

MEMORIA DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACION DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

Elaborado: 14/05/2020

Página: 1/4

MEMORIA DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

Índice

1.	ANTECEDENTES	3
2.	NECESIDAD DEL SERVICIO	3
3.	DESCRIPCIÓN DEL SERVICIO	3
4.	IMPORTE LÍMITE	3
5.	PLAZO DE EJECUCIÓN	4

MEMORIA DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

1. Antecedentes

Debido a la evolución de la funcionalidad de las torres a Operativa sin Ficha ha sido necesaria la separación técnica de los entornos de Aproximación y Torre en el Sistema Automatizado de Control de Tráfico Aéreo (SACTA).

Esta separación tiene impacto directo sobre el Sistema de Comunicaciones Voz (SCV) de las torres en que se comparten los servicios de Torre y Aproximación, en particular sobre el interfaz que comunica el SCV con SACTA.

En estas torres el SCV es único mientras que, a raíz de este cambio, el SACTA pasa a estar configurado como dos subsistemas: el subsistema de torre encargado de gestionar la sectorización asociada a las operaciones de aeródromos, y el subsistema de APP encargado de la sectorización de los sectores de aproximación.

Los SCV actualmente desplegados en las torres en que se comparten los servicios de Torre y Aproximación no están preparados para recibir comunicaciones de dos subsistemas SACTA simultáneamente. Por tanto es necesario modificar estos SCV de forma que respondan a esta nueva necesidad.

2. Necesidad del Servicio

En base a lo anteriormente expresado se hace necesaria la modificación de los SCV de aquellas dependencias en que la prestación del servicio de control de TWR y APP se realiza utilizando un único sistema SCV (Santiago, Bilbao, Tenerife Norte y Tenerife Sur) para adaptarse a esta nueva arquitectura SACTA.

3. Descripción del Servicio

El objeto del presente expediente es la contratación de los servicios necesarios para la adaptación del SCV a la nueva arquitectura SACTA en las TWRs de Santiago, Bilbao, Tenerife Norte y Tenerife Sur. Estos servicios se desarrollarán conforme a lo especificado en el Pliego de Prescripciones Técnicas de este expediente.

4. Importe límite

El importe límite del presente expediente asciende a CUATROCIENTOS CUARENTA Y CUATRO MIL QUINIENTOS VEINTE EUROS (444.520,00 €), CUATROCIENTOS CUARENTA Y CUATRO MIL QUINIENTOS VEINTE EUROS (444.520,00 €), impuestos no incluidos.

MEMORIA DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

5. Plazo de Ejecución

El plazo de ejecución del servicio es de DIECIOCHO MESES (18 meses), a partir de la fecha que figure en el contrato o en su defecto la de firma del Acta de Inicio del Servicio.

El desarrollo y validación de la solución deberán llevarse a cabo en los cuatro (4) meses siguientes al inicio del expediente.

Realizado por:

SANCHEZ
BARRO
AURORA -
08977040W

Fdo.: Aurora Sánchez Barro

Firmado digitalmente por
SANCHEZ BARRO AURORA -
08977040W
Nombre de reconocimiento (DN):
c=ES,
serialNumber=IDCES-08977040W,
givenName=AURORA,
sn=SANCHEZ BARRO,
cn=SANCHEZ BARRO AURORA -
08977040W
Fecha: 2020.05.14 11:13:52 +02'00'

Aprobado por:

García
Martín,
Manuel

Fdo.: Manuel García Martín

Firmado digitalmente por García
Martín, Manuel
Nombre de reconocimiento (DN):
dc=es, dc=nav, dc=na, dc=lean,
ou=Dirección de Sistemas,
ou=División Comunicaciones,
cn=García Martín, Manuel,
email=mangarcia@enaire.es
Fecha: 2020.05.14 17:23:09 +02'00'

PLIEGO DE PRESCRIPCIONES TÉCNICAS (PPT) DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACION DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

Elaborado: 14/05/2020

Página: 1/15

**PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E
IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN**

Índice

1. ANTECEDENTES	3
2. NECESIDAD DEL SERVICIO.....	3
3. OBJETO DEL SERVICIO.....	3
4. PRESUPUESTO BASE DE LICITACIÓN.....	3
5. PLAZO DE EJECUCIÓN	4
6. LUGAR DE LA PRESTACIÓN DEL SERVICIO	4
7. REQUISITOS DE SEGURIDAD OPERACIONAL.....	4
8. REQUISITOS DE INTEROPERABILIDAD	4
9. SEGURIDAD EN LA INFORMACIÓN.....	4
10. DIRECCIÓN DEL SERVICIO	9
11. RESPONSABILIDADES	9
12. CLÁUSULA DE MEDIOS HUMANOS.....	10
13. CLAUSULA SOBRE MEDIOS MATERIALES.....	12
14. CLÁUSULA DE ESPACIOS	12
15. MEDIOS INFORMÁTICOS	13
16. CLÁUSULA DE HUELGA.....	13
17. ANEXOS.....	14

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

1. Antecedentes

Debido a la evolución de la funcionalidad de las torres a Operativa sin Ficha ha sido necesaria la separación técnica de los entornos de Aproximación y Torre en el Sistema Automatizado de Control de Tráfico Aéreo (SACTA).

Esta separación tiene impacto directo sobre el Sistema de Comunicaciones Voz (SCV) de las torres en que se comparten los servicios de Torre y Aproximación, en particular sobre el interfaz que comunica el SCV con SACTA.

En estas torres el SCV es único mientras que, a raíz de este cambio, el SACTA para estar configurado de dos subsistemas: el subsistema de torre encargado de gestionar la sectorización asociada a las operaciones de aeródromos, y el subsistema de APP encargado de la sectorización de los sectores de aproximación.

Los SCV actualmente desplegados en las torres en que se comparten los servicios de Torre y Aproximación no están preparados para recibir comunicaciones de dos subsistemas SACTA simultáneamente. Por tanto es necesario modificar estos SCV de forma que respondan a esta nueva necesidad.

2. Necesidad del Servicio

En base a lo anteriormente expresado se hace necesaria la modificación de los SCV de aquellas dependencias en que la prestación del servicio de control de TWR y APP se realiza utilizando un único sistema SCV (Santiago, Bilbao, Tenerife Norte y Tenerife Sur) para adaptarse a esta nueva arquitectura SACTA.

3. Objeto del Servicio

El objeto del presente expediente es la contratación de los servicios necesarios para la adaptación del SCV a la nueva arquitectura SACTA en las TWRs de Santiago, Bilbao, Tenerife Norte y Tenerife Sur. Estos servicios se desarrollarán conforme a lo especificado en el A 1 a este documento.

4. Presupuesto Base de Licitación

El presupuesto base de licitación del presente expediente asciende a **CUATROCIENTOS CUARENTA Y CUATRO MIL QUINIENTOS VEINTE EUROS (444.520,00 €)**, **CUATROCIENTOS CUARENTA Y CUATRO MIL QUINIENTOS VEINTE EUROS (444.520,00 €)**, impuestos no incluidos.

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

5. Plazo de Ejecución

El plazo de ejecución del servicio es de DIECIOCHO MESES (18 meses), a partir de la fecha que figure en el contrato o en su defecto la de firma del Acta de Inicio del Servicio.

El desarrollo y validación de la solución deberán llevarse a cabo en los cuatro (4) meses siguientes al inicio del expediente.

6. Lugar de la prestación del Servicio

La prestación de este servicio se realizará en las dependencias de los SSCC de ENAIRe en Madrid y en las TWRs de Santiago, Bilbao, Tenerife Norte y Tenerife Sur. Las labores de desarrollo se llevarán a cabo en las oficinas de adjudicatario.

7. Requisitos de Seguridad Operacional

El contratista deberá ejecutar el expediente conforme a los Requisitos de seguridad operacional, general y/o específicos definidos por la División de Comunicaciones de ENAIRe que se encuentran en el Anexo 3 denominado "Requisitos Seguridad Adaptación Interfaz SCV-SACTA v 1.1".

8. Requisitos de Interoperabilidad

El contratista deberá ejecutar el expediente conforme a los Requisitos de Interoperabilidad (IOP) definidos por la División de Comunicaciones de ENAIRe que se encuentran en el Anexo 4 denominado "Requisitos de Interoperabilidad. División de Comunicaciones", DSIS-13-DTC-045. El anexo está basado en el Reglamento (UE) 2018/1139 que deroga al (CE) n° 552/2004. Se debe dar cumplimiento a este requisito para el sistema SCV incluyendo esta nueva funcionalidad/mejora que es el nuevo interfaz SCV-SACTA.

9. Seguridad en la Información

ENAIRe confirma su firme compromiso con la Seguridad de la Información mediante la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) que permite contar con unos niveles de seguridad adecuados para proteger la información y garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información.

Cualquier versión impresa o en soporte informático, total o parcial de este documento, se considera como copia no controlada y siempre debe ser contrastada con su versión vigente en el Gestor Documental de ENAIRe.

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

En ese sentido, a continuación, se enumeran las condiciones que deberá cumplir el adjudicatario de obras, servicios y suministros externos en materia de Seguridad de la Información y Ciberseguridad.

En los apartados que siguen aplicarán las siguientes definiciones:

- Personal del adjudicatario: Cualquier persona que presta los servicios solicitados en el pliego por cuenta del adjudicatario sea personal propio del adjudicatario o personal de terceros contratados por el adjudicatario.
- Equipos del adjudicatario: Cualquier equipamiento informático propiedad del adjudicatario o de terceros contratados por el adjudicatario empleado en la prestación del servicio solicitado y que requiere conectarse, para la prestación de dichos servicios, a las redes o sistemas de ENAIRe.

A. Condiciones Generales

- El adjudicatario realizará los trabajos y servicios objeto de la contratación de acuerdo, en todo momento, a la legislación vigente, a la regulación aplicable, a las políticas y normativa de seguridad de ENAIRe y, en cualquier caso, de manera alineada con las buenas prácticas, procedimientos y estándares de referencia a nivel nacional e internacional en materia de Gestión de la Seguridad de la Información.
- El adjudicatario quedará expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en este pliego, ni tampoco ceder a otros ni siquiera a efectos de conservación, sin el previo consentimiento por escrito de ENAIRe.
- Se considerará como información confidencial a cualquier información a la que el adjudicatario acceda en virtud de la presente contratación, en especial:
 - a) la información y datos propios de ENAIRe.
 - b) la información de los usuarios y beneficiarios de los productos y servicios objeto del presente pliego.
 - c) la información que con tal carácter se indique.
 - d) cualquier otra información a la que acceda durante la ejecución de los trabajos asociados a la presente contratación, incluyendo la documentación.
- La duración de las obligaciones de confidencialidad asociadas a la presente contratación será indefinida mientras la misma ostente tal carácter, manteniéndose en vigor con posterioridad a la finalización, por cualquier causa, de la relación entre el adjudicatario y ENAIRe.
- El adjudicatario tratará la información proporcionada por ENAIRe o cualquier otra información relativa a ENAIRe a la que, en virtud de los trabajos objeto del presente pliego, tenga acceso con el cuidado debido y, en cualquier caso, de acuerdo a las políticas de clasificación y tratamiento de la información vigentes en ENAIRe.

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

- El adjudicatario informará a su personal, colaboradores y subcontratistas de las obligaciones establecidas en relación con el tratamiento de la información de ENAIRE, la confidencialidad de la información, obligaciones relativas al tratamiento automatizado de datos de carácter personal y normativa de seguridad. El adjudicatario deberá poner todos los medios a su alcance para que su personal y colaboradores cumplan tales obligaciones.
- El personal del adjudicatario que acceda, de forma fortuita o accidental, a información de ENAIRE que no esté relacionada con el objeto del presente pliego, adquirirá la obligación de guardar estricta confidencialidad sobre la misma e informar puntualmente a ENAIRE del hecho acontecido. El adjudicatario informará fehacientemente a su personal sobre esta obligación.
- Asimismo, una vez finalice el contrato, el adjudicatario se comprometerá a la destrucción segura y completa de toda la información alojada en sus propios medios o instalaciones relativa a ENAIRE y sus sistemas que haya sido recabada durante la ejecución del contrato y/o proporcionada por ENAIRE en relación al mismo, salvo aquella que por ley le sea exigible preservar y de la que notificará puntualmente a ENAIRE. El adjudicatario deberá hacer extensivo este compromiso a todos los recursos asignados al contrato.
- El adjudicatario estará obligado a comunicar puntualmente a ENAIRE, de acuerdo al procedimiento que se establezca, cualquier violación o incumplimiento de las condiciones de seguridad establecidas en el presente clausulado. En caso de incumplimiento, el adjudicatario presentará puntualmente un plan de remediación a ENAIRE que, en caso de ser aprobado por ENAIRE, deberá ser implementado sin coste adicional para ENAIRE.

B. Personal del Adjudicatario

- El adjudicatario se asegurará de que todo el personal del adjudicatario (incluyendo el personal de terceros que preste servicios para el adjudicatario) que tenga acceso a información de ENAIRE haya firmado un acuerdo de confidencialidad antes de acceder a cualquier información de ENAIRE.
- El adjudicatario se asegurará de que el personal del adjudicatario que participe en las tareas asociadas a la contratación esté adecuadamente formado en Seguridad de la Información (tratamiento de la información, gestión de incidentes de seguridad, etc.) y sobre las condiciones particulares de su desempeño para ENAIRE (políticas de seguridad, condiciones de uso de sistemas, etc.).
- Cuando las condiciones de seguridad del objeto de la contratación así lo demanden, el adjudicatario se asegurará de que el personal que participe en las tareas relacionadas con los productos clasificados disponga de las necesarias certificaciones de seguridad.
- El adjudicatario comunicará de forma inmediata a ENAIRE los cambios en el personal asignado al contrato objeto del pliego con el fin de tramitar las bajas en los accesos a instalaciones y sistemas de la forma más ágil posible.

C. Acceso a Entornos y Sistemas de ENAIRE

Cualquier versión impresa o en soporte informático, total o parcial de este documento, se considera como copia no controlada y siempre debe ser contrastada con su versión vigente en el Gestor Documental de ENAIRE.

**PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E
IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN**

No aplica.

D. Acceso a Sistemas de Información de ENAIRe desde Equipos o Instalaciones del Adjudicatario

No aplica.

E. Cumplimiento ENS

No aplica.

F. Organización de Seguridad de la Información

No aplica.

G. Valoración de la Seguridad y Auditoría

No aplica.

H. Tratamiento de Incidentes y Brechas de Seguridad de la Información

No aplica.

I. Configuración Segura de Sistemas

No aplica.

J. Suministro de Productos de Seguridad de las Tecnologías de la Información y la Comunicación

No aplica.

K. Seguridad en Desarrollo Software

No aplica.

L. Traslado, Reparación y Retirada de Equipos de ENAIRe

No aplica.

M. Servicios de Alojamiento

No aplica.

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

N. Servicios en la Nube

No aplica.

O. Penalizaciones

Sin perjuicio de otras penalizaciones que pudieran ser aplicables con carácter general, ENAIRe estará facultado para imponer las siguientes penalizaciones en caso de incumplimiento por parte del adjudicatario, en relación con las obligaciones relativas a la Seguridad de la Información establecidas en el presente pliego, cuando dicho incumplimiento origine un incidente de Seguridad de la Información o Ciberseguridad. Para ello, se aplicará la siguiente escala de niveles:

- a) Nivel ALTO: la penalización será del 20% (VEINTE POR CIENTO), pudiendo derivar en la resolución del contrato, cuando se produzca un incidente con impacto "Muy Alto" o "Crítico".
- b) Nivel MEDIO: la penalización será del 10% (DIEZ POR CIENTO), cuando se produzca un incidente con impacto "Medio" o "Alto".
- c) Nivel BAJO: la penalización será del 5% (CINCO POR CIENTO), cuando se produzca un incidente con impacto "Bajo" o "Nulo" ("Sin Impacto").

La escala de valoración de incidentes estará en consonancia con la "Guía nacional de notificación y gestión de ciberincidentes" vigente, disponible en la página web del Ministerio del Interior y en la de INCIBE-CERT (entre otros organismos), quedando a criterio de ENAIRe la valoración del impacto real del Incidente de Seguridad originado.

Este porcentaje se aplicará sobre el importe de la factura correspondiente al período / certificación en el que tenga lugar el incumplimiento.

Si, una vez impuestas 3 penalizaciones de nivel bajo, 2 de nivel medio o 1 de nivel alto, se produjera un nuevo incumplimiento del mismo nivel, se impondrá una nueva penalización por reiteración del 20% (VEINTE POR CIENTO) sobre el importe de la factura correspondiente al período / certificación en el que tenga lugar el incumplimiento.

Si, una vez impuesta la penalización por reiteración, se produjera un nuevo incumplimiento de cualquier nivel, ENAIRe estará facultado para proceder a la resolución del contrato.

Los incidentes de seguridad y las penalizaciones a aplicar seguirán los mismos criterios, tanto si están relacionados con tratamientos automatizados, con tratamientos no automatizados o tratamientos mixtos.

En aquellos incidentes de seguridad en los que concurren varias circunstancias que permitan determinar diferentes niveles según el criterio aplicable, se considerará el nivel más alto entre todos los posibles.

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

10. Dirección del Servicio

Tanto ENAIRE como la empresa adjudicataria se comprometen a designar representantes.

Durante el desarrollo del servicio, todas las relaciones con Enaire referentes al contrato, se establecerán a través del Director del Expediente o persona en quien delegue.

El Director del Expediente establecerá los criterios y líneas generales para la actuación en relación con el servicio contratado para el cumplimiento de los fines del mismo.

Por otra parte, la empresa adjudicataria deberá nombrar un Coordinador, cuya función principal será la de responder de la correcta realización del servicio contratado, responsabilizándose del nivel de calidad deseado en los resultados. Dicho Coordinador deberá estar permanentemente localizado servicio, al menos, durante el horario de prestación del servicio y, en todo caso tendrá las obligaciones siguientes:

- a) Actuar como interlocutor de la empresa contratista frente a ENAIRE, canalizando la comunicación entre la empresa contratista y el personal integrante del equipo de trabajo adscrito al contrato, de un lado, y ENAIRE, de otro lado, en todo lo relativo a las cuestiones derivadas de la ejecución del contrato.
- b) Distribuir el trabajo entre el personal encargado de la ejecución del contrato, e impartir a dichos trabajadores las órdenes e instrucciones que sean necesarias en relación con la prestación del servicio contratado.
- c) Supervisar el correcto desempeño por parte del personal integrante del equipo de trabajo de las funciones que tienen encomendadas, así como controlar la asistencia de dicho personal al puesto de trabajo.
- d) Organizar el régimen de vacaciones del personal adscrito a la ejecución del contrato a efectos de no alterar el buen funcionamiento del servicio
- e) Informar a ENAIRE acerca de las variaciones, ocasionales o permanentes, en la composición del equipo de trabajo adscrito a la ejecución del contrato

11. Responsabilidades

El Adjudicatario se hará responsable de los errores que pudieran cometerse en los servicios realizados o de los productos entregados por su personal y de su comportamiento, así como de aquellas actuaciones que pudieran inducir a ENAIRE al error. La declaración de comportamientos y errores será siempre a juicio de ENAIRE, por indicación expresa del Director del Expediente.

El Adjudicatario deberá señalar explícitamente que conoce en detalle el objeto del expediente y las funciones que ha de cumplir, de acuerdo con lo descrito en este PPT, no pudiendo alegar posteriormente falta o defecto de información en lo referente al mismo. Por consiguiente, aceptará la aportación a su cargo exclusivo, sin variación en el plazo establecido, de los servicios adicionales que, no habiendo sido considerados en su oferta, resulten luego necesarios para la completa realización del expediente.

