a RENFE total colaboración en la investigación del mismo.
3. EL Encargado del tratamiento se adhiere al Documento de Seguridad de RENFE -a la versión actualizada del mismo en cada momento y a los documentos que recojan las medidas de seguridad de RENFE, como por ejemplo el las medidas de seguridad indicadas en el Registro de Tratamientos de RENFE- y asume el compromiso de cumplir con las Políticas y procedimientos corporativos de Seguridad de la Información de RENFE, que resulten de aplicación a los proveedores de servicios que tengan acceso a datos personales.

Por tanto, será de aplicación lo establecido en el Documento de Seguridad de RENFE, así como todas las medidas de seguridad incluidas en el citado documento o cualesquiera relacionadas.

4. El Encargado del tratamiento deberá garantizar que el personal está cualificado para realizar los servicios contratados y correctamente formado en materia de seguridad de la información.

Obligaciones sobre seguridad en el uso de la información

1. La información utilizada y generada durante el desempeño del servicio es propiedad de RENFE. El Encargado del tratamiento debe abstenerse de almacenar datos de RENFE, fuera del objeto de los servicios a prestar, sin que dicho grupo, conozca, analice, autorice e indique la forma en que puedan ser almacenados, el método de archivo y transmisión, y establezca las medidas adecuadas para la auditoría de estas actuaciones. En el caso de que en el transcurso del servicio, pudiera acceder a otro tipo de datos no contemplados en el objeto de este contrato, deberá notificar a RENFE y proceder a la eliminación de esta información.
2. El acceso a la información por parte del Encargado del tratamiento en las aplicaciones de RENFE deberá cumplir las medidas de seguridad en materia de identificación y autenticación vigentes en RENFE. De este modo, aquellos usuarios que realicen log-in para acceder a cualquier información de RENFE o información asociada a sus clientes, deberán cumplir con las medidas de seguridad en materia de identificación y autenticación que establece RENFE en su Documento de Seguridad y/o Normativa vigente.
3. El Encargado del tratamiento, se compromete a proporcionar conocimiento y documentación relacionada con el servicio al personal de RENFE para facilitar el mantenimiento y desarrollo del servicio.
4. El Encargado del tratamiento, se compromete a realizar el traspaso de conocimiento mediante la colaboración con el personal de RENFE en la realización de las diferentes actividades y facilitar documentación del trabajo realizado.
5. El Encargado del tratamiento se compromete a mantener la disponibilidad de los servicios según las necesidades de disponibilidad del Negocio de RENFE. De este modo, se compromete a facilitar de forma periódica:
 - (i) Informes e indicadores de disponibilidad de los servicios ofrecidos.
 - (ii) Resultados de las pruebas de los planes de continuidad y recuperación del Encargado del tratamiento sobre los servicios ofrecidos.
 - (iii) Colaboración en la ejecución en los planes de continuidad y recuperación de RENFE en los servicios que se vean afectados.
6. El Encargado del tratamiento debe mantener en todo momento los datos cifrados además de cifrar aquellas comunicaciones que impliquen la transmisión de información propiedad de RENFE o proporcionada por clientes de RENFE.
7. El Encargado del tratamiento debe notificar, de forma previa a llevarlas a cabo, las actualizaciones y tareas de mantenimiento que realice sobre los sistemas, aplicativos, sistemas operativos, bases de datos y elementos de red sobre los que se prestan los servicios contratados con RENFE.
8. Respecto a la administración de usuarios:

(i) El Encargado del tratamiento debe establecer una segregación interna de funciones adecuada, con la finalidad de gestionar el riesgo de acceso por parte de usuarios no autorizados. El Encargado del tratamiento establecerá las medidas suficientes y necesarias para asegurar que los derechos de acceso (roles y perfiles) asignados internamente por el Encargado del tratamiento para prestar el servicio, lo son de acuerdo a las necesidades funcionales del proyecto y a la seguridad para RENFE.

(ii) El Encargado del tratamiento deberá garantizar la trazabilidad de las acciones realizadas en los sistemas/información de RENFE pudiendo identificarse en todo momento la persona concreta que las realizó. No se permitirá la existencia de usuarios genéricos salvo aquellos requeridos por las tecnologías empleadas y en este caso, su uso debe estar inventariado y controlado. Debe ser aprobado y validado por RENFE.