A estos efectos, el Adjudicatario especificará en su oferta que aceptará que el Director del Expediente o persona en quien delegue certifique únicamente aquellos servicios o productos que, incluidos en la oferta,

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

hayan sido efectivamente realizados y que la totalidad de servicios que ofrece suministrar son los adecuados y suficientes para el fin perseguido.

12. Cláusula de Medios Humanos

I.- El adjudicatario se compromete a realizar la actividad, objeto del Pliego, con los medios humanos y materiales adecuados a tal fin.

II.- La facultad de dirección, organización y control de los trabajadores corresponde a la empresa adjudicataria por disponer la misma de una titularidad independiente a la de ENAIRe, así como de organización autónoma.

III.- No obstante, el adjudicatario, con el fin de que no quede dañada la imagen de ENAIRe, se compromete a adoptar todas aquellas medidas que considere necesarias para que su personal cumpla con los siguientes requisitos:

1. Desempeñar sus funciones sujeto al cumplimiento de la normativa que regule los recintos aeronáuticos y/o aeroportuarios; resultando el adjudicatario el único y exclusivo responsable por las infracciones en que pueda incurrir dicho personal, siendo ENAIRe ajena a esta responsabilidad.

En el supuesto que se produzcan quejas contra trabajadores de la adjudicataria motivadas por falta de capacidad o comportamiento incorrecto, el/la Director/a del Expediente dará traslado de las mismas al adjudicatario, a los efectos oportunos.

2. En particular, en el Centro de trabajo, llevar visible la tarjeta de identificación individual (acreditación) asignada por los servicios de Seguridad, cumpliendo escrupulosamente las autorizaciones y restricciones de la misma.

IV.- Respecto al personal, el adjudicatario se obliga expresamente a:

a) Realizar su actividad con una plantilla de trabajadores adecuada para el rendimiento óptimo y calidad del servicio. Respecto del personal del adjudicatario, adscrito a la actividad objeto de este pliego, una vez finalizada ésta o si la misma se resolviera antes de finalizar la vigencia pactada se estará a lo dispuesto en la legislación vigente y en los propios convenios colectivos que resulten de aplicación en materia de subrogación empresarial.

En ningún caso, el personal de la adjudicataria se incorporará a la plantilla de ENAIRe, ni ésta se subrogará en las relaciones laborales existentes entre el adjudicatario y sus trabajadores; siendo ENAIRe totalmente ajena a las referidas relaciones laborales, así como a las eventuales responsabilidades que de las mismas pudieran derivarse, que el adjudicatario acepta expresamente serán de su cuenta y cargo.

b) Aceptar todas las responsabilidades que se deriven de las relaciones que pueda establecer con terceras personas, durante la vigencia de la asistencia técnica, para desarrollar el objeto de la misma, por lo que ENAIRe no se subrogará en dichas relaciones.

c) Remitir a la autoridad correspondiente de ENAIRe, a los solos efectos de control y seguridad, relación nominal de los medios humanos que la empresa adjudicataria vaya a asignar a la prestación del servicio, con indicación del período de vinculación, así como la documentación que sea exigible; todo ello, a los solos efectos de determinar el período de validez de las tarjetas de seguridad (acreditaciones).

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

Sin esta remisión, no se entregará la tarjeta de seguridad (acreditación) que, a efectos de seguridad, será exigible portar.

Es responsabilidad de la empresa adjudicataria comunicar, con carácter inmediato, al Director/a del Expediente, cualquier variación de los datos contenidos en la citada relación nominal (nombre, vinculación, horario, etc.) con el objeto de que estén debidamente actualizadas las tarjetas de seguridad (acreditación).

Enaire, en atención al servicio público que presta, podrá retirar las tarjetas de seguridad (acreditaciones) cuando, por razones debidamente justificadas, peligre la seguridad o pueda quedar dañada la imagen de la Entidad.

d) El personal del adjudicatario quedará sometido a las normas que sobre la seguridad, policía y régimen interior ríjan en el Centro de trabajo.

e) Cumplimiento de toda la normativa aplicable a los trabajadores en materia de trabajo, empleo, Seguridad Social y prevención de riesgos laborales."

V.- Corresponde exclusivamente a la Empresa Adjudicataria la selección del personal que, reuniendo los requisitos de titulación y experiencia exigidos en los pliegos, formará parte del equipo de trabajo adscrito a la ejecución del contrato, sin perjuicio de la verificación por parte de ENAIRE del cumplimiento de aquellos requisitos.

La Empresa Adjudicataria procurará que exista estabilidad en el equipo de trabajo, y que las variaciones en su composición sean puntuales y obedezcan a razones justificadas, en orden a no alterar el buen funcionamiento del servicio informando en todo momento a ENAIRE.

VI.- La Empresa Adjudicataria asume la obligación de ejercer de modo real, efectivo y continuo, sobre el personal integrante del equipo de trabajo encargado de la ejecución del contrato, el poder de dirección inherente a todo empresario. En particular, asumirá la negociación y pago de los salarios, la concesión de permisos, licencias y vacaciones, la sustituciones de los trabajadores en casos de baja o ausencia, las obligaciones legales en materia de Seguridad Social, incluido el abono de cotizaciones y el pago de prestaciones, cuando proceda, las obligaciones legales en materia de prevención de riesgos laborales, el ejercicio de la potestad disciplinaria, así como cuantos derechos y obligaciones se deriven de la relación contractual entre empleado y empleador.

VII.- La Empresa Adjudicataria velará especialmente porque los trabajadores adscritos a la ejecución del contrato desarrollen su actividad sin extralimitarse en las funciones desempeñadas respecto de la actividad delimitada en los pliegos como objeto del contrato.

VIII.- Cuando la ejecución del contrato se lleve a cabo en dependencias de ENAIRE, el personal de la empresa adjudicataria ocupará espacios de trabajo diferenciados del que ocupan los empleados de ENAIRE. Corresponde también a la empresa adjudicataria velar por el cumplimiento de esta obligación.

IX.- Si como consecuencia del ejercicio de cualquier acción judicial o actuación administrativa , ENAIRE resultare responsable económica o empresarialmente por virtud de resolución firme de cualquier obligación derivada directa o indirectamente del incumplimiento de la obligación contenida en los párrafos anteriores, el Contratista quedará obligado a reintegrar, en el plazo de treinta (30) días desde el requerimiento que al efecto le haga ENAIRE, el montante dinerario que se derive de la aludida resolución o resoluciones y/o los gastos totales en que hubiere incurrido ENAIRE para su defensa y quedar ajena a las obligaciones de que se trate. ENAIRE podrá, cautelarmente, condicionar el pago de cualquier liquidación pendiente con dicho Contratista a

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

la eliminación previa de tales riesgos, así como a retener la fianza hasta que se haga efectivo su abono pudiendo proceder, en otro caso, a su incautación.

13. Clausula sobre Medios Materiales

Cuando el servicio se lleve a cabo en las dependencias de ENAIRe, la empresa adjudicataria facilitará a su personal todos los medios materiales para su correcta prestación.

14. Cláusula de Espacios

Dependiendo de la disponibilidad de locales, ENAIRe podrá facilitar a la Empresa Adjudicataria, los espacios que considere oportunos para la realización de aquellas actividades relacionadas con el contrato que deban ser desarrolladas necesariamente en las instalaciones de la Entidad y durante la vigencia del mismo.

Dichos espacios estarán diferenciados de los ocupados por el personal de ENAIRe

El equipamiento interior de tales espacios será totalmente a cargo de la empresa adjudicataria, así como cualquier reforma o modificación para su adaptación al uso, incluso las necesarias para cumplir las exigencias de la Legislación Laboral vigente y la normativa de Seguridad y Salud Laboral que resultasen aplicables a los medios humanos de la empresa adjudicataria, con motivo o derivados de la relación contractual que se establezca para la ejecución de este expediente. Dichas reformas deberán ser autorizadas previamente por Enaire.

Al final del período de vigencia del contrato, serán devueltos a Enaire en perfecto estado de uso, resultando en beneficio de los mismos cualquier reforma o mejora efectuada de acuerdo con los párrafos anteriores, sin que pueda ser reclamada cantidad alguna a Enaire por dichos conceptos. Cuando así se indique al Adjudicatario, por Enaire, aquél los devolverá en la situación inicial en que los recibió.

Si a la finalización del contrato no estuviesen en perfecto estado de conservación y limpieza, Enaire se reserva el derecho de realizar por su cuenta los trabajos necesarios, siendo imputable su coste al Adjudicatario, al margen de las sanciones que procedan.

Asimismo, y durante todo el periodo de duración del contrato, Enaire se reserva el derecho de traslado o desalojo de espacios concedidos, sin que el Adjudicatario tenga derecho a ningún tipo de indemnización.

En caso de que el adjudicatario solicitara disponer de mayor espacio, Enaire facilitará, dentro de la disponibilidad que al efecto exista.

Enaire estará libre de cualquier responsabilidad en cuanto a robo, deterioro, rotura o cualquier otro perjuicio que pudiera sufrir el material almacenado en dichos espacios, de cuya custodia será único responsable la Empresa Adjudicataria.

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

15. Medios Informáticos

La empresa adjudicataria aportará los medios informáticos. En el caso de que se considere inviable el uso de los ordenadores de la empresa adjudicataria en las oficinas de Enaire, debido a la imposibilidad de adaptar la infraestructura a las configuraciones de las distintas asistencias, Enaire podrá facilitar los medios informáticos, siendo el coste de alquiler mensual de los mismos, el siguiente:

Puesto con PC normal: 155 euros

Puesto con PC portátil: 168 euros

Puesto con PC gráfico (monitor de 20''): 163 euros (183 euros en caso de utilizar Autocad).

Dichos importes incluyen el soporte técnico así como licencias de software base, etc.

16. Cláusula de Huelga

En el caso de originarse algún conflicto del que pudiera verse afectado este servicio, dicha circunstancia deberá ponerse en conocimiento de la Dirección del Expediente, con una antelación mínima de diez días naturales.

Asimismo, el adjudicatario tendrá la obligación de comunicar a la Dirección del Expediente, con la suficiente y máxima antelación posible, los servicios mínimos acordados, en su caso, por la Autoridad competente, en el supuesto de huelgas o paros que afecten a su personal.

Durante el desarrollo de la huelga, el adjudicatario estará obligado a informar a la Dirección del Centro de la evolución e incidentes, en los plazos y formas fijados por el Director del expediente.

En las situaciones de huelga que afecten al personal de la empresa adjudicataria, se deberán mantener los servicios necesarios a fin de asegurar la prestación de los mismos, de acuerdo con la legislación vigente.

Durante el periodo de huelga, se suspenderá la contraprestación por parte de Enaire, en tanto el adjudicatario acuerde con ésta los niveles de servicio que se van a prestar y las formas de retribución correspondientes.

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

17. Anexos

Anexo 1: Descripción de la solución para interconexión SACTA – SCV en Torres con servicio de Aproximación.

Anexo 2: Especificación de la interfaz SACTA – SCV en SACTA 3.5 para ACC, T-ACC Y TWR.

Anexo 3: Requisitos Seguridad Adaptación Interfaz SCV-SACTA v 1.1

Anexo 4: Requisitos de Interoperabilidad. División de Comunicaciones”, DSIS-13-DTC-045

Realizado por:

SANCHEZ
BARRO
AURORA -
08977040W

Firmado digitalmente por SANCHEZ
BARRO AURORA - 08977040W
Nombre de reconocimiento (DN):
cn=ES,
serialNumber=IDCES-08977040W,
givenName=AURORA, sn=SANCHEZ
BARRO, cn=SANCHEZ BARRO
AURORA - 08977040W
Fecha: 2020.05.14 11:05:00 +02'00'

Fdo.: Aurora Sánchez Barro

Aprobado por:

García
Martín,
Manuel

Fdo.: Manuel García Martín

Firmado digitalmente por García
Martín, Manuel
Nombre de reconocimiento (DN):
dc=es, dc=nav, dc=na, dc=lean,
ou=Dirección de Sistemas,
ou=División Comunicaciones,
cn=García Martín, Manuel,
email=mangarcia@enaire.es
Fecha: 2020.05.14 17:22:34 +02'00'

Pliego de Prescripciones Técnicas:

Desarrollo e implantación de Interfaz SCV-SACTA en Torres con Servicio de Aproximación

ANEXO I

Descripción de la solución para interconexión SACTA – SCV en Torres con servicio de Aproximación

Elaborado: 14/05/2020

Página: 1/11

ANEXO 1: "Descripción de la solución para interconexión SACTA – SCV en Torres con servicio de Aproximación"

Índice

1. INTRODUCCIÓN.....	3
2. DESCRIPCIÓN DE LA SOLUCIÓN INTERFAZ SACTA - SCV.....	3
3. VALIDACIÓN DE LA SOLUCIÓN.....	4
4. DESPLIEGUE E INSTALACIÓN.....	5
5. DOCUMENTACIÓN.....	5
5.1 PLAN DE PRUEBAS.....	5
5.2 GESTIÓN DE SEGURIDAD OPERACIONAL (SAFETY)	6
6. FORMACIÓN	6
7. ASISTÉNCIA TÉCNICA	6
8. GESTIÓN DEL PROYECTO.....	7
8.1. PLAN DE GESTIÓN DEL PROYECTO	7
8.2. PLANIFICACIÓN DE ACTIVIDADES.....	9
8.3. INFORMES Y REUNIONES DE SEGUIMIENTO.....	10
8.4. INSPECCIONES.....	11

ANEXO 1: "Descripción de la solución para interconexión SACTA – SCV en Torres con servicio de Aproximación"

1. Introducción

El presente documento describe la solución técnica para la interconexión SACTA – SCV en Torres con servicio de Aproximación en que debido a la evolución de la funcionalidad a Operativa sin Ficha ha sido necesaria la separación técnica de los entornos de Aproximación y Torre en el Sistema Automatizado de Control de Tráfico Aéreo (SACTA). Esta separación tiene impacto directo sobre el Sistema de Comunicaciones Voz (SCV) de las torres en que se comparten los servicios de Torre y Aproximación, en particular sobre el interfaz que comunica el SCV con SACTA.

Esta solución será de aplicación en las Torres de los siguientes aeropuertos: Tenerife Norte y Santiago, equipados con un SCV CD-30 y Tenerife Sur y Bilbao equipados con un SCV ULISES V5000i, ambos de la firma NÚCLEO.

2. Descripción de la solución Interfaz SACTA - SCV

La solución técnica se basará en el desarrollo de una aplicación Software (PROXY) para incorporar entre SACTA y SCV. La misión fundamental del PROXY será trasladar las sectorizaciones recibidas en dos o más sesiones de SACTA a una sola hacia el SCV manteniendo en cada lado los protocolos adecuados.

Este PROXY manejará sesiones SACTA independientes para TWR y APP mientras que el SCV manejará una sesión única. En la medida de lo posible se evitará realizar modificaciones en los SCV CD-30 y ULISES V5000i.

El PROXY emulará un SCV en sus comunicaciones con SACTA y emulará SACTA en sus comunicaciones con el SCV. En ambos lados cumplimentará el Protocolo descrito en el documento "ESPECIFICACIÓN DE LA INTERFAZ SACTA – SCV EN SACTA 3.5 PARA ACC, T-ACC Y TWR" (SGFCI801.100). Asimismo, el PROXY dispondrá de los servicios de configuración de sectores, posiciones/UCS y cualquier otro servicio de configuración necesario para su funcionamiento. La configuración de sectorizaciones, logs e históricos relacionados se mantendrá tal como están implementados en los SCV.

Las premisas que deberán ser consideradas para el desarrollo de esta solución son las siguientes:

- El sistema SACTA dividirá la gestión de las torres complejas en, al menos, dos dependencias independientes. El sistema SCV debe gestionar esta nueva organización en su servicio de interfaz a SACTA, admitiendo recibir la sectorización de sus elementos en dos sesiones SACTA diferentes.
- Direcciones de Red: Cada sesión SACTA tendrá direcciones de red (origen y destino) diferenciadas.
- Datos de Protocolo: Cada sesión SACTA tendrá sus propios identificadores (Dominios, IDs, usuarios, grupos) diferenciados.
- ID Sectores: En cada una de las sesiones, los ID de Sector pueden estar repetidos.
- ID UCS: En cada una de las sesiones, los IDs de UCS pueden estar repetidos.

ANEXO 1: "Descripción de la solución para interconexión SACTA – SCV en Torres con servicio de Aproximación"

- Presencia de SACTA: El SCV considerará la presencia de SACTA cuando estén activas todas las sesiones SACTA, al objeto de evitar que se deshabiten las configuraciones locales relacionadas con las sesiones no activas.
- Presencia de SACTA. El SCV mantendrá la operativa actual ante la presencia de SACTA.
- Configuración: El SCV mantendrá la configuración de servicio actual (como si fuera una sola dependencia).
- Mantenimiento: El SCV mantendrá la supervisión y gestión actual del servicio SACTA (como si fuera una sola dependencia).
- Históricos: El SCV mantendrá los históricos del subsistema SACTA actuales (como si fuera una sola dependencia).

El PROXY se instalará en los servidores de los SCV, no requiriendo maquina adicional específica. Estará diseñado para respetar la arquitectura Main-Stand by de los servidores de ambos SCV, es decir, el PROXY será un servicio dual.

Se dotarán a los servidores del SCV con las tarjetas ETH necesarias para soportar las diferentes sesiones SACTA. Igualmente se realizará el cableado de datos ETH entre los servidores del SCV y los Firewalls de SACTA por las bandejas de audio y datos existentes.

Un servicio de configuración del PROXY establecerá el direccionamiento IP así como los grupos multicast de respuesta al SACTA.

Se dispondrá de un servicio de mantenimiento a través del cual se podrá conocer el estado operativo de cada uno de los PROXYs que conforman la solución dual de redundancia. Los errores, incidencias, e históricos en relación con ambos protocolos serán registrados en el PROXY, siendo accesible para mantenimiento desde un servicio web para tal fin.

3. Validación de la solución

Se llevarán a cabo todas las actividades y servicios para que esta solución sea desarrollada y validada en maqueta antes de su puesta en servicio operativo. Las validaciones se llevarán a cabo en las instalaciones del fabricante y/o las instalaciones del CED de ENAIRE.

El Adjudicatario elaborará un Plan de Pruebas de Validación detallado que sirva para comprobar y trazar el cumplimiento de los requisitos del PROXY y de la interfaz SCV-SACTA.

El desarrollo y validación de la solución deberán llevarse a cabo en los cuatro (4) meses siguientes al inicio del expediente.

ANEXO 1: "Descripción de la solución para interconexión SACTA – SCV en Torres con servicio de Aproximación"

4. Despliegue e instalación

Se llevarán a cabo todas las actividades y servicios necesarios para que esta solución sea instalada, puesta en marcha y probada con éxito en los 4 aeropuertos siguientes:

- Tenerife Norte
- Tenerife Sur
- Bilbao
- Santiago

5. Documentación

La empresa adjudicataria de los trabajos deberá aportar la siguiente documentación por cada uno de los aeropuertos considerados:

- Plan de Instalación y Transición
- Plan de Pruebas (PdV y PdA)
- Manual de instalación
- Gestión de Seguridad operacional (Safety).
- DSU actualizadas según normativa vigente de SCV CD-30 y ULISES 5000
- Documentación de Sistema y Equipos. Manual del Proxy SACTA-SCV

5.1 PLAN DE PRUEBASPruebas de Validación del Sistema (PdV):

El objetivo de estas PdV es comprobar que el Proxy SACTA-SCV cumple con prestaciones solicitadas en el PPT, tanto en lo que se refiere a requisitos específicos como a estándares (normativa, recomendaciones, etc.) Estas pruebas serán realizadas bien en instalaciones del adjudicatario, bien en instalaciones de ENAIRe, según el caso.

Pruebas de Aceptación en emplazamiento (PdA)

El objetivo de estas PdA es asegurar la correcta implantación de la solución proporcionada por el adjudicatario en los emplazamientos detallados en este PPT.

ANEXO 1: "Descripción de la solución para interconexión SACTA – SCV en Torres con servicio de Aproximación"

Durante estas pruebas, que se realizarán en el emplazamiento, se validará la operatividad del Proxy SACTA-SCV. Para ello se comprobarán los parámetros configurados y se realizarán pruebas integración y sectorización reales antes de la puesta en servicio operativo del conjunto.

5.2 GESTIÓN DE SEGURIDAD OPERACIONAL (SAFETY)

Las exigencias de Seguridad (Safety) en ATM imponen la necesidad de realizar un proceso formal y sistemático que permita anticipar y controlar la Seguridad de los Sistemas. El adjudicatario deberá elaborar los siguientes documentos de acuerdo a las especificaciones recogidas en el apartado 7 "Requisitos de Seguridad Operacional (SAFETY)" del P.P.T:

- Plan de Gestión de la Seguridad (Safety) del servicio y/o suministro. Se entregará una versión de este documento al inicio del expediente o como máximo un mes después de la fecha del Acta de Replanteo y una versión actualizada, si procede, ante cualquier cambio.
- Análisis de Seguridad (safety) del servicio y/o suministro. Se entregará una versión de este documento al inicio del expediente o como máximo un mes después de la fecha del Acta de Replanteo, una versión completada y actualizada un mes antes de la instalación (en caso necesario), otra versión completada y actualizada antes de la entrada en operación del equipamiento modificado (en caso necesario) y una versión definitiva una vez se dispongan de los resultados de las pruebas pertinentes antes de la recepción definitiva

6. Formación

El presente suministro incluirá los cursos de Formación y Entrenamiento del personal de ENAIRe que se vaya a hacer cargo de la operación y el mantenimiento de los sistemas y equipos a suministrar (GCI/PST, Área de Mantenimiento e Ingeniería de Explotación de Sistemas CNS).

Para ello se impartirá un curso en cada uno de los aeropuertos dividido en dos turnos de 5 horas cada uno.

7. Asistencia Técnica

Se incluye en el presente expediente una Asistencia Técnica telefónica 24 h durante tres días tras la implementación de esta solución en cada uno de los aeropuertos considerados.

ANEXO 1: "Descripción de la solución para interconexión SACTA – SCV en Torres con servicio de Aproximación"

8. Gestión del Proyecto

El Adjudicatario designará un Jefe de Proyecto, que será responsable del contrato e interlocutor principal del Director del Expediente de ENAIRe, coordinando todas las actividades del suministro.

8.1. PLAN DE GESTIÓN DEL PROYECTO

El Jefe de Proyecto designado por el Adjudicatario deberá elaborar, como primera acción, un Plan de Gestión del Proyecto donde se defina, de forma concreta, la organización del Adjudicatario implicado en el desarrollo del proyecto, la planificación de las fases y actividades del mismo, los productos parciales a obtener y los hitos a alcanzar a lo largo del desarrollo.

Este plan deberá estructurarse de forma que permita realizar un seguimiento a lo largo de todo el proyecto modificando las partes que precisen una actualización periódica.

Los diferentes datos que se exponen en el Plan de Gestión deberán estar de acuerdo con lo indicado por el Adjudicatario en la oferta.

Así mismo, el Adjudicatario definirá en este plan las responsabilidades de cada uno de los grupos organizativos definidos en la realización de las actividades planificadas.

Estructura y contenido

Se elaborará un Plan de Gestión, teniendo en cuenta los siguientes puntos:

1. Desglose de Actividades

El Adjudicatario deberá presentar el desglose de todas las actividades incluidas en el suministro. Este desglose servirá de base de partida para la realización del desglose de costes.

El Adjudicatario deberá presentar de forma gráfica, con la herramienta que se indica posteriormente, la descomposición del trabajo del suministro en actividades. El proyecto se descompondrá en tantos niveles como sea necesario.

Para cada actividad se deberá proporcionar la siguiente información:

- Denominación
- Fase del suministro
- Código
- Responsable y grupo responsable
- Fecha de comienzo y terminación

ANEXO 1: "Descripción de la solución para interconexión SACTA – SCV en Torres con servicio de Aproximación"

- Lista de productos / actividades que deben estar terminados, e hitos necesarios para comenzar esta actividad
 - Lista de entregables
2. Diagramas secuenciales

El Adjudicatario deberá realizar un diagrama con las actividades identificadas necesarias para la realización del Proyecto, después de haber realizado los análisis que permiten identificar las interdependencias y duración de cada una de las actividades. Este diagrama se preparará en base al Método del Camino Crítico (Critical Path Method, CPM), identificando aquellas actividades que son críticas.

Se considerarán dos niveles de presentación:

- Diagrama Secuencial Principal: Reflejará las relaciones entre las actividades de más alto nivel, y será la conclusión lógica de los Diagramas Secuenciales.
- Diagramas Secuenciales Detallados: Reflejarán las relaciones entre las actividades correspondientes a componentes o áreas que se consideren importantes o críticas del proyecto.

3. Calendario de actividades / hitos / entregas

El Adjudicatario deberá presentar:

- Una lista de actividades del proyecto con la duración, fechas de comienzo y terminación de las mismas especificadas para cada emplazamiento.
- Un diagrama de barras detallado de las actividades del proyecto e hitos asociados en función del tiempo.
- Una lista de los hitos del proyecto remarcando aquellos correspondientes a certificaciones con la fecha de cumplimiento, entregables correspondientes y actividad a la que pertenece.
- La definición de hitos.
- La planificación de entregas parciales.

4. Calendario de Certificaciones

El Adjudicatario deberá preparar una propuesta de Certificaciones. Esta propuesta deberá ser coherente con el calendario previsto de plazos parciales de entrega. Las entregas se realizarán tras pasar el hito de control correspondiente.

El criterio básico que se aplicará para la expedición de certificaciones parciales es la correspondencia entre cada certificación parcial asociada a cada hito en particular y la justificación de la realización satisfactoria de todas las actividades previas al paso de este hito y en todo caso según lo que se indica en otros puntos de este expediente.

ANEXO 1: "Descripción de la solución para interconexión SACTA – SCV en Torres con servicio de Aproximación"

La planificación de certificaciones deberá ser elaborada siguiendo los siguientes pasos:

- Agrupando las actividades asociadas a cada hito.
- Estableciendo una propuesta de calendario de cumplimiento de hitos.
- Proponiendo la certificación parcial asociada a cada hito, y considerando la valoración dada en el desglose de costes de acuerdo con las directrices que ENAIRe dicte tras la adjudicación.

ENAIRe podrá revisar y modificar esta propuesta de planificación con el objetivo de:

- Incluir hitos adicionales y / o modificar o suprimir los propuestos.
- Incluir actividades adicionales entre las asociadas a un hito y / o modificar o suprimir los propuestos.
- Modificar los recursos asociados a las actividades.
- Alterar el calendario previsto de plazos de entrega del suministro.

Métodos y herramientas

Para realizar la planificación del proyecto se utilizará la herramienta Microsoft Project y como procesador de textos se utilizará MS Word. De cada uno de los informes mensuales, actas, registros se entregará una copia en soporte magnético y una copia en papel.

Cuando el Adjudicatario estime necesarias otras herramientas, éstas deberán ser previamente aprobadas por la Dirección del Expediente.

8.2. PLANIFICACIÓN DE ACTIVIDADES

El Adjudicatario deberá recoger en el Plan de Gestión del Proyecto claramente las fechas y duración de, como mínimo, las siguientes tareas e hitos principales:

Tipo Actividad	Actividad
♦ Hito	Acta de inicio del expediente
Tarea	Definición especificaciones finales del PROXY
Tarea	Replanteo de instalaciones
♦ Hito	Acta de replanteo
Tarea	Desarrollo del Proxy
Tarea	Pruebas PdV en Fabrica
Tarea	Pruebas PdV en CED

ANEXO 1: "Descripción de la solución para interconexión SACTA – SCV en Torres con servicio de Aproximación"

Tipo Actividad	Actividad
♦ Hito	Inicio de instalación y adecuación de servidores en emplazamiento. Despliegue
Tarea	Trabajos de instalación en emplazamiento
Tarea	Configuración y Puesta a punto de los Servidores
Tarea	Formación
Tarea	Pruebas de aceptación (PdA)
♦ Hito	Puesta en operación / Transición
Tarea	Asistencia Técnica
♦ Hito	Recepción provisional

Tabla 1: Plan básico de gestión del proyecto

Plan de certificaciones

El Adjudicatario presentará un plan de certificaciones al Director del Expediente y una vez aprobado se incluirá en el Plan de Gestión del Proyecto.

8.3. INFORMES Y REUNIONES DE SEGUIMIENTO

El Adjudicatario elaborará mensualmente un informe de seguimiento de las actividades del programa de acuerdo con un estándar previamente acordado con el Director del Expediente.

Los informes de seguimiento deberán servir para:

- Mantener actualizados los Planes de Proyecto.
- Realizar el seguimiento de las actividades realizadas y los hitos alcanzados.
- Reflejar las entregas de productos parciales.
- Reflejar la planificación detallada de las actividades a corto plazo.
- Identificar las áreas de mayor riesgo.
- Definir puntos de acción a realizar ya sea por el Contratista o por ENAIRe.
- Realizar el seguimiento de los problemas y puntos abiertos registrados.

Antes del comienzo de los trabajos de instalación, el Adjudicatario impartirá una sesión informativa al personal técnico de la Región, en las instalaciones afectadas por el expediente. Se deberán realizar varios turnos de dicha sesión en caso necesario para tener total disponibilidad del personal, y en ella se explicará el alcance del expediente, los sistemas y equipos a instalar, su configuración, plan de instalación y plan de transición de los

ANEXO 1: "Descripción de la solución para interconexión SACTA – SCV en Torres con servicio de Aproximación"

nuevos sistemas. El Adjudicatario dotará a los asistentes del material didáctico necesario (presentaciones, documentación, esquemas, etc.) que permita una mejor y más fácil comprensión de la sesión.

A lo largo del suministro se realizarán reuniones de seguimiento, convocadas por el Director del Expediente. Las reuniones podrán celebrarse bien en Madrid o bien en las instalaciones en las que se ejecuta del proyecto, y a ellas deberá asistir obligatoriamente el Adjudicatario.

El Adjudicatario será responsable de mantener un registro de los puntos de acción acordados así como de su estado. La revisión de los puntos de acción será el primer tema a tratar en las reuniones de seguimiento.

8.4. INSPECCIONES

A lo largo del desarrollo del Suministro, ENAIRE se reserva el derecho a realizar tantas inspecciones, tanto en fábrica como en la instalación, como crea conveniente para verificar que se están realizando las actividades del suministro de acuerdo a los informes emitidos por el Adjudicatario.

Pliego de Prescripciones Técnicas:

Desarrollo e implantación de Interfaz SCV-SACTA en Torres con Servicio de Aproximación

ANEXO II



“ESPECIFICACIÓN DE LA INTERFAZ SACTA – SCV EN SACTA 3.5 PARA ACC, T-ACC Y TWR”

El contenido de este documento es propiedad de Aena, no pudiendo ser reproducido, ni comunicado total o parcialmente, a otras personas distintas de las incluidas en la lista de distribución adjunta a este documento, sin la autorización expresa de Aena.

Copia N°: 1/6



HOJA DE CONTROL DE LA DISTRIBUCIÓN

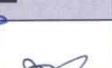
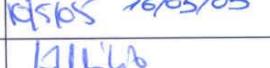
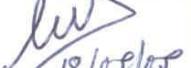
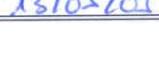
COPIA	NOMBRE	PUESTO	ORGANIZACIÓN
1	Emilio Gómez	Jefe División de Automatización	Aena
2	Jesús Cid	Jefe División de Comunicaciones	Aena
3	Myriam Santamaría	Jefe Departamento de Supervisión	Aena
4	José Luis Mancebo	Jefe Departamento de SCV	Aena
5	Fernando Criado	Jefe Departamento de Comunicaciones Tierra-Aire	Aena
6	Aurora Sánchez	Departamento de Comunicaciones Tierra-Aire	Aena

HOJA DE REGISTRO DE CAMBIOS

VERSIÓN	FECHA	PÁGINAS AFECTADAS	NOTAS Y RAZONES DEL CAMBIO
1	10/05/05	1ª Edición	



HOJA DE CONTROL DE LA DOCUMENTACIÓN

TÍTULO		
“ESPECIFICACIÓN DE LA INTERFAZ SACTA – SCV EN SACTA 3.5 PARA ACC, T-ACC Y TWR”		
CÓDIGO	1^a EDICIÓN	EDICIÓN VIGENTE
SGCIF801.100	FECHA: 10/05/05	EDICIÓN N°: 1 Fecha: 10/05/05
CLASIFICACIÓN	TIPO DE DOCUMENTO	ESTADO
Público	Documento Técnico	X Borrador
Interno.....X	Presentación	En Revisión
De exclusivo uso por Aena	Propuesta/Informe	Actualizable
Confidencial	Otros:	Informe Final: X
NOMBRE DE FICHERO	SGCIF801.100	
RUTA EN ARCHIVO	P\Dir Ingeniería Explotación Técnica\Div Automatización\División_automatización\ Documentación Aena\ Navegación Aérea\Automatización\SACTA\General\Comunicaciones\Interfaces	
PALABRAS CLAVE		
RESUMEN DEL CONTENIDO		
<p>El presente documento especifica la interfaz entre los Sistemas SACTA y SCV en la versión de SACTA 3.5 para ACC, T-ACC y TWR.</p>		
	<u>NOMBRE/PUESTO</u>	<u>FIRMA/VALIDADO</u>
REALIZADO	Begoña Tebar Alberto Pinto Julia Sánchez	10/05/05   
REVISADO	Myriam Santamaría José Luis Mancebo Fernando Criado	   16/05/05 16/05/05
APROBADO	Emilio Gómez Jesús Cid	   13/05/05 18/05/05



ÍNDICE

1. INTRODUCCIÓN.....	6
1.1. OBJETO	6
1.2. ORGANIZACIÓN DEL DOCUMENTO	6
1.3. DOCUMENTOS DE REFERENCIA	6
1.4. ACRÓNIMOS	7
2. PROTOCOLO DE COMUNICACIÓN	7
2.1. ARQUITECTURA FÍSICA	7
2.2. PILA DE PROTOCOLOS.....	8
2.3. NIVEL FÍSICO	9
2.4. NIVEL DE ENLACE.....	9
2.5. NIVEL DE RED.....	9
2.6. NIVEL DE TRANSPORTE.....	9
2.7. NIVEL DE APLICACIÓN	10
2.7.1. <i>GESTIÓN DE LOS MENSAJES</i>	11
2.7.2. <i>FORMATO DE LOS MENSAJES</i>	11
2.7.3. <i>CABECERAS</i>	12
2.7.4. <i>TIPOS DE MENSAJES SACTA-SCV</i>	12
2.7.4.1. MENSAJE DE INICIO DE SECUENCIA SCV → SACTA	13
2.7.4.2. MENSAJE DE INICIO DE SECUENCIA SACTA → SCV	14
2.7.4.3. MENSAJE DE PRESENCIA SCV → SACTA	15
2.7.4.4. MENSAJE DE PRESENCIA SACTA → SCV	17
2.7.4.5. MENSAJE DE PETICIÓN DE SECTORIZACIÓN SCV → SACTA	18
2.7.4.6. MENSAJE DE SECTORIZACIÓN SACTA → SCV	20
2.7.4.7. MENSAJE DE RESPUESTA DE SECTORIZACIÓN SCV → SACTA.....	22
3. INFORMACIÓN COMPARTIDA SACTA-SCV	24
ANEXO A. INTRODUCCIÓN AL MODELO CONCEPTUAL PARA SACTA 3.5	A-1
1. INTRODUCCIÓN.....	A-2
2. DIAGRAMA.....	A-2
3. RESPONSABILIDADES DE CONTROL.....	A-3



3.1.	ESPACIO SACTA	A-3
3.2.	REGIÓN SACTA.....	A-3
3.3.	AGRUPACIÓN SACTA.....	A-4
3.4.	OBJETO DE RESPONSABILIDAD	A-4
4.	RECURSOS DE CONTROL	A-4
4.1.	CENTRO DE CONTROL	A-4
4.2.	SERVICIOS	A-5
4.3.	DEPENDENCIA DE CONTROL.....	A-5
4.4.	UNIDAD DE CONTROL.....	A-5
4.5.	POSICIÓN DE CONTROL.....	A-5
4.6.	FORMA DE OPERACIÓN.....	A-6
5.	RELACIONES ENTRE RESPONSABILIDADES DE CONTROL Y RECURSOS DE CONTROL.....	A-6
5.1.	ASIGNACIÓN DE RESPONSABILIDADES A DEPENDENCIAS (ARD)	A-6
5.2.	CONFIGURACIÓN OPERACIONAL	A-6
5.3.	ASIGNACIÓN DE FORMAS DE OPERACIÓN (AFO)	A-7

1. INTRODUCCIÓN

1.1. OBJETO

Este documento tiene por objeto especificar la interfaz de comunicaciones entre los sistemas SACTA y SCV en aquellos centros de control (ACC y T-ACC) y torres de control de tipo VICTOR Fase 3 (con funcionalidad SACTA TPVT), en que se encuentra disponible la versión SACTA 3.5, y para cualquier nuevo SCV que se instale durante la vigencia de dicha versión SACTA.

1.2. ORGANIZACIÓN DEL DOCUMENTO

Este documento se divide en las siguientes partes:

- Capítulo 1: Introducción
- Capítulo 2: Protocolo de comunicación
 - I. Arquitectura Física
 - II. Pila de Protocolos
 - III. Nivel Físico
 - IV. Nivel de Enlace
 - V. Nivel de Red
 - VI. Nivel de Transporte
 - VII. Nivel de Aplicación
- Capítulo 3: Información Compartida SACTA – SCV
- Anexos

1.3. DOCUMENTOS DE REFERENCIA

- [1] SACTA v3.4 - Especificación de Requisitos del Subsistema de Comunicaciones (SCOME2.001), AENA (División de Automatización).
- [2] RFC 768 - User Datagram Protocol (Internet's technical documentation)
- [3] RFC 791 - Internet Protocol (Internet's technical documentation)
- [4] IEEE 802.3 - Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 1985
- [5] ANSI X3.28 - Procedures for the Use of the Communication Control Characters of the American National Standard Code for Information Interchange in Specified Data Communications Links, 1976 (Reaffirmed 1986, 1992)
- [6] Plan de Numeración IP de Redes conectadas con REDAN (RDN_IP_031127), AENA (División de Comunicaciones).
- [7] Plan de Numeración IP de redes SACTA III.5, AENA (División de Automatización).
- [8] Plan de Numeración IP de redes SCV (versión Borrador 04/2005), AENA (División de Comunicaciones).

1.4. ACRÓNIMOS

ANSI	American National Standards Institute
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
ISO	International Standards Organization
OSI	Open Systems Interconnection
PSI	Posición de Supervisión Integrada
PST	Posición de Supervisión de TWR
SCV	Sistema de Comunicación de Voz
SACTA	Sistema Automático de Control de Tráfico Aéreo
TCP	Transport Control Protocol
UDP	User Datagram Protocol

2. PROTOCOLO DE COMUNICACIÓN

2.1. ARQUITECTURA FÍSICA

Aunque la arquitectura física de la interfaz SACTA – SCV pueda sufrir ligeras variaciones en función de las necesidades de disponibilidad, seguridad, etc. del centro en cuestión, el criterio general consistirá en una conexión entre el SCV y SACTA, a través de las redes de ambos sistemas. SACTA dispondrá de una doble red LAN (red de control o red radar) y cada SCV dispondrá de su propia red LAN que podrá ser simple o doble.

Cada uno de los dos sistemas, SACTA y SCV, dispondrá de una *Aplicación de Comunicaciones*, que permitirá el envío, recepción y gestión de los mensajes por las redes LAN.

En cualquier centro de navegación aérea habrá un máximo de ocho (8) PSI/T's. En los Centros de Control de Ruta y TMA, SACTA tratará a todos los SCVs existentes en el centro como un único SCV a través de una única conexión física (por doble LAN). En el caso de las Torres de Control existirá un máximo de cinco (5) SCV's diferentes y la comunicación entre los sistemas SACTA y SCV se realizará de forma que SACTA trate los SCVs físicos existentes en el centro como sistemas independientes.

La solución de arquitectura para la interfaz SACTA – SCV se presenta en la siguiente figura:

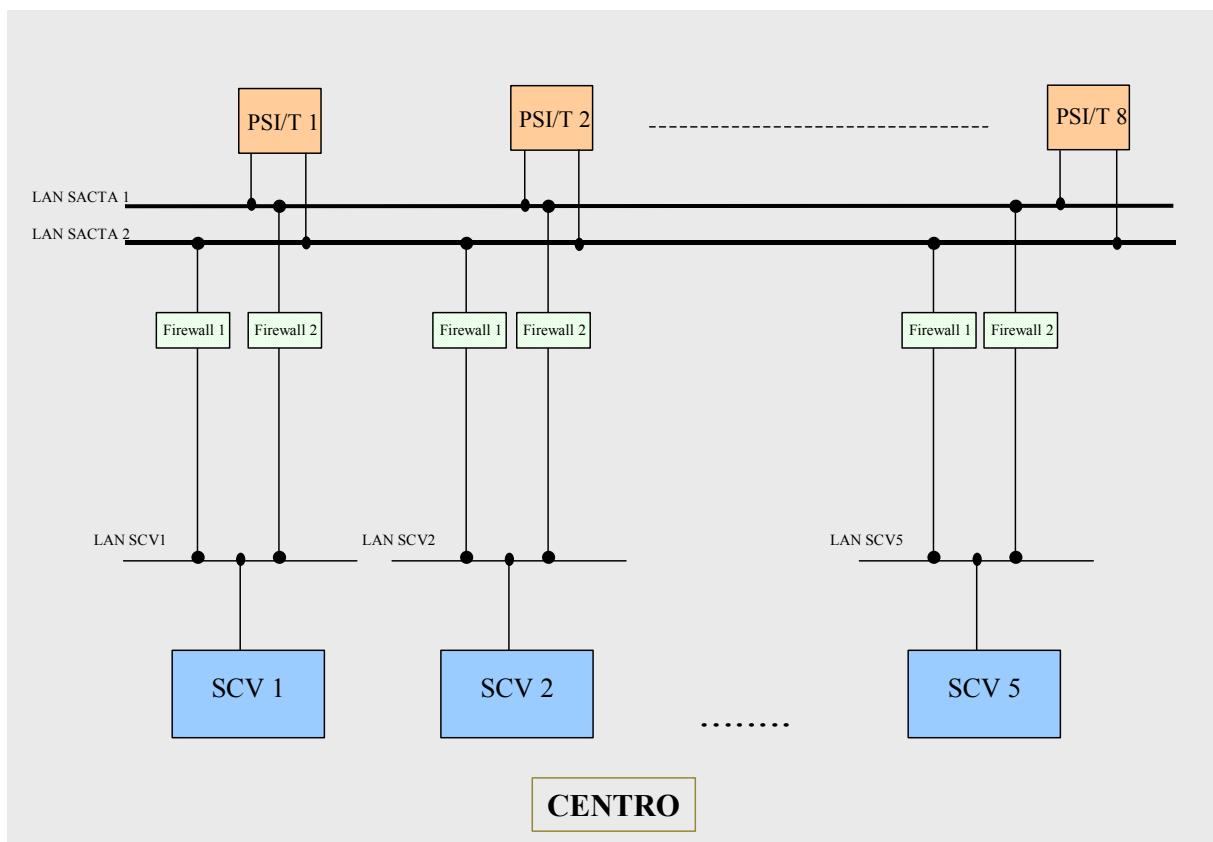


Figura 2.1- Arquitectura Física de la Interfaz SACTA – SCV

Nota: Los equipos Firewall pueden no existir en todos los centros. Los sistemas SCV han empleado hasta ahora para conectarse con SACTA, direcciones IP del sistema SACTA. En la actualidad, REDAN ha asignado a los sistemas SCV un rango de direcciones IP propias (direcciones no SACTA). Aún así, en algunos emplazamientos, los sistemas SCV seguirán manteniendo durante algún tiempo su direccionamiento IP SACTA. Sin embargo, tanto para los nuevos sistemas SCV que se vayan a instalar como en aquellos emplazamientos en los que se solicite, los mencionados sistemas emplearán direcciones IP propias. En estos emplazamientos, si no existen firewalls, SACTA proveerá los medios necesarios para hacer la traducción de direcciones IP.

2.2. PILA DE PROTOCOLOS

El intercambio de mensajes SACTA con SCV se basará en el conjunto de protocolos UDP/IP que se muestra en la **Figura 2.2**. En dicha figura se indica el protocolo empleado en cada nivel equivalente aproximado del Modelo de Referencia ISO/OSI.

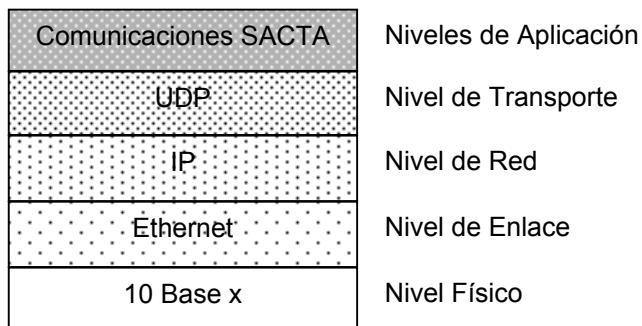


Figura 2.2 - Pila de Protocolos de Comunicación SACTA – SCV

En los siguientes apartados se especifican los diferentes niveles por referencia a estándares, concretándose, si da lugar, las particularidades de cada nivel.

2.3. NIVEL FÍSICO

La interfaz física SACTA – SCV será mediante Par trenzado (10 Base T), por conexión de las redes de SCV:

- En ACC y T-ACC: A ambas redes de control SACTA.
- En TWR: A ambas redes radar SACTA.

2.4. NIVEL DE ENLACE

El protocolo del nivel de enlace será **Ethernet**, conforme IEEE 802.3 [4].

2.5. NIVEL DE RED

El protocolo del nivel de red será **IP**, conforme RFC 791 [3].

Las direcciones IP unicast necesarias para la comunicación entre SACTA – SCV están definidas, para sus tres primeros octetos, en el documento RDN_IP_031127 Plan de Numeración IP de Redes conectadas con REDAN [véase Ref. 6] y, para el cuarto octeto, en los documentos Plan de Numeración IP de Redes SACTA III.5 y Plan de numeración IP de Redes SCV. Las direcciones IP multicast SACTA cumplirán, asimismo, el direccionamiento definido en el Plan de Numeración IP de Redes SACTA III.5.

El envío de mensajes en sentido SCV -> SACTA se realizará en **multicast**, y el usuario destino del mismo será el “grupo de PSI/Ts”.

El envío de mensajes en sentido SACTA -> SCV se realizará en **unicast**.

2.6. NIVEL DE TRANSPORTE

El protocolo del nivel de transporte será **UDP**, conforme RFC 768 [2].

Los **puertos** necesarios para la comunicación entre SACTA – SCV estarán definidos en el fichero de configuración correspondiente. En virtud de dicho fichero las aplicaciones escuchan en los siguientes puertos:

- SCVs → 19204
- PSI/Ts → 15100

2.7. NIVEL DE APLICACIÓN

Los identificadores de **usuario** necesarios para la comunicación entre SACTA – SCV estarán definidos en el fichero de configuración COM_USUARIOS.CFG de SACTA v3.5. En virtud de dicho fichero se tienen los identificadores para los siguientes usuarios:

- SCV1
- SCV2
- SCV3
- SCV4
- SCV5
- Grupo de PSI/Ts (usuario SPSI_PSI)
- PSI/T1 (usuario SPSI_PSI1)
- PSI/T2 (usuario SPSI_PSI2)
- PSI/T3 (usuario SPSI_PSI3)
- PSI/T4 (usuario SPSI_PSI4)
- PSI/T5 (usuario SPSI_PSI5)
- PSI/T6 (usuario SPSI_PSI6)
- PSI/T7 (usuario SPSI_PSI7)
- PSI/T8 (usuario SPSI_PSI8)
- PSI/T1 (usuario SPV_PSI1)
- PSI/T2 (usuario SPV_PSI2)
- PSI/T3 (usuario SPV_PSI3)
- PSI/T4 (usuario SPV_PSI4)
- PSI/T5 (usuario SPV_PSI5)
- PSI/T6 (usuario SPV_PSI6)
- PSI/T7 (usuario SPV_PSI7)
- PSI/T8 (usuario SPV_PSI8)

Nota 1: En los ACC y T-ACC, el identificador de usuario de SCV será siempre el correspondiente a SCV1.

Nota 2: Los mensajes con origen en la red SACTA y destino la red SCV tendrán diferente identificador de usuario, para una misma máquina, en función del tipo de mensaje enviado. Los Mensajes de Presencia e Inicio de Secuencia se enviarán con usuarios identificados

como 'SPV_PSI' y los Mensajes de Sectorización se enviarán con usuarios identificados como 'SPSI_PSI'.

2.7.1. GESTIÓN DE LOS MENSAJES

La aplicación de comunicaciones encargada de la gestión de los mensajes LAN en el SCV, realizará el envío de los mensajes a ambas redes de control SACTA o a ambas redes radar SACTA y permitirá la recepción de los mensajes desde ambas redes de forma simultánea. Dicha aplicación será capaz de interpretar y traducir el contenido de cada uno de los mensajes descritos en el apartado 2.7.4.

De igual forma, la aplicación SACTA (PSI/T) encargada de la gestión de los mensajes LAN SCV/SACTA, enviará siempre de forma simultánea los mensajes hacia los SCVs por ambas redes de control SACTA o por ambas redes radar SACTA y permitirá la recepción igualmente por dichas redes.

Ambas aplicaciones, mediante el número de secuencia de los mensajes, podrán identificar si un nuevo mensaje recibido es copia de alguno de los últimos mensajes recibidos y así descartar los mensajes duplicados. Independientemente de esto, puede ser implementado cualquier otro método para el descarte de mensajes duplicados sin hacer uso del campo "Secuencia".

2.7.2. FORMATO DE LOS MENSAJES

En el documento “Programa SACTA. Proyecto SACTA v3.4 - Especificación de Requisitos del Subsistema de Comunicaciones” [1] puede consultarse el detalle de la especificación de las comunicaciones internas y externas del sistema SACTA. El presente documento particulariza la citada especificación para la interfaz SACTA – SCV.

El formato de los mensajes intercambiados entre SACTA y SCV seguirán el formato genérico de los mensajes SACTA [1], recogido en la **Figura 2.3**, en la que se ha sombreado la cabecera que precede a la información propiamente dicha del mensaje.

32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
DOMINIO ORIGEN										CENTRO ORIGEN										USUARIO ORIGEN											
DOMINIO DESTINO										CENTRO DESTINO										USUARIO DESTINO											
OPCIÓN										SECUENCIA										TIPO DE MENSAJE											
INFORMACIÓN										HORA										LONGITUD											
INFORMACIÓN																															

Figura 2.3 - Formato de un mensaje SACTA

2.7.3. CABECERAS

A continuación se detalla el contenido de las cabeceras a usar por los mensajes ligados a la comunicación entre SACTA y SCV. Los únicos valores dependientes del emplazamiento corresponden a los campo Centro Origen y Centro Destino.

CAMPO	CONTENIDO	TAMAÑO
DOMINIO ORIGEN	Número asignado en archivos de configuración. “1” (01 Hex.) = OPERACIONAL “2” (02 Hex.) = SIMULACION	1 byte
CENTRO ORIGEN	Número asignado en archivos de configuración y definido en el documento SACTA v3.4 [1]	1 byte
USUARIO ORIGEN	Número asignado en archivos de configuración, definido en apartado 2.7.	2 bytes
DOMINIO DESTINO	Número asignado en archivos de configuración. “1” (01 Hex.) = OPERACIONAL “2” (02 Hex.) = SIMULACION	1 byte
CENTRO DESTINO	Número asignado en archivos de configuración y definido en el documento SACTA v3.4 [1]	1 byte
USUARIO DESTINO	Número asignado en archivos de configuración, definido en apartado 2.7.	2 bytes
SESIÓN	0	2 bytes
TIPO DE MENSAJE	Identificador del tipo de mensaje intercambiado: • “0” = Mensaje de inicio de secuencia • “707” (2C3 Hex.) = Mensaje de Petición de Sectorización • “710” (2C6 Hex.) = Mensaje de Respuesta de Sectorización • “1530” (5FA Hex.) = Mensaje de Presencia (“sincro”) • “1632” (660 Hex.) = Mensaje de Sectorización	2 bytes
OPCIÓN DE SECUENCIA	“000” = Mensaje de datos “010” = Mensaje de inicio de secuencia	3 bits
NÚMERO DE SECUENCIA	Número puesto por el proceso de comunicaciones en origen, en función del usuario origen y del usuario destino (secuencia 0..287)	13 bits
LONGITUD	Longitud del campo Datos en “shorts” (1 short equivale a 2 bytes) (“0” = mensaje de inicio de secuencia y de petición de sectorización)	2 bytes
HORA	Hora UNÍX del mensaje (número de segundos transcurridos desde el 1 de enero de 1970)	4 bytes
DATOS (Longitud 1 - 65484 bytes) (no existe para los mensajes de inicio de secuencia)		

Tabla 2.1 - Formato de la cabecera del mensaje de datos

2.7.4. TIPOS DE MENSAJES SACTA-SCV

Los tipos de mensaje que soportará la interfaz son los siguientes:

- Mensaje de inicio de secuencia SCV → SACTA
- Mensaje de inicio de secuencia SACTA → SCV
- Mensaje de Presencia SCV → SACTA

- Mensaje de Presencia SACTA → SCV
- Mensaje de Petición de Sectorización SCV → SACTA
- Mensaje de Sectorización SACTA → SCV
- Mensaje de Respuesta de Sectorización SCV → SACTA

Mediante el uso del UML (diagramas de secuencia) se representa gráficamente el intercambio de mensajes entre SACTA y SCV.

2.7.4.1. MENSAJE DE INICIO DE SECUENCIA SCV → SACTA

El campo de número de secuencia es utilizado por las comunicaciones SACTA con el fin de descartar los mensajes duplicados que son recibidos por una red doble SACTA (LANes redundantes).

Entre cada dos usuarios (SCV y SACTA) se mantendrán siempre un flujo de conversación. Cada flujo manejará una secuencia diferente, incrementándose estas de forma independiente en cada nuevo mensaje enviado (en SACTA v3.5, para los mensajes entre SACTA y SCV, el campo secuencia es un valor cíclico entre 0 y 287).

El mensaje de inicio de secuencia tendrá siempre como número de secuencia el “0” (ver **Tabla 2.2**) y lo generará y enviará un usuario (SACTA ó SCV) antes de iniciar por vez primera un flujo de conversación con un nuevo usuario (SCV ó SACTA). Comenzará así una nueva secuencia de mensajes donde el próximo mensaje a enviar tendrá el número de secuencia “1”.

De esta forma, este mensaje de “*inicio de secuencia SCV → SACTA*” lo generará cada SCV antes de iniciar por vez primera un flujo de conversación con un nuevo usuario SACTA. El usuario SACTA será en este caso el “Grupo de PS/TIs” (definido en el apartado 2.7).

Cada SCV mantendrá únicamente un flujo de conversación con el usuario “Grupo de PSI/Ts”. Existirá así, un máximo de cinco (5) flujos de conversación independientes en sentido SCV → SACTA, cuyos mensajes se enviarán siempre en **multicast** (ver apartado 2.5).

Cada SCV enviará el “*mensaje de inicio de secuencia SCV → SACTA*”:

- Al arrancar, en **multicast** al “Grupo de PSI/Ts”, y antes de enviar el mensaje de petición de sectorización (previo al primer mensaje de presencia), ver **Figura 2.4**.
- Al detectar la recuperación del enlace con SACTA (cuando previamente se hayan sobrepasado 30 segundos sin recibir presencia de las PSI/Ts), en **multicast** al “Grupo de PSI/Ts”, y antes de enviar su mensaje de petición de sectorización (previo al primer mensaje de presencia), ver **Figura 2.4**.

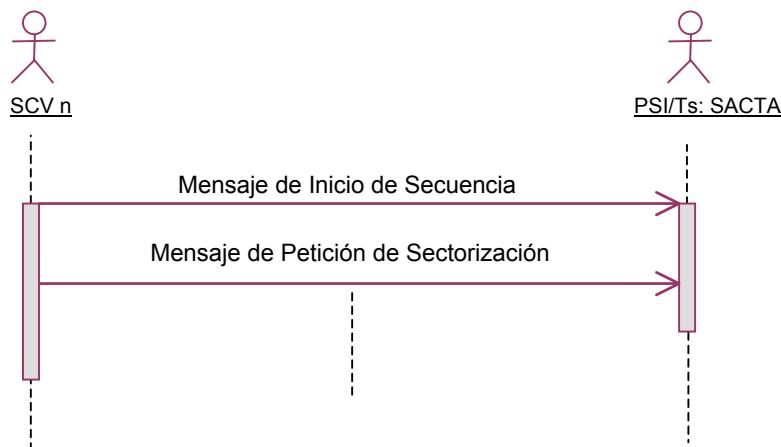


Figura 2.4 - Intercambio del mensaje de inicio de secuencia SCV → SACTA (Caso 1 y 2)

A continuación se detalla el contenido del mensaje de inicio de secuencia a usar por los mensajes ligados a la comunicación SCV → SACTA:

CAMPO	CONTENIDO		TAMAÑO
DOMINIO ORIGEN	“1” (01 Hex.) = OPERACIONAL		1 byte
CENTRO ORIGEN	Número asignado en archivos de configuración.		1 byte
USUARIO ORIGEN	ACC y T-ACC: “X” (XX XX Hex.) = SCV1	TWR: “X” (XX XX Hex.) = SCV1 ó “X” (XX XX Hex.) = SCV2 ó “X” (XX XX Hex.) = SCV3 ó “X” (XX XX Hex.) = SCV4 ó “X” (XX XX Hex.) = SCV5	2 bytes
DOMINIO DESTINO	“1” (01 Hex.) = OPERACIONAL		1 byte
CENTRO DESTINO	Número asignado en archivos de configuración.		1 byte
USUARIO DESTINO	“X” (XX XX Hex.) = Grupo de PSI/Ts		2 bytes
SESIÓN	0		2 bytes
TIPO DE MENSAJE	0		2 bytes
OPCIÓN DE SECUENCIA	“010” = Mensaje de inicio de secuencia		3 bits
NÚMERO DE SECUENCIA	0		13 bits
LONGITUD	0		2 bytes
HORA	Hora UNÍX del mensaje (número de segundos transcurridos desde el 1 de enero de 1970)		4 bytes

Tabla 2.2 - Formato de la cabecera del mensaje de inicio de secuencia SCV → SACTA

2.7.4.2.MENSAJE DE INICIO DE SECUENCIA SACTA → SCV

Este mensaje de “*inicio de secuencia SACTA → SCV*” lo generará cada usuario SACTA (PSI/T1, PSI/T2, PSI/T3, PSI/T4, PSI/T5, PSI/T6, PSI/T7 y PSI/T8), antes de iniciar por vez primera un flujo de conversación con un nuevo usuario SCV. En este caso los usuarios SCV serán cada uno de los SCVs (definidos en el apartado 2.7).

Cada usuario SACTA (PSI/T1, PSI/T2, PSI/T3, PSI/T4, PSI/T5, PSI/T6, PSI/T7 y PSI/T8) mantendrá un flujo de conversación con cada usuario SCV. Existirá así un máximo de 8x(número de SCVs) flujos de conversación independientes en sentido SACTA → SCV, cuyos mensajes se enviarán siempre en **unicast** (ver apartado 2.5).

Cada usuario SACTA enviará el “mensaje de inicio de secuencia SACTA → SCV”:

- Al arrancar, en **unicast** a cada uno de los SCV conectados, y antes de enviar el primer mensaje de presencia, ver **Figura 2.5**.

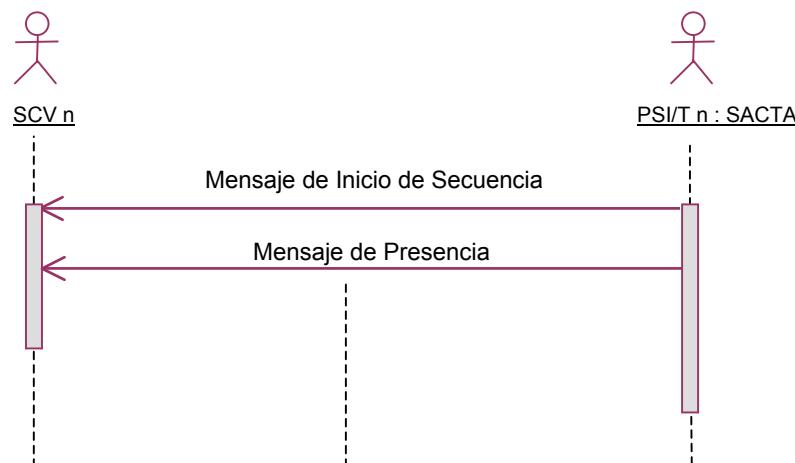


Figura 2.5 - Intercambio del mensaje de inicio de secuencia SACTA → SCV

A continuación se detalla el contenido del mensaje de inicio de secuencia a usar por los mensajes ligados a la comunicación SACTA → SCV:

CAMPO	CONTENIDO	TAMAÑO
DOMINIO ORIGEN	“1” (01 Hex.) = OPERACIONAL	1 byte
CENTRO ORIGEN	Número asignado en archivos de configuración.	1 byte
USUARIO ORIGEN	“X” (XX XX Hex.) = PSI/T1 ó “X” (XX XX Hex.) = PSI/T2 ó “X” (XX XX Hex.) = PSI/T3 ó “X” (XX XX Hex.) = PSI/T4 ó “X” (XX XX Hex.) = PSI/T5 ó “X” (XX XX Hex.) = PSI/T6 ó “X” (XX XX Hex.) = PSI/T7 ó “X” (XX XX Hex.) = PSI/T8	2 bytes
DOMINIO DESTINO	“1” (01 Hex.) = OPERACIONAL	1 byte
CENTRO DESTINO	Número asignado en archivos de configuración.	1 byte
USUARIO DESTINO	ACC y T-ACC: “X” (XX XX Hex.) = SCV1	2 bytes
	TWR: “X” (XX XX Hex.)= SCV1 ó “X” (XX XX Hex.) = SCV2 ó “X” (XX XX Hex.) = SCV3 ó “X” (XX XX Hex.)= SCV4 ó “X” (XX XX Hex.) = SCV5	
SESIÓN	0	2 bytes
TIPO DE MENSAJE	0	2 bytes
OPCIÓN DE SECUENCIA	“010” = Mensaje de inicio de secuencia	3 bits
NÚMERO DE SECUENCIA	0	13 bits
LONGITUD	0	2 bytes
HORA	Hora UNÍX del mensaje (número de segundos transcurridos desde el 1 de enero de 1970)	4 bytes

Tabla 2.3 - Formato de la cabecera del mensaje de inicio de secuencia SACTA → SCV

2.7.4.3. MENSAJE DE PRESENCIA SCV → SACTA

El objetivo de este mensaje es proporcionar información a SACTA de la presencia de los SCVs.

Lo enviará periódicamente cada uno de los SCVs activos en el centro, en **multicast**, al “Grupo de PSI/Ts” con una “cadencia” de 5 segundos. Si pasados 30 segundos las PSI/Ts no reciben ningún mensaje de presencia de un determinado SCV, estas informarán de la pérdida del enlace con dicho SCV. Ambos periodos, formarán parte de la información contenida en el mensaje de presencia (ver **Tabla 2.4**) y podrán ser modificados desde el archivo de configuración correspondiente.

El SCV enviará el “*mensaje de presencia SCV → SACTA*”:

- Desde el momento del arranque (después del mensaje de petición de sectorización), ver **Figura 2.6**.

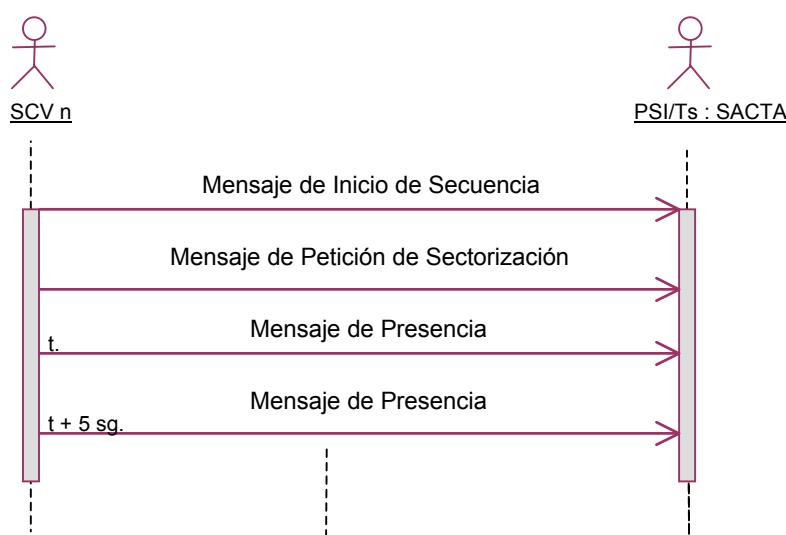


Figura 2.6 - Intercambio del mensaje de presencia SCV → SACTA

El contenido de los campos del mensaje se indica en la tabla adjunta:

CAMPO	CONTENIDO	TAMAÑO
DOMINIO ORIGEN	“1” (01 Hex.) = OPERACIONAL	1 byte
CENTRO ORIGEN	Número asignado en archivos de configuración.	1 byte
USUARIO ORIGEN	ACC y T-ACC: “X” (XX XX Hex.) = SCV1	2 bytes
	“X” (XX XX Hex.) = SCV2 ó “X” (XX XX Hex.) = SCV3 ó “X” (XX XX Hex.) = SCV4 ó “X” (XX XX Hex.) = SCV5	
DOMINIO DESTINO	“1” (01 Hex.) = OPERACIONAL	1 byte
CENTRO DESTINO	Número asignado en archivos de configuración.	1 byte
USUARIO DESTINO	“X” (XX XX Hex.) = Grupo de PSI/Ts	2 bytes
SESIÓN	0	2 bytes
TIPO DE MENSAJE	“1530” (05 FA Hex.) = Mensaje de Presencia	2 bytes
OPCIÓN DE SECUENCIA	“000” = Datos	3 bits
NÚMERO DE SECUENCIA	(Secuencia 0..287)	13 bits
LONGITUD	11	2 bytes
HORA	Hora UNIX del mensaje.	4 bytes
NÚMERO DE CARACTERES	3	2 bytes

CAMPO	CONTENIDO	TAMAÑO
DEL TIPO DE PROCESADOR		
TIPO PROCESADOR	“SCV” + 1 Nulo + No usado (CÓDIGO ASCII) (534356 + 00 + XXXXXXXXXXXX Hex.)	10 bytes
NÚMERO PROCESADOR	ACC y T-ACC: 1 TWR: 1, 2, 3, 4 ó 5	2 bytes
NO USADO	0	2 bytes
ESTADO PROCESADOR	1 (Disponible)	1 byte
SUBESTADO PROCESADOR	0 (No tiene)	1 byte
TIEMPO DE INFORME (segundos)	5	2 bytes
TIEMPO MÁXIMO DE INFORME (seg.)	30	2 bytes

Tabla 2.4 - Formato del mensaje de presencia SCV → SACTA

2.7.4.4.MENSAJE DE PRESENCIA SACTA → SCV

Mediante este mensaje se mantendrá informado a los SCVs de la presencia de las PSI/Ts de SACTA.

Para ello, este mensaje se enviará cada 5 segundos por cada una de las PSI/Ts que estén activas en el sistema en **unicast** hacia cada uno de los SCVs. Si pasados 30 segundos, el SCV no recibe ningún mensaje de presencia de las PSI/Ts, este informará de la pérdida del enlace con SACTA. Ambos periodos, formarán parte de la información contenida en el mensaje de presencia (ver **Tabla 2.5**) y podrán ser modificados desde el archivo de configuración correspondiente.

SACTA enviará el “*mensaje de presencia SACTA → SCV*”:

- Desde el momento del arranque de la PSI/T (después del envío del mensaje de inicio de secuencia), ver **Figura 2.7**.

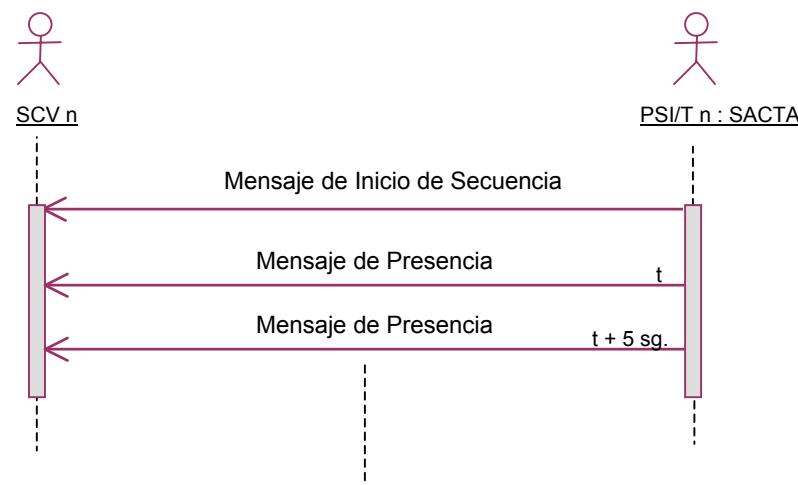


Figura 2.7 - Intercambio del mensaje de presencia SACTA → SCV

El contenido de los campos del mensaje se indica en la tabla adjunta:

CAMPO	CONTENIDO	TAMAÑO	
DOMINIO ORIGEN	“1” (01 Hex.) = OPERACIONAL	1 byte	
CENTRO ORIGEN	Número asignado en archivos de configuración.	1 byte	
USUARIO ORIGEN	“X” (XX XX Hex.) = PSI/T1 ó “X” (XX XX Hex.) = PSI/T2 ó “X” (XX XX Hex.) = PSI/T3 ó “X” (XX XX Hex.) = PSI/T4 ó “X” (XX XX Hex.) = PSI/T5 ó “X” (XX XX Hex.) = PSI/T6 ó “X” (XX XX Hex.) = PSI/T7 ó “X” (XX XX Hex.) = PSI/T8	2 bytes	
DOMINIO DESTINO	“1” (01 Hex.) = OPERACIONAL	1 byte	
CENTRO DESTINO	Número asignado en archivos de configuración.	1 byte	
USUARIO DESTINO	ACC y T-ACC: “X” (XX XX Hex.) = SCV1	TWR: “X” (XX XX Hex.)= SCV1 ó “X” (XX XX Hex.) = SCV2 ó “X” (XX XX Hex.) = SCV3 ó “X” (XX XX Hex.)= SCV4 ó “X” (XX XX Hex.) = SCV5	2 bytes
SESIÓN	0	2 bytes	
TIPO DE MENSAJE	“1530” (05 FA Hex.) = Mensaje de Presencia	2 bytes	
OPCIÓN DE SECUENCIA	“000” = Datos	3 bits	
NÚMERO DE SECUENCIA	(Secuencia 0..287)	13 bits	
LONGITUD	11	2 bytes	
HORA	Hora UNIX del mensaje.	4 bytes	
NUMERO DE CARACTERES DEL TIPO DE PROCESADOR	3	2 bytes	
TIPO PROCESADOR	“PSI” + 1 Nulo + No usado (CÓDIGO ASCII) (505349 + 00 + XXXXXXXXXXXX Hex.)	10 bytes	
NÚMERO PROCESADOR	1,2,3,4,5,6,7 u 8	2 bytes	
NO USADO	0	2 bytes	
ESTADO PROCESADOR	1 (Disponible)	1 byte	
SUBESTADO PROCESADOR	0 (No tiene)	1 byte	
TIEMPO DE INFORME (segundos)	5	2 bytes	
TIEMPO MÁXIMO DE INFORME (seg.)	30	2 bytes	

Tabla 2.5 - Formato del mensaje de presencia SACTA → SCV

2.7.4.5.MENSAJE DE PETICIÓN DE SECTORIZACIÓN SCV → SACTA

Este mensaje lo enviará cada SCV en **multicast** al “Grupo de PSI/Ts”, para solicitar cuál es la sectorización vigente en SACTA (ya que la desconoce en ese momento).

El SCV enviará el “*mensaje de petición de sectorización SCV → SACTA*”:

- En el momento del arranque (después del mensaje de inicio de secuencia), ver **Figura 2.8**.
- En el momento de detectar la recuperación del enlace con SACTA (cuando previamente se hayan sobrepasado 30 segundos sin recibir presencia de las PSI/Ts), y después del mensaje de inicio de secuencia. Ver **Figura 2.8**.

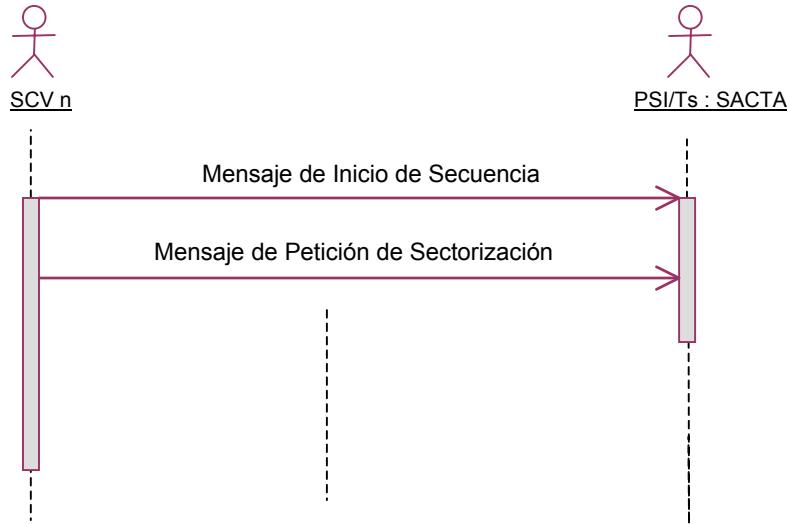


Figura 2.8 - Intercambio del mensaje de petición de sectorización SCV → SACTA

Este mensaje lo enviará cada SCV en **multicast** al “Grupo de PSI/Ts” por lo que el SCV recibirá una contestación de cada una de las PSI/Ts que se encuentre operativa en el sistema (nunca del “Grupo de PSI/Ts”). Este mensaje no tiene datos adjuntos, su recepción por una PSI/T provocará el envío de la sectorización vigente en SACTA al SCV que realizó la petición. Los mecanismos de coherencia implementados en SACTA evitarán la recepción por parte del SCV de sectorizaciones distintas desde cada PSI/T.

El contenido de los campos del mensaje se indica en la tabla adjunta:

CAMPO	CONTENIDO		TAMAÑO
DOMINIO ORIGEN	“1” (01 Hex.) = OPERACIONAL		1 byte
CENTRO ORIGEN	Número asignado en archivos de configuración.		1 byte
USUARIO ORIGEN	ACC y T-ACC: “X” (XX XX Hex.) = SCV1	TWR: “X” (XX XX Hex.) = SCV1 ó “X” (XX XX Hex.) = SCV2 ó “X” (XX XX Hex.) = SCV3 ó “X” (XX XX Hex.) = SCV4 ó “X” (XX XX Hex.) = SCV5	2 bytes
DOMINIO DESTINO	“1” (01 Hex.) = OPERACIONAL		1 byte
CENTRO DESTINO	Número asignado en archivos de configuración.		1 byte
USUARIO DESTINO	“X” (XX XX Hex.) = Grupo de PSI/Ts		2 bytes
SESIÓN	0		2 bytes
TIPO DE MENSAJE	“707” (02 C3 Hex.) = Mensaje de Petición de Sectorización		2 bytes
OPCIÓN DE SECUENCIA	“000” = Datos		3 bits
NÚMERO DE SECUENCIA	(Secuencia 0..287)		13 bits
LONGITUD	0		2 bytes
HORA	Hora UNIX del mensaje.		4 bytes

Tabla 2.6 - Formato del mensaje de petición de sectorización

2.7.4.6. MENSAJE DE SECTORIZACIÓN SACTA → SCV

Este mensaje se enviará desde cualquiera de las PSI/Ts (PSI/T1, PSI/T2, PSI/T3, PSI/T4, PSI/T5, PSI/T6, PSI/T7 y PSI/T8) operativas en SACTA, en **unicast**.

SACTA enviará el “*mensaje de sectorización SACTA → SCV*”:

- Con el fin de implantar una nueva sectorización en el sistema SCV, con lo cual el mensaje será enviado por aquella PSI/T desde la cual el operador implantó la sectorización en SACTA hacia cada SCV que se encuentre configurado, ver **Figura 2.9**.
- Como respuesta al mensaje de petición de sectorización de un determinado SCV, con lo cual, será enviado un mensaje de sectorización por cada una de las PSI/Ts que se encuentran operativas en SACTA a dicho SCV, ver **Figura 2.10**.

La sectorización que el SCV implantará será siempre la última recibida desde SACTA, independientemente del estado en que se encuentre el SCV en el momento de recibir dicha sectorización (estado de los recursos físicos del sistema, estado de las comunicaciones, conmutación de sistema, procesamiento de una sectorización anterior, etc).

Ante la recepción de una sectorización desde SACTA que coincide con la sectorización vigente, el SCV no deberá implantar dicha sectorización por coincidir con la que ya se encuentra operativa en el mismo.

Cuando en la sectorización recibida desde SACTA, no se encuentren todos los sectores u objetos de responsabilidad configurados para dicha dependencia, el SCV no implantará dicha sectorización y mantendrá la sectorización anterior.

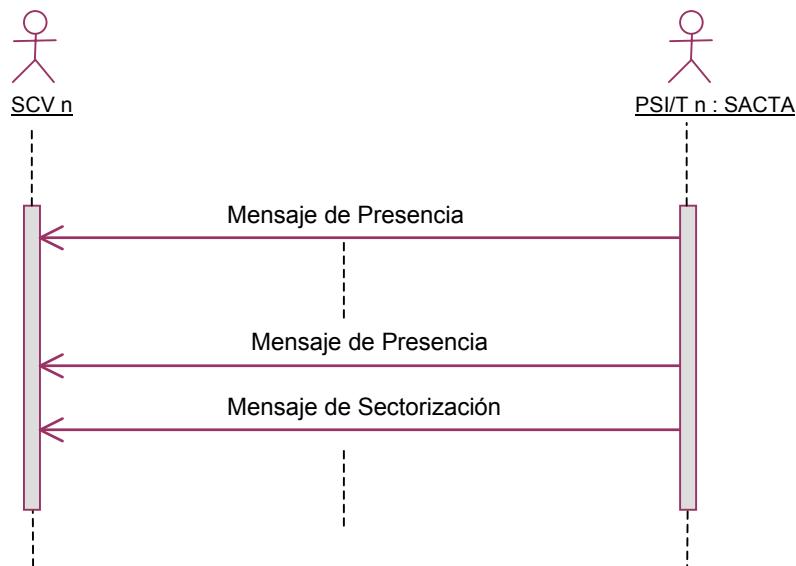


Figura 2.9 - Intercambio del mensaje de sectorización SACTA → SCV (Caso 1)

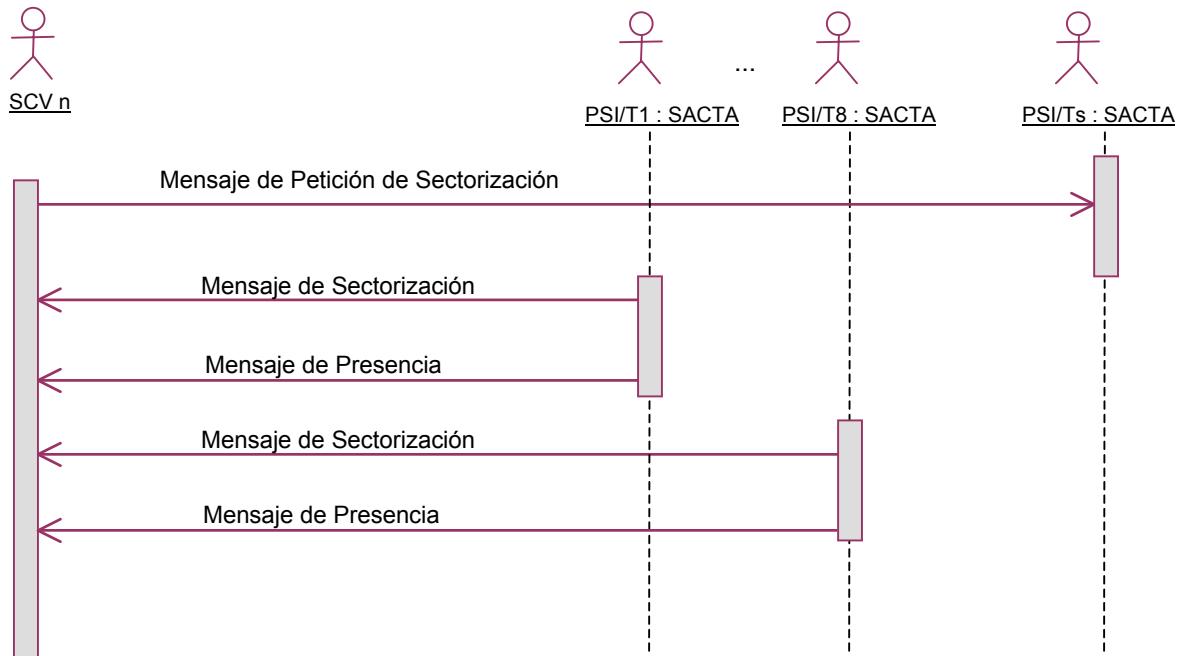


Figura 2.10 - Intercambio del mensaje de sectorización SACTA → SCV (Caso 2)

El contenido de los campos del mensaje de sectorización se indica en la tabla adjunta:

CAMPO	CONTENIDO	TAMAÑO
DOMINIO ORIGEN	“1” (01 Hex.) = OPERACIONAL	1 byte
CENTRO ORIGEN	Número asignado en archivos de configuración.	1 byte
USUARIO ORIGEN	“X” (XX XX Hex.) = PSI/T1 ó “X” (XX XX Hex.) = PSI/T2 ó “X” (XX XX Hex.) = PSI/T3 ó “X” (XX XX Hex.) = PSI/T4 ó “X” (XX XX Hex.) = PSI/T5 ó “X” (XX XX Hex.) = PSI/T6 ó “X” (XX XX Hex.) = PSI/T7 ó “X” (XX XX Hex.) = PSI/T8	2 bytes
DOMINIO DESTINO	“1” (01 Hex.) = OPERACIONAL	1 byte
CENTRO DESTINO	Número asignado en archivos de configuración	1 byte
USUARIO DESTINO	ACC y T-ACC: “X” (XX XX Hex.) = SCV1 “X” (XX XX Hex.) = SCV2 ó “X” (XX XX Hex.) = SCV3 ó “X” (XX XX Hex.) = SCV4 ó “X” (XX XX Hex.) = SCV5	2 bytes
SESIÓN	0	2 bytes
TIPO DE MENSAJE	“1632” (06 60 Hex.) = Mensaje de Sectorización	2 bytes
OPCIÓN DE SECUENCIA	“000” = Datos	3 bits
NÚMERO DE SECUENCIA	(Secuencia 0..287)	13 bits
LONGITUD	4 + (4 x número de sectores / objetos de responsabilidad)	2 bytes
HORA	Hora UNIX del mensaje.	4 bytes
VERSIÓN DE LA SECTORIZACIÓN	(versión)	4 bytes
NO USADO	0	2 bytes
NÚMERO DE SECTORES / OBJETOS DE RESPONSABILIDAD	N (Número de total de Sectores u Objetos de Responsabilidad configurados en el centro)	2 bytes
SECTORES / OBJETOS DE RESPONSABILIDAD	Conjunto de sectores / objetos de responsabilidad (el contenido para cada sector / objeto de responsabilidad se indica en la)	N * 8 bytes

CAMPO	CONTENIDO	TAMAÑO
	siguiente tabla)	

Tabla 2.7 - Formato del mensaje de sectorización

Para cada sector / objeto de responsabilidad: 8 bytes

CAMPO	TAMAÑO
PCV SACTA LÓGICA (No usado por el SCV; interno SACTA)	1 byte
NO USADO	1 byte
CÓDIGO SCV DEL SECTOR / OBJETO DE RESPONSABILIDAD (En código ASCII)	4 bytes
NÚMERO DE UCS / POSICIÓN (Relativo al Grupo de Posiciones ≡ Tipo de Posición) Remota = 1 – 20 Ruta = 1 – 30 TMA = 1 – 20 Torre = 1 – 50	1 byte
TIPO DE POSICIÓN (Grupo: Remota = 0; Ruta =1; TMA = 2; Reservado -POS_TMA2- = 3; Torre = 4)	1 byte

Tabla 2.8 - Formato del campo de Sectores / Objetos de Responsabilidad del mensaje de sectorización

Nota: En el caso de coexistir varios SCVs de TWR conectados a la misma red SACTA, la sectorización que este enviará a cada uno de los SCVs, será la misma y contendrá todos los sectores/objetos de responsabilidad y posiciones integrantes de este conjunto de SCVs o centro.

2.7.4.7. MENSAJE DE RESPUESTA DE SECTORIZACIÓN SCV → SACTA

Este mensaje se enviará desde el SCV en **multicast** al grupo de PSI/Ts para informar sobre el resultado de la última sectorización solicitada.

El SCV enviará el “*mensaje de respuesta de sectorización SCV → SACTA*”:

- En multicast al “grupo de PSI/Ts” como respuesta a la sectorización enviada desde la PSI/T desde la cual el operador implantó la sectorización en SACTA ver **Figura 2.11**.
- Como respuesta a los mensajes de sectorización enviados por todas aquellas PSI/Ts que han respondido al mensaje de petición de sectorización recibido desde un SCV. En este caso, el SCV enviará un único mensaje de respuesta de sectorización, en multicast al “grupo de PSI/Ts”, independientemente del número de mensajes de sectorización que reciba de las PSI/Ts, ver **Figura 2.12**.

Este mensaje contendrá información sobre el resultado de la sectorización en el SCV y lo enviará el SCV siempre como respuesta a un mensaje de sectorización. Si no se devuelve “sectorización implantada”, las PSI/Ts generarán el Registro Histórico de código PSIsrv001.

En el caso de que una sectorización enviada por SACTA coincida con la implantada en el SCV, este no realizará el proceso de sectorización, pero devolverá a SACTA "sectorización implantada".

Cuando en la sectorización recibida desde SACTA, no se encuentren todos los sectores u objetos de responsabilidad configurados para dicha dependencia, el SCV no implantará dicha sectorización y devolverá a SACTA "sectorización rechazada".

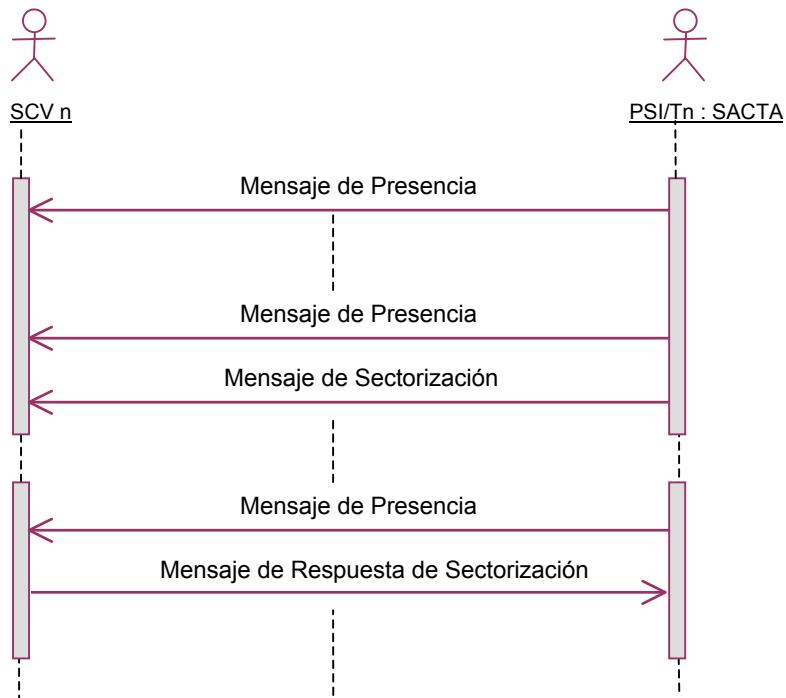


Figura 2.11 - Intercambio del mensaje de respuesta de sectorización SCV → SACTA (Caso 1)

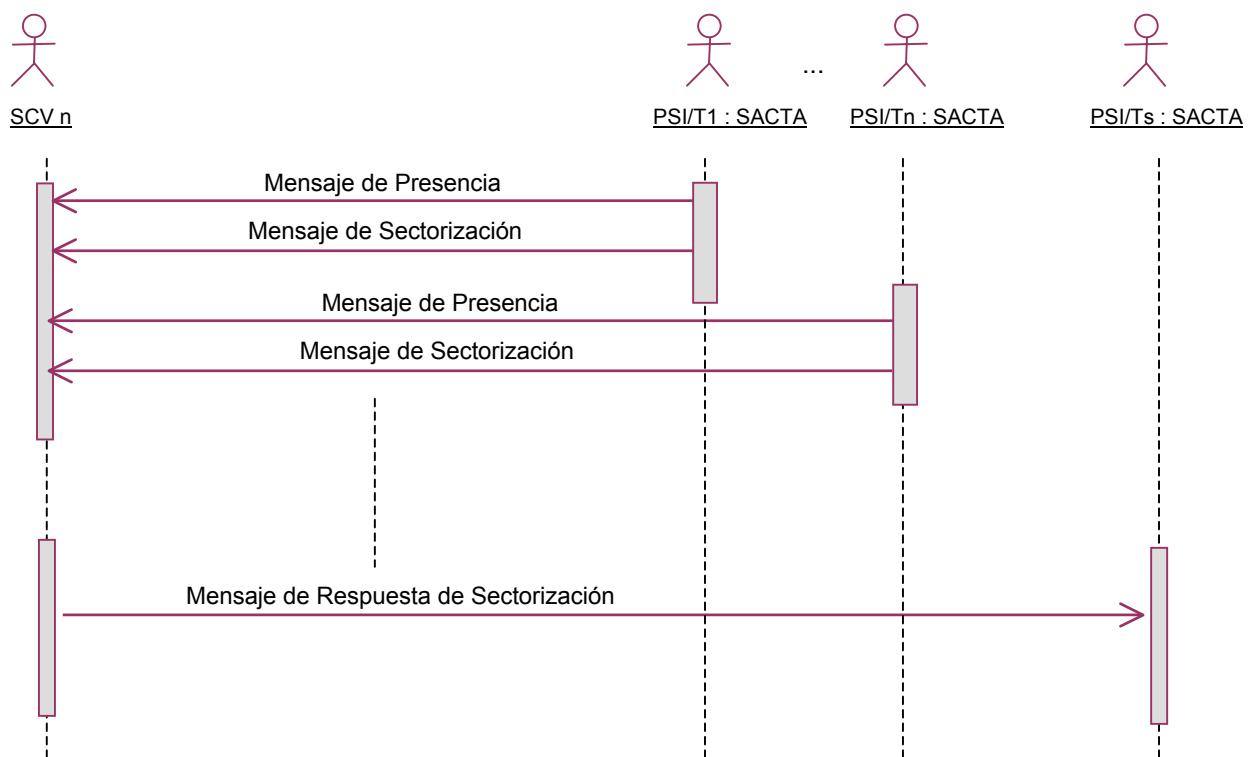


Figura 2.12 - Intercambio del mensaje de respuesta de sectorización SCV → SACTA (Caso 2)

El contenido de los campos del mensaje de respuesta de sectorización se indica en la tabla adjunta:

CAMPO	CONTENIDO		TAMAÑO
DOMINIO ORIGEN	“1” (01 Hex.) = OPERACIONAL		1 byte
CENTRO ORIGEN	Número asignado en archivos de configuración.		1 byte
USUARIO ORIGEN	ACC y T-ACC: “X” (XX XX Hex.) = SCV1 “X” (XX XX Hex.) = SCV2 “X” (XX XX Hex.) = SCV3 “X” (XX XX Hex.) = SCV4 “X” (XX XX Hex.) = SCV5	TWR: “X” (XX XX Hex.)= SCV1 ó “X” (XX XX Hex.) = SCV2 ó “X” (XX XX Hex.) = SCV3 ó “X” (XX XX Hex.)= SCV4 ó “X” (XX XX Hex.) = SCV5	2 bytes
DOMINIO DESTINO	“1” (01 Hex.) = OPERACIONAL		1 byte
CENTRO DESTINO	Número asignado en archivos de configuración.		1 byte
USUARIO DESTINO	“X” (XX XX Hex.) = Grupo de PSI/Ts		2 bytes
SESIÓN	0		2 bytes
TIPO DE MENSAJE	“710” (02 C6 Hex.) = Mensaje de Respuesta de Sectorización		2 bytes
OPCIÓN DE SECUENCIA	“000” = Datos		3 bits
NÚMERO DE SECUENCIA	(Secuencia 0..287)		13 bits
LONGITUD	3		2 bytes
HORA	Hora UNIX del mensaje.		4 bytes
VERSIÓN DE LA SECTORIZACIÓN	(versión)		4 bytes
RESULTADO	<ul style="list-style-type: none"> • “0” (00 Hex.) = RECHAZADA • “1” (01 Hex.) = IMPLANTADA 		1 byte
NO USADO	0		1 byte

Tabla 2.9 - Formato del mensaje de respuesta de sectorización

3. INFORMACIÓN COMPARTIDA SACTA-SCV

Toda la información que sea compartida entre SACTA y SCV o sea necesaria para su configuración, ha de ser coherente en ambos Sistemas. Por ello, cuando esta información sea modificada, dicha modificación deberá realizarse simultáneamente en los dos Sistemas.

Esta información es la siguiente:

- Direccionamiento IP del centro (ver apartado 2.5). Este se encuentra definido en los documentos RDN_IP_031127 Plan de Numeración IP de Redes conectadas con REDAN [véase Ref. 6], Plan de Numeración IP de Redes SACTA III.5. [véase Ref. 7], y Plan de numeración IP de redes SCV [véase Ref. 8].
- Número identificador del Dominio. Utilizado en las cabeceras de los mensajes (ver apartado 2.7.3) en los campos dominio origen y dominio destino. Dicho número se especifica en el apartado 2.7.3 de este documento.
- Número identificador del Centro. Utilizado en las cabeceras de los mensajes (ver apartado 2.7.3) en los campos centro origen y centro destino. Dicho número se define en el documento SACTA v3.4 [véase Ref. 1] y se encuentra especificado en el archivo de configuración COM_IP_CENTROS.CFG / COM_IP_CENTROS.CFG_twr de SACTA v3.4.

- Número identificador del usuario. Utilizado en las cabeceras de los mensajes (ver apartado 2.7.3) en los campos usuario origen y usuario destino. Dicho número se define en el apartado 2.7 de este documento y se encuentra especificado en el archivo de configuración COM_USUARIOS.CFG de SACTA v3.5.
- Identificador del tipo de mensaje. Utilizado en las cabeceras de los mensajes (ver apartado 2.7.3) en el campo Tipo de Mensaje. Dicho número se especifica en el apartado 2.7.3 de este documento.
- Número de opción de secuencia. Utilizado en las cabeceras de los mensajes (ver apartado 2.7.3) en el campo Opción de Secuencia. Dicho número se especifica en el apartado 2.7.3 de este documento.

Los datos que se especifican a continuación, varían con la creación/borrado de Sectores/Objetos de Responsabilidad, UCSs, cambio de nombre de Sectores/Objetos de Responsabilidad y modificación del tipo de las Posiciones. Por ello, esta información será coordinada por el personal de los Departamentos de Sistemas y de Comunicaciones del Centro de Control correspondiente:

- Número de Sectores/Objetos de Responsabilidad de la dependencia. Utilizado en los mensajes de sectorización en el campo Sectores/Objetos de Responsabilidad (ver Tabla 2.7). El número de Sectores/Objetos de Responsabilidad debe ser el mismo en SACTA y en SCV.
- Código SCV-OR de cada Sector/Objeto de Responsabilidad. Utilizado en el campo de datos del mensaje de sectorización (ver **Tabla 2.8**). El código SCV-OR es un valor numérico y la correspondencia entre un Sector/Objeto de Responsabilidad y su código SCV (contenido en el mensaje de sectorización) debe ser igual en ambos Sistemas.
- Número de UCS/Posición y Tipo de Posición. Utilizados en el campo de datos del mensaje de sectorización (ver **Tabla 2.8**). La correspondencia entre una Posición física y el número y tipo que la identifica en el mensaje de sectorización debe ser coherente en los dos Sistemas.
- Numeración de las posiciones de control de los SCVs de TWR, en caso de coexistir varios SCVs de este tipo conectados a la misma red SACTA. Esta numeración ha de ser diferente entre las posiciones de estos SCVs, debido a que cada uno de estos recibe de SACTA una sectorización global con los sectores y posiciones correspondientes al conjunto de los SCVs. Cada uno de los SCVs filtrará el mensaje de sectorización recibido, extrayendo la parte del mensaje que corresponde a las posiciones de control definidas para ese SCV y se implantará la sectorización correspondiente a cada SCV.

**ANEXO A. INTRODUCCIÓN AL MODELO CONCEPTUAL PARA
SACTA 3.5**

1. INTRODUCCIÓN

Para la especificación de la versión SACTA 3.5 se identificaron una serie de objetivos de evolución que requerían una redefinición de las responsabilidades de control, los recursos de control y las relaciones entre ellos manejadas por el sistema. Estas definiciones se agruparon bajo la denominación de Modelo Conceptual [PC_723_ESPEC120303(90).doc].

El proceso de especificación e implementación de la versión 3.5 ha requerido recortar parcialmente los objetivos previstos, por lo que la aplicación efectiva del Modelo Conceptual en la versión 3.5 estará limitada a lo indicado en el documento ARQ-R6.5-MIN_ESPEC221004.doc. Sin embargo, en toda la especificación de la versión 3.5 se aplicará la nomenclatura en él recogida, cuyas equivalencias con los conceptos utilizados actualmente se establecerán en este documento.

En los apartados sucesivos se describen los conceptos manejados, las capacidades previstas y la equivalencia con los conceptos actualmente existentes en el sistema. Los conceptos se han organizado en tres grupos: los que definen y agrupan las responsabilidades de control, los que definen y agrupan los recursos de control (HW y SW) que asistirán al controlador en el cumplimiento de las responsabilidades de control que tienen asignadas y los que establecen las relaciones entre los dos anteriores.

2. DIAGRAMA

El siguiente diagrama (Figura A.1) establece las relaciones entre los distintos conceptos que se van a presentar.

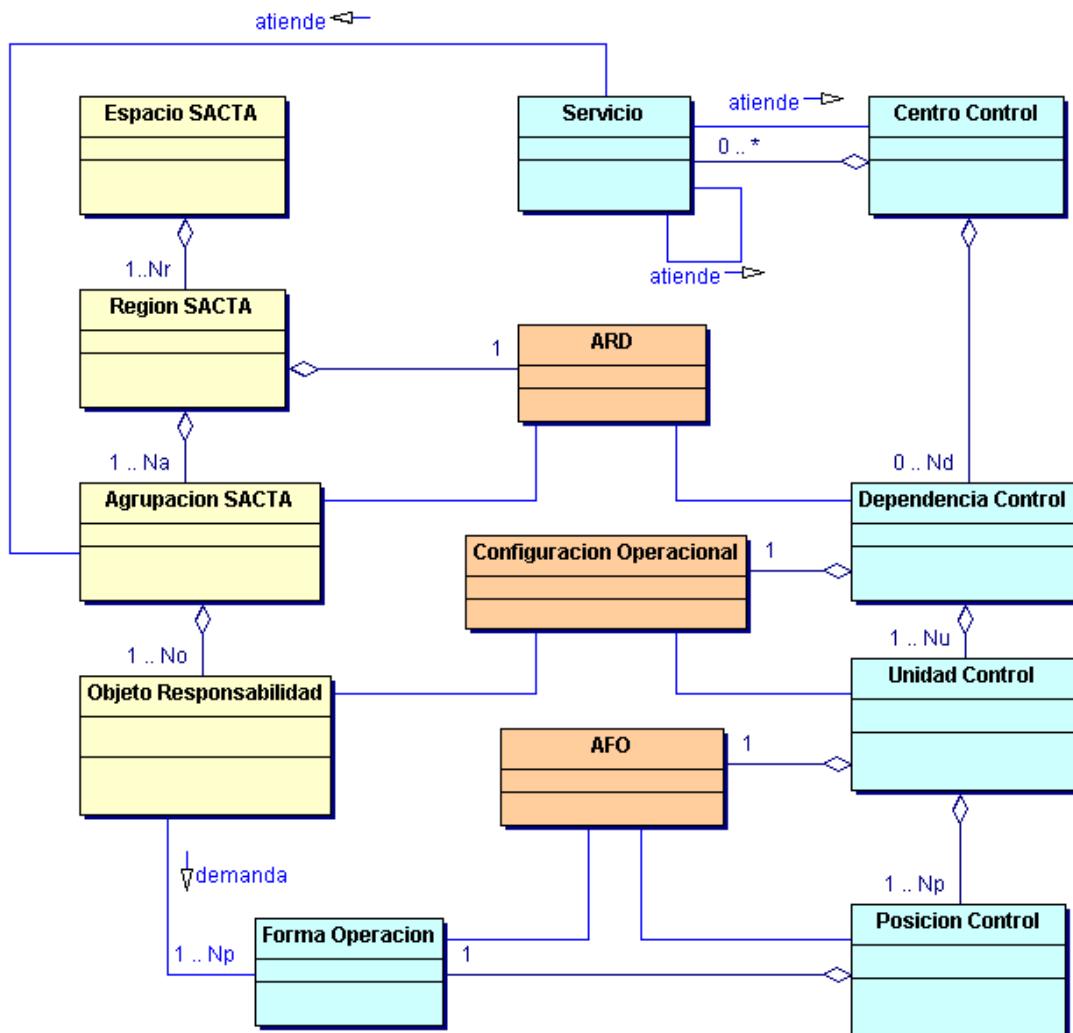


Figura A.1

3. RESPONSABILIDADES DE CONTROL

3.1. Espacio SACTA

Espacio SACTA será el conjunto de responsabilidades de control sobre un espacio geográfico. El espacio **SACTA** se caracteriza por estar soportado por un único sistema SACTA.

*Actualmente existen dos **espacios SACTA**: Península + Baleares y Canarias.*

3.2. Región SACTA

Una **región SACTA** es un conjunto de responsabilidades de control, pertenecientes al mismo **espacio SACTA**, que comparten algún elemento que da coherencia entre ellas. El número máximo de **regiones SACTA** que componen un **espacio SACTA** será 6 y el mínimo 1.

*En la actualidad, existen 5 **regiones SACTA**: Barcelona, Canarias, Madrid, Palma y Sevilla.*

3.3. Agrupación SACTA

Se trata de cada uno de los subconjuntos de responsabilidades de control que componen una misma **región SACTA** que compartirán una serie de características tanto estáticas (datos de adaptación) como dinámicas (configuraciones, servicios que las atienden...). Una **agrupación SACTA** no está necesariamente caracterizada por el tipo de control que se presta en ella (Ruta, TMA o Torre), aunque esta característica será normalmente la que determine la creación de **agrupaciones SACTA**. El número de **agrupaciones SACTA** que forman una **región SACTA** estará comprendido entre 1 y 50.

A modo de ejemplo, en la región SACTA “Barcelona” se tendrán las siguientes agrupaciones SACTA: Ruta Barcelona, TMA Barcelona, CAO Barcelona, TMA Valencia, TWR Barcelona, TWR Valencia, TWR Alicante, etc.

3.4. Objeto de Responsabilidad

Un **objeto de responsabilidad** es una responsabilidad de control indivisible. Los **objetos de responsabilidad** se caracterizan por un espacio geográfico concreto, y por una característica o regla que deben cumplir los vuelos que estén asignados a dicha responsabilidad de control. Los **objetos de responsabilidad** serán disjuntos entre sí de manera que un mismo punto del espacio no podrá pertenecer simultáneamente a dos **objetos de responsabilidad** para la misma característica o regla del vuelo. Una **agrupación SACTA** tendrá un mínimo de 1 y un máximo de 50 **objetos de responsabilidad**.

Los Objetos de Responsabilidad se corresponderán con los actuales sectores SACTA salvo para las Agrupaciones SACTA de TWR que dispongan de un servidor específico de Plan de Vuelo (TPVT). En este último caso el actual sector SACTA pasará a constituir la Agrupación SACTA y se definirán objetos de responsabilidad específicos de los tipos Autorizaciones, Rodadura, Local ó Aproximación.

4. RECURSOS DE CONTROL

4.1. Centro de Control

Se trata de un conjunto de recursos de control que comparten un servicio de comunicaciones locales común. Un **centro de control** puede ubicar hasta 6 **dependencias de control** y un conjunto de **servicios**.

A modo de ejemplo, mientras que el ACC Madrid es un único Centro de Control, el Centro de Control TWR Barajas comprende las TWRS Norte y Sur de Barajas.

4.2. Servicios

El concepto de **servicio** integra a las diferentes funciones que residen en los servidores actuales, y a otras funciones distribuidas como la supervisión. Los **servicios** residen en un **centro de control** determinado, pero proporcionan su funcionalidad a: **Centros de control, Dependencias de control, Otros Servicios**, etc.

Una lista de servicios del sistema actual sería: TCPV, TLPV, TCMT, TLMT, TDVM, GIPV, GSI, EDR (UAST+UDDE), SPV, SDL, SDV, SIA, SDR, SPIVL, SIS, ...

4.3. Dependencia de Control

Se trata de un subconjunto de recursos de control de un mismo **centro de control** que podrán tener asignados **objetos de responsabilidad** que compartan una serie de características estáticas (datos de adaptación). Una **dependencia de control** no está necesariamente caracterizada por la homogeneidad del HW y de la configuración de todos los recursos que la componen, aunque esta característica será normalmente la que determine la creación de **dependencias de control**. El número de **dependencias de control** que forman un **centro de control** estará comprendido entre 0 y 6.

A modo de ejemplo, en el centro de control del ACC Barcelona están ubicadas las siguientes dependencias de control: Ruta Barcelona, TMA Barcelona y CAO Barcelona.

4.4. Unidad de Control

Una **unidad de control** es un conjunto de **recursos de control** disponibles en una **dependencia de control** para atender a los **objetos de responsabilidad** que se les asignen de entre los pertenecientes a las **agrupaciones SACTA** asignadas a dicha **dependencia de control**. Una **dependencia de control** tendrá un número de **unidades de control** desde 1 a un máximo de 60.

Las unidades de control se corresponderán con las actuales UCSs para las dependencias de control de Ruta y TMA. Para las dependencias de control de TWR y APP sin servidor específico de Plan de Vuelo (TPVT), la unidad de control la constituirá el conjunto de recursos que están asociados a una misma remota lógica (POS TOR, IFV, UCS REM). Para las Agrupaciones SACTA de TWR que dispongan de un servidor específico de Plan de Vuelo (TPVT), cada POS TOR constituirá una unidad de control.

4.5. Posición de Control

Una **posición de control** corresponde a la posición de usuario propiamente dicha. Es el puesto de trabajo desde el que el controlador dialoga con el sistema. El número máximo de **posiciones de control** en una **unidad de control** será 2. El número máximo de **posiciones de control** en un mismo **centro de control** será 150.

Las posiciones de control se corresponderán con las actuales POS A y POS B para las dependencias de control de Ruta y TMA.

Para las dependencias de control de TWR y APP sin servidor específico de Plan de Vuelo (TPVT), aunque podrán asignarse hasta 25 POS TOR por cada remota lógica, se comportarán como una única posición de control.

Para las Agrupaciones SACTA de TWR que dispongan de un servidor específico de Plan de Vuelo (TPVT), cada POS TOR constituirá una unidad de control.

4.6. Forma de Operación

Cada **posición de control** tendrá una **forma de operación**, es decir, tendrá una disposición particular de los recursos gráficos y operativos que posibilite y favorezca la labor del controlador para desarrollar un rol o unos roles determinados y vendrá fijada por los objetos de responsabilidad asignados a la unidad de control a la que pertenece la posición de control. Cada **objeto de responsabilidad** demandará una serie de **formas de operación**, de 1 a 2.

Las posiciones de control de Ruta y TMA podrán adoptar las siguientes formas de operación: Ejecutivo, Planificador, Integrado y No Operacional

Las posiciones de control de TWR y APP sin servidor específico de Plan de Vuelo (TPVT) podrán adoptar las siguientes formas de operación: Integrada y No Operacional.

Las posiciones de control de las Agrupaciones SACTA de TWR que dispongan de un servidor específico de Plan de Vuelo (TPVT), podrán adoptar las siguientes formas de operación: Autorizaciones, Rodadura, Local y APP e Integradas (Autorizaciones + rodadura + local, Autorizaciones + rodadura, Rodadura + local, Local + app y Autorizaciones + rodadura + local + app).

5. RELACIONES ENTRE RESPONSABILIDADES DE CONTROL Y RECURSOS DE CONTROL

5.1. Asignación de Responsabilidades a Dependencias (ARD)

Establece la relación entre las **agrupaciones SACTA** de una **región SACTA** y las **dependencias de control** definidas para toda la región SACTA.

En la actualidad cada dependencia de control tendrá asignada una y sólo una agrupación SACTA de forma estática, que vendrá dada por el conjunto de sectores SACTA que tiene asignados.

5.2. Configuración Operacional

Establece la relación entre los objetos de responsabilidad de la agrupación (o las agrupaciones SACTA) asignadas a la dependencia de control y las unidades de control de dicha dependencia de control. Una unidad de control podrá no tener asignado ningún objeto de responsabilidad, pero todos los objetos de responsabilidad deberán estar asignados a alguna unidad de control. En la función que modifica una configuración operacional se podrán establecer restricciones. Por ejemplo, para que un objeto de responsabilidad nunca quede aislado en una unidad de control (sectores no

autónomos que pertenecen a varios sectores operativos), o para que ciertos objetos de responsabilidad no puedan agruparse en una misma unidad de control (núcleos).

Este concepto se corresponde con la actual sectorización para las dependencias de control de Ruta, TMA y TWR/APP sin servidor específico de Plan de Vuelo (TPVT). Para las dependencias de control de torre con servidor específico de plan de vuelo (TPVT) se corresponde con la función de configuración operacional.

Las únicas restricciones a la asignación de objetos de responsabilidad implementadas son las debidas a los núcleos.

5.3. Asignación de Formas de Operación (AFO)

Existirá una asignación de formas de operación para cada unidad de control. De esta manera se asignarán las formas de operación que demandan los objetos de responsabilidad asignados a la unidad de control a las diferentes posiciones de control.

La asignación de formas de operación seguirá ciertas reglas. Actualmente, estas reglas obligan al agrupamiento de las formas de operación ejecutivas en la misma posición de control o a la asignación de la forma de operación “no operacional” a una posición de control cuando:

- *La unidad de control a la que pertenece no tiene asignado ningún objeto de responsabilidad.*
- *El total de las formas de operación están asignadas a otras posiciones de control de la misma unidad de control.*

Pliego de Prescripciones Técnicas:

Desarrollo e implantación de Interfaz SCV-SACTA en Torres con Servicio de Aproximación

ANEXO III

Requisitos Seguridad (Safety) División de Comunicaciones

**Asistencia para el Desarrollo e
Implantación de Interfaz SCV-SACTA en
Torres con Servicio de Aproximación**

[Requisitos de Seguridad \(Safety\) – Interfaz SCV-SACTA](#)

ÍNDICE

1. Objeto.....	3
2. Ámbito de Aplicación	3
3. Documentación de Referencia y Normativa aplicable	4
4. Terminología y definiciones.....	5
4.1. Definiciones	5
4.2. Acrónimos.....	7
5. Plan de Gestión de la Seguridad (Safety)	7
6. Análisis de Seguridad (Safety) del Servicio	8
6.1. Evidencia de cumplimiento de los RSG y RSE	9
6.2. Requisitos de Seguridad Generales (RGS)	12
6.3. Requisitos de Seguridad Específicos (RSE)	19
6.3.1. Requisitos de Garantía del Software (SW)	21
7. Fichas de Divulgación en materia de Seguridad Operacional	24

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

1. Objeto

El objeto de este documento es determinar los requisitos de seguridad generales (RSG), específicos (RSE) y de interlocutores (RSI) que deben incluirse en el pliego de prescripciones técnicas del **Asistencia para el Desarrollo e Implementación de Interfaz SCV-SACTA en Torres con Servicio de Aproximación**, así como la definición de las evidencias que el potencial proveedor exterior debe proporcionar para demostrar el cumplimiento de los requisitos de seguridad establecidos.

De este modo se documentan las actividades de garantía de seguridad AGS2 y AGS3 indicadas en la Instrucción de trabajo para la garantía de seguridad de los servicios y suministros exteriores de ENAIRe [2], una vez que la División de Comunicaciones (COMU) ha valorado que el servicio exterior (ver definiciones en el punto 4 sí puede tener impacto sobre la seguridad operacional de los servicios prestados por ENAIRe. Garantizando de este modo que se acredita la seguridad de los servicios y suministros exteriores.

2. Ámbito de Aplicación

El contenido de este Anexo es de aplicación al potencial proveedor exterior y al que finalmente resulte adjudicatario del expediente de **Asistencia para el Desarrollo e Implementación de Interfaz SCV-SACTA en Torres con Servicio de Aproximación**.

Todas las relaciones contractuales de la División de Comunicaciones, con los proveedores de servicios o suministros exteriores deberán garantizar el correcto funcionamiento del Sistema de Gestión de Seguridad de ENAIRe, garantizando que los peligros para la seguridad de la aviación que impliquen sus actividades sean identificados y evaluados, y se gestionen y mitiguen los riesgos asociados, además de que se garantice que las actividades que realice sean conformes a los requisitos aplicables, tal y como establece el Reglamento (UE) 2017/373 [9].

Este Anexo describe todos los requisitos para garantizar la seguridad de los servicios exteriores y que serán exigibles al proveedor exterior:

- Requisitos de Seguridad Generales (RSG)
- Requisitos de Seguridad Específicos (RSE)
- Requisitos de Seguridad de Interlocutores (RSI) – **NO APICAN A ESTE PPT.**

Todos los servicios y suministros (materiales y no materiales) que contribuyan a la prestación de servicios ATM, CNS o AIS proporcionados directamente por la Dirección de Servicios de Navegación Aérea de ENAIRe donde se establezcan contactos formales con proveedores externos les será de aplicación el contenido de este anexo.

El proveedor exterior con el que se formaliza el contacto formal será el responsable de cumplir los requisitos de seguridad que le sean aplicables, así como obtener las evidencias de cumplimiento correspondientes para facilitárselas a ENAIRe en el momento que corresponda sin que sea necesario solicitárselas.

Este Anexo pretende ser una guía orientativa para ayudar al proveedor exterior definiendo la forma más clara y eficiente de documentar el cumplimiento de los requisitos de seguridad exigidos en el expediente en las distintas fases del servicio.

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

El servicio se define que al menos pasa por las siguientes fases:

- **Definición y Oferta:** Desde que se origina la necesidad de un servicio exterior hasta que ésta se plasma en un contacto formal.
- **Previo al inicio:** Desde que se establece el contacto formal con el proveedor exterior hasta el inicio de las tareas del servicio contratado.
- **Ejecución:** Desde el inicio efectivo del servicio contratado hasta su finalización formal, entendiendo como tal el momento en el que se firma el acta de extinción de la relación definitiva o equivalente.

3. Documentación de Referencia y Normativa aplicable

Documentación Interna – ENAIRe

[1]	A111-19-PES-005: Procedimiento de control y mitigación del riesgo en relación con interfaces formales y actividades contratadas que puedan afectar a la seguridad. ¡NUEVO!
[2]	A111b-12-INS-001: Instrucción de trabajo para la garantía de seguridad de los servicios y suministros exteriores. Nota: Esta instrucción estará vigente hasta que sea actualizada por la nueva instrucción A111-19-INS-004.
[3]	A111-19-PES-001: Procedimiento específico para la elaboración de estudios de seguridad. ¡NUEVO!
[4]	A111-19-PES-003: Procedimiento para la elaboración de evaluaciones de seguridad del soporte (Safety Support assessments) para cambios relacionados con la provisión de servicios No ATS. ¡NUEVO!
[5]	A111-19-INS-002: Instrucción para la garantía de la seguridad del Software. ¡NUEVO!

Documentación Externa – Reglamentos y Estándares aplicables

[6]	Reglamento (CE) 550/2004 relativo a la prestación de servicios de navegación aérea en el cielo único europeo.
[7]	Reglamento (UE) Nº 1035/2011 por el que se establecen requisitos comunes para la prestación de servicios de navegación aérea. Nota: Este reglamento está derogado por el (UE) 2017/373.
[8]	Reglamento (CE) Nº 482/2008 por el que se establece un sistema de garantía de la seguridad del software que deberán implantar los proveedores de servicios de navegación aérea. Nota: Este reglamento está derogado por el (UE) 2017/373.
[9]	Reglamento (UE) 2017/373 por el que se establecen requisitos comunes para los proveedores de servicios de gestión del tránsito aéreo/navegación aérea y otras funciones de la red de gestión del tránsito aéreo y su supervisión, por el que se derogan el Reglamento (CE) Nº 482/2008 y los Reglamentos de Ejecución (UE) Nº 1034/2011, (UE) Nº 1035/2011 y (UE) 2016/1377, y por el que se modifica el Reglamento (UE) Nº 677/2011. ¡EN VIGOR! Nota: Este reglamento es de aplicación a partir del 02/01/2020.
[10]	Easy Access Rules for Air Traffic Management/Air Navigation Services (EU) 2017/373. Derivado de la decisión ED 2019/022/R. December 2019
[11]	ED-153 "Guidelines for ANS Software Safety Assurance".

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

4. Terminología y definiciones

En este documento se aludirá a los servicios y suministros exteriores como a los servicios CNS prestados por ENAIRe que tengan un potencial impacto directo en la seguridad como servicios exteriores, a su prestatario se le denominará proveedor exterior y se entenderá como contacto formal a la relación formalizada a través de un acuerdo, convenio, pliego de prescripciones técnicas o documento contractual entre el proveedor y ENAIRe.

De forma general aplicará lo indicado en la instrucción A111-19-PES-001 [3], que referencia al siguiente enlace: <http://safety.nav.es/glosarioyenlaces.html>. Así como los recogidos en el Anexo I del Reglamento (EU) 2017/373 [9].

4.1. Definiciones

Actividad contratada (AC) (ref. en [1] y [9]): Incluyen todas las actividades dentro del alcance de las operaciones del proveedor de servicios, de conformidad con los términos del certificado, que son realizadas por otras organizaciones certificadas para llevar a cabo tal actividad o, en caso de no estar certificadas, que trabajan bajo la supervisión del proveedor de servicios. ¡NUEVO!

Contacto formal (ref. en [2]): Relación entre el proveedor de servicios de navegación aérea (ATS y/o CNS) y el proveedor de servicios exteriores, formalizada a través de un acuerdo, convenio, pliego de prescripciones técnicas o documento contractual equivalente.

Interfaz formal (IF) (ref. en [1]): Relación entre el proveedor de servicios ATS y/o no ATS CNS con empresas de aviación (entidad, persona, organización, distinta de los proveedores de servicios regulados por el Reglamento (UE) 2017/373) o con ANSP, que se ven afectadas por los servicios prestados por ENAIRe o pueden afectar a un servicio prestado. ¡NUEVO!

Equipos relacionados con la seguridad (ref. en [2]): Se entenderán como tales, en el ámbito de esta instrucción, los “equipos ATM/CNS relacionados con la seguridad” y los pertenecientes a “sistemas auxiliares”. (ref. en [2]).

Equipos ATMC/CNS homologados relacionados con la seguridad (ref. en [2]): Sistemas y dispositivos de ingeniería relacionados con la seguridad que hayan sido puestos en operación para ser utilizados directamente por los usuarios del espacio aéreo y/o soportan los servicios prestados por:

Proveedores de servicios de tránsito aéreo (ATS), solicitantes o ya certificados.

Proveedores de servicios de comunicación, navegación y vigilancia (CNS), solicitantes o ya certificados.

Personal ATSEP (ref. en [9]): Personal de electrónica de seguridad del tránsito aéreo. Todo personal autorizado con capacidad para operar, mantener, liberar y devolver a estado de funcionamiento el equipo del sistema funcional. ¡NUEVO!

Proveedor de Servicios de Navegación Aérea (PSNA, ANSP) (ref. en [6]): Cualquier entidad pública o privada encargada de la prestación de servicios de navegación aérea para la circulación aérea general.

Riesgo (ref. en [9]): Combinación de la probabilidad o de la frecuencia de aparición de un efecto perjudicial provocado por una situación peligrosa, y la severidad de tal efecto. ¡NUEVO!

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

Servicios ATS: ATC (elusión de colisiones, separación táctica, coordinación y transferencia, secuenciamiento y gestión del tráfico, gestión de Plan de Vuelo), FIS (información de vuelo), AL (alerta). ¡NUEVO!

Servicios exteriores (ref. en v2.1 de [2] y en Apéndice A de ESARR 3): Todo suministro o servicio material o no material que sea proporcionado por una organización que esté fuera del sistema de gestión de seguridad del proveedor de servicios ATM.

Servicios externalizados (ref. en [2]): Se consideran como tales aquellos servicios que se presten totalmente o en su mayoría con personal, equipos y procedimientos propios de un proveedor exterior.

Servicios No ATS: CNS (comunicaciones, navegación y vigilancia), ASM (gestión del espacio aéreo), ATFM (gestión de afluencia), AIS/AIM (provisión de información aeronáutica). ¡NUEVO!

Sistema (ref. en [6]): Engloba los componentes de tierra y los embarcados, así como los equipos espaciales, que prestan apoyo a los servicios de navegación aérea en todas las fases de vuelo.

Sistema funcional (ref. en [9]): combinación de procedimientos, recursos humanos y equipos, incluido hardware y software, organizados para desempeñar una función en el contexto de ATM/ANS y otras funciones de red ATM. ¡NUEVO!

Sistemas Auxiliares (ref. en [2]): Se entenderán como tales las instalaciones de energía y las instalaciones de climatización.

Situación peligrosa (ref. en [9]): Cualquier condición, suceso o circunstancia que pueda dar lugar a un efecto perjudicial. ¡NUEVO!

Tareas de seguridad (ref. en [2]): Listado de tareas operativas relacionadas con la seguridad que aparecen recogidas en el siguiente cuadro:

INGENIERÍA Y MANTENIMIENTO	TAREAS DE SEGURIDAD ¹
	Seguimiento de la estabilidad del software de las aplicaciones de proceso de datos de vuelo y radar y actuaciones sobre las mismas.
	Monitorización de los sistemas CNS/ATM, evaluación de los fallos, reconfiguración y restablecimiento de dichos sistemas, excluyéndose la actuación que conlleve sólo monitorización o sólo evaluación.
	Mantenimiento preventivo y correctivo de los sistemas CNS y del hardware de soporte de las aplicaciones.
	Calibración de la instrumentación necesaria para el mantenimiento, excluyéndose la “gestión de las calibraciones”.
	Mantenimiento preventivo y correctivo de los sistemas auxiliares que contribuyen al funcionamiento de los equipos ATM/CNS homologados relacionados con la seguridad, entendiéndose sistemas auxiliares como las instalaciones de energía y las instalaciones de climatización.

¹ Esta tabla viene del documento “SGOP-14-INF-036-1.0 Informe sobre la definición de Tareas de Seguridad en la DNA”, del 30/04/2014. Pasado a histórico el 31/01/2020 debido a la entrada en vigor del Reglamento (UE) 2017/373 [9]. Se indica aquí por trazabilidad y coherencia con las definiciones en vigor, hasta que se actualice la instrucción [2].

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

TAREAS DE SEGURIDAD ¹	
OPERACIONES	Tratamiento de la información aeronáutica en tiempo real (NOTAM), mediante la gestión y operación de dicha información.
	Coordinación de las comunicaciones entre aeronaves y control, en áreas transoceánicas, mediante emisoras HF para la retransmisión de información y/o la retransmisión de autorizaciones de control de tráfico aéreo.
	Suministro de información de vuelo de aeródromo AFIS (en caso de que existiera dicha función).

4.2. Acrónimos

Acrónimo	Descripción
AMR	Análisis y Mitigación de Riesgos.
ANSP	Air Navigation Service Provider. Proveedor de Servicios de Navegación Aérea
AS	Análisis de Seguridad.
CNS	Comunicación, Navegación y Vigilancia.
HW	Hardware.
PGS	Plan de Gestión de Seguridad (Safety).
PPT	Pliego de Prescripciones Técnicas.
R&A	Reliability & Availability. Fiabilidad y Disponibilidad
RSE	Requisito de Seguridad Específico.
RSG	Requisito de Seguridad General.
RSI	Requisito de Seguridad de Interlocutores.
SACTA	Sistema Automatizado de Control de Tránsito Aéreo
SCV	Sistema de Comunicaciones Voz
SW	Software.
T/A	Tierra/Aire.

5. Plan de Gestión de la Seguridad (Safety)

El proveedor exterior elaborará un Plan de Gestión de la Seguridad (safety) (PGS) del servicio que contendrá cómo mínimo el siguiente contenido o las referencias a la documentación donde se encuentre, incluyendo los aspectos relativos al SW:

- a) Organización interna de seguridad, descripción de funciones y responsabilidades y su interrelación con otros grupos de ingeniería. Deberá quedar claro quién será el interlocutor (con los datos de contacto en la versión actualizada al inicio del servicio) por parte del proveedor exterior para los temas de seguridad (safety) con el personal de ENAIRe.
- b) Definición del entorno operacional del sistema (Ver “Guidance Material: Operational Environment definition – SAF.ET1.ST03.1000-MAN-01-01-01-A” de la metodología SAM de

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

Eurocontrol y material guía de apoyo de Easy Access Rules de EASA [10], punto AMC4 ATM/ANS.OR.C.005(a)(2). "Determination of the operational context for the change"). **¡NUEVO!**

- c) Regulación y Estándares aplicables.
- d) Metodología, técnicas y herramientas a utilizar para la evaluación/análisis de seguridad.
- e) **Planificación de actividades de garantía de seguridad:** Calendario, responsabilidades, asignación de recursos. Para cada actividad de análisis de seguridad se deberá: describir la acción y su objetivo, definir entradas, salidas y metodología aplicada.
- f) Relación entre el ciclo de vida de seguridad y el ciclo de vida del servicio (fases del proyecto). Vinculado con la planificación de las actuaciones a realizar, incluyendo sus interrelaciones.
- g) Lista de entregables asociados a cada actividad de seguridad.
- h) Seguimiento y revisiones del Plan de seguridad.

Según se indica en el punto 4 Definiciones, se entiende por servicio todo suministro o servicio material o no material.

El objetivo del PGS es describir las actividades de seguridad que se van a llevar a cabo durante la ejecución del expediente indicando qué se va a hacer, cómo se va a hacer y cuándo se va a hacer.

En el PGS no se incluye ningún análisis de riesgos, ni las evidencias de cumplimiento de los distintos requisitos de seguridad, es un plan de gestión de la seguridad, una planificación de las actividades de seguridad.

Las actividades de garantía de seguridad son las que se desarrollarán en el Análisis de Seguridad, como mínimo deberán describirse las siguientes: Descripción del servicio, evidencia de cumplimiento de los requisitos de seguridad generales, evidencia de cumplimiento de los requisitos de seguridad específicos y entre ellos se han de destacar los requisitos de Fiabilidad y Disponibilidad (R&A) si se suministra equipamiento HW, los requisitos relativos al SW y el AMR de las fases de instalación, puesta en servicio y desinstalación (si procede) del expediente.

Al ser un documento de gestión, es un documento vivo, que deberá actualizarse, si procede, durante las principales fases del ciclo de vida del sistema o durante la ejecución del expediente.

6. Análisis de Seguridad (Safety) del Servicio

El proveedor exterior realizará un Análisis de seguridad (safety) (AS) del servicio que contendrá como mínimo el siguiente contenido:

- a) Descripción del servicio a prestar (descripción completa de las actuaciones, del equipamiento sobre el que van a realizarlas, sus funciones y elementos, la interrelación entre ellos y las interfaces externas), entendiéndose como sistema al conjunto de equipamiento (HW y SW), personal y procedimientos objeto del servicio).

El objetivo de esta descripción es poder llevar a cabo el cumplimiento de los requisitos de seguridad asociados a la fiabilidad y disponibilidad, de garantía del SW y del análisis y mitigación de riesgos.

- b) Análisis y evidencia de cumplimiento de los Requisitos de Seguridad Generales (RSG) para todo el ciclo de vida del servicio, ver punto 6.2. Como mínimo se requiere que se evidencien los requisitos del modo indicado en ese punto.

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

Estos requisitos los establece ENAIRe para los contactos formales con los proveedores exteriores, han sido extraídos de la instrucción interna [1], indicando únicamente los aplicables al servicio requerido.

- c) Análisis y evidencia de cumplimiento de los Requisitos de Seguridad Específicos (RSE) para todo el ciclo de vida del servicio, ver punto 6.3. Como mínimo se requiere que se evidencien los requisitos del modo indicado en ese punto.

Estos requisitos los establece la unidad responsable del servicio, en este caso la División de Comunicaciones de ENAIRe para los proveedores exteriores, se clasifican en 4 tipos:

c.1 RSE – Asociados al producto. Estos requisitos provienen de análisis de seguridad de más alto nivel para dar cumplimiento a objetivos y/o requisitos de seguridad asociados al cambio, de requisitos directamente derivados de la normativa aplicable o de juicio de expertos.

c.2 RSE – Asociados a la Fiabilidad y Disponibilidad (R&A). En caso de que el servicio incluya el suministro de equipamiento Hardware, se incluirán requisitos de R&A derivados de las prestaciones técnicas de los distintos sistemas relacionados con el expediente. – **NO APlican a este PPT.**

c.3 RSE – Asociados al SW. En caso de que el servicio incluya el suministro de Software, se incluirán requisitos asociados al nivel SWAL asignado a dicho SW, derivados de la instrucción para la garantía de la Seguridad del Software de ENAIRe [5] y de expertos en seguridad (safety), que provienen del estándar de EUROCAE ED-153 [11].

c.4 RSE – Asociados a Servicios parcialmente externalizados. En caso de que el servicio incluya la externalización parcial de servicios ATS, CNS o AIS, se incluirán requisitos sobre los niveles de servicio a satisfacer a efectos de seguridad y sobre su monitorización continua. – **NO APlican a este PPT.**

- d) Análisis y evidencia de cumplimiento de los Requisitos de Seguridad de Interlocutores (RSI) para todo el ciclo de vida del servicio. Como mínimo se requiere que se evidencien los requisitos del modo indicado. – **NO APlican a este PPT.**

El contenido del AS puede verse modificado una vez sea derogada la Instrucción de trabajo para la garantía de seguridad de los servicios y suministros exteriores - A111b-12-INS-001 (Ref. [2]) y entre en vigor la instrucción A111-19-INS-004.

Si durante el transcurso de la ejecución del expediente estos requisitos se ven modificados, la empresa adjudicataria deberá dar cumplimiento de los mismo.

6.1. Evidencia de cumplimiento de los RSG y RSE

A continuación, se indican de forma genérica las evidencias de cumplimiento de los RSG y RSE en función de las distintas fases del servicio.

Provienen de la instrucción interna de ENAIRe [2], de las que se han añadido evidencias adicionales en los requisitos en los que la División de Comunicaciones de ENAIRe estima que requiere más información para evaluar la capacidad del potencial proveedor exterior para satisfacer los requisitos.

Fase Definición y Oferta:

En la etapa de definición y oferta del servicio existen una serie de requisitos para los que se considera que la aportación de una Declaración Responsable en la oferta del potencial proveedor exterior indicando que cumplirá los requisitos de seguridad especificados en el expediente, que

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

dispondrá de las evidencias que así lo acrediten y que se compromete a mantener su cumplimiento durante todo el periodo de vigencia del contrato, daría cumplimiento a esta primera fase. Estos requisitos están marcados con un (1).

La presentación de esta declaración se considera una evidencia “necesaria”, pero no en todos los RSG y RSE es “suficiente”, para garantizar que la capacidad del proveedor exterior de cumplimiento de los requisitos generales de seguridad, la División de Comunicaciones requiere que se indique para cada uno de los requisitos cómo garantizará dicho cumplimiento.

Por ejemplo, para el requisito RSG2.1, no es suficiente con que en la Declaración Responsable se indique que se cumplirá, sería necesario además añadir que dispone del sistema de gestión documental y registro identificándolo e indicar que lo aplicará a la documentación del servicio a proporcionar.

En esta fase, el proveedor exterior deberá entregar:

- Plan de Gestión de la Seguridad (Safety) del servicio. Versión borrador (v.0).
- Análisis de Seguridad (safety) del servicio. Versión borrador (v.0). En esta versión de deberá incluir la Declaración responsable y las evidencias adicionales requeridas, entre ellas la explicación de cómo se garantizará el cumplimiento de los requisitos de seguridad.

Fase Previo al inicio:

En la etapa anterior al inicio del servicio existen una serie de requisitos para los que se considera que bastará como evidencia la firma por parte del proveedor exterior de un acuerdo o contrato que refleje los requisitos. La propia Declaración Responsable también podrá valer como evidencia si está firmada. Estos requisitos están marcados con un (2).

En esta fase existen requisitos donde también se requerirá la entrega de una evidencia sin la cual no se podrán iniciar los trabajos objetos del contrato.

Por ejemplo, para el requisito RSG6.1, se deberán entregar los registros de entrega de las Fichas de divulgación de seguridad operacional de servicios exteriores con los “recibí” del personal asignado al servicio antes del inicio de este.

En esta fase, el proveedor exterior deberá entregar:

- Plan de Gestión de la Seguridad (Safety) del servicio. Versión actualizada como muy tarde un mes después del replanteo o inicio del expediente.
- Análisis de Seguridad (safety) del servicio. Versión actualizada como muy tarde un mes después del replanteo o inicio del expediente (v.1). En esta versión de deberá incluir la Declaración responsable firmada y las evidencias adicionales requeridas, entre ellas la entrega del certificado ISO 9001 (RSG2.1), los registros de entrega de las Fichas de divulgación (RSG6.1), acreditación de la competencia del personal (RSG6.2), como ejemplo.

Fase Ejecución:

En la etapa de ejecución del servicio existen una serie de requisitos para los que se considera que bastará como evidencia de cumplimiento la ausencia de no conformidades o desviaciones detectadas durante la ejecución del servicio. Estos requisitos están marcados con un (3).

En esta fase también existen requisitos donde se requerirá la entrega de otras evidencias para garantizar el cumplimiento del requisito en esta fase.

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

Por ejemplo, para el requisito RSG6.1, si se ha incorporado nuevo personal asignado al servicio, se deberán entregar los registros de entrega de las Fichas de divulgación de seguridad operacional con el “recibí” de ese nuevo personal, para el RSG11, se deberá entregar el Plan de Instalación, el análisis de riesgos de la instalación y evidencias de implantación de medidas de mitigación derivadas del análisis de riesgos realizado.

En esta fase, el proveedor exterior deberá entregar:

- Plan de Gestión de la Seguridad (Safety) del servicio. Versión actualizada, si procede, ante cualquier cambio.
- Análisis de Seguridad (safety) del servicio. Versión completada y actualizada ante cualquier cambio. Como mínimo se deberán entregar las siguientes versiones:
 - V2. Un mes antes del inicio de la instalación, en caso necesario.
 - V3. Dos meses antes del inicio de la transición y/o entrada en operación del equipamiento actualizado/modificado, en caso necesario.
 - Versión definitiva una vez se dispongan de los resultados de las pruebas pertinentes y por tanto de las evidencias necesarias, en caso necesario si no se encontraban referenciadas en versiones anteriores.

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

6.2. Requisitos de Seguridad Generales (RGS)

RSG	DESCRIPCIÓN	EVIDENCIA DE CUMPLIMIENTO / FASE		
		OFERTA	PREVIO INICIO	EJECUCIÓN
RSG1. Requisitos para la gestión de la seguridad	RSG1.1. El proveedor exterior se comprometerá a colaborar con la unidad de ENAIRe responsable del servicio para el cumplimiento de los sus procedimientos internos, instrucciones, métodos de trabajo, manuales, acuerdos, o similar, que le puedan ser de aplicación en función de la naturaleza del servicio, y en particular con lo establecido en relación con la gestión de la seguridad en el "Manual del Sistema de Gestión de Navegación Aérea" de ENAIRe.	(1)	(2)	(3)
RSG2. Requisitos para los sistemas de gestión documental y registro	RSG2.1. El proveedor exterior deberá disponer de un sistema de gestión documental y registro aplicado por lo menos al servicio a proporcionar.	(1) Explicar cómo se garantizará el requisito	– Certificado ISO 9001 o – Descripción del sistema de gestión documental	N/A
	RSG2.2. El proveedor exterior deberá