9. Respecto a la gestión de eventos:

(i) El Encargado del tratamiento deberá mantener un registro actualizado de las actividades de cada sistema o aplicación. El registro reflejará las actividades y sucesos acontecidos en la infraestructura tecnológica ofrecida a RENFE.

(ii) El Encargado del tratamiento deberá disponer de un procedimiento de gestión y reporte de eventos (incidencias, vulnerabilidades, incidentes, etc.), para lo cual los eventos deben ser gestionados y transmitidos a RENFE, informando del modo de resolución.

(iii) El Encargado del tratamiento participará, en caso de que fuera necesario, de los Planes de Continuidad de Negocio y Planes de Recuperación de RENFE bajo el ámbito del contrato de prestación de servicios.

(iv) Cualquier acción de mantenimiento y/o soporte realizada sobre los sistemas de RENFE deberá ser registrada por el Encargado del tratamiento, de forma que se mantenga un histórico de acciones.

(v) El Encargado del tratamiento deberá resolver las vulnerabilidades críticas en el plazo de 1 mes desde que hayan sido detectadas y en caso de no ser críticas tendrán un plazo máximo de 4 meses para su resolución.

10. Respecto a la documentación de procesos:

(i) El Encargado del tratamiento deberá formalizar los criterios de configuración en documentación específica que estará a disposición de RENFE y alineada a los requisitos que establezca RENFE.

11. Respecto a la documentación generada:

(i) El Encargado del tratamiento deberá formalizar los criterios de configuración de procesos en documentación específica, la cual estará a disposición de RENFE y alineada a los requisitos que establezca el mismo.

(ii) El Encargado del tratamiento deberá formalizar los criterios de funcionamiento y utilización del servicio prestado para un uso adecuado por parte del personal de RENFE.

12. Respecto a la seguridad de las comunicaciones:

(i) El Encargado del tratamiento deberá garantizar el adecuado aislamiento entre los diferentes clientes.

(ii) Se deberán de reducir al mínimo necesario las conexiones entre ambas empresas.

(iii) El Encargado del tratamiento deberá tomar las medidas preventivas necesarias para evitar que un incidente potencial en cualquier elemento de su red sea propagado a RENFE.

(iv) RENFE podrá realizar auditorías técnicas para validar la adecuada segmentación de dichas redes así como el nivel de seguridad de los elementos conectados.

13. Respecto al personal

(i) El Encargado del tratamiento deberá garantizar que toda persona asignada al servicio tiene las capacidades adecuadas para el desempeño de sus funciones.

(ii) El Encargado del tratamiento deberá disponer de una política de seguridad de la información, alineada con las mejores prácticas de seguridad, en el que se incluyan las obligaciones del personal.

(iii) El Encargado del tratamiento deberá disponer de un plan de concienciación sobre la seguridad en el que se incluya la formación respecto a la política de seguridad, las obligaciones del personal, las buenas prácticas y el uso adecuado de las credenciales.

(iv) Toda persona con acceso a los sistemas/información de RENFE deberá de haber firmado un acuerdo de confidencialidad en el que se especifique su responsabilidad respecto a la seguridad de la información, incluyendo el uso de sus credenciales.

Medidas técnicas específicas para proveedores que se conectan de forma telemática a la red del Responsable del tratamiento

1. Dado el tipo de servicio, en el que desde la infraestructura tecnológica de RENFE se conecta a la del Encargado del tratamiento, se requiere que el mismo facilite:

(i) Relación de medidas de seguridad sobre la información que recoge de los activos tecnológicos de RENFE y el tratamiento/almacenamiento que realiza sobre los mismos. Estas medidas deben estar alineadas a los requerimientos establecidos en los ANEXOS del Documento de Seguridad.

(ii) Certificación y plan de pruebas realizada sobre la infraestructura que ofrece a RENFE.

- (iii) Plan de gestión de vulnerabilidades pruebas de seguridad sobre la infraestructura ofrece a RENFE.
- (iv) Canales de comunicación seguros y documentación asociada a los mismos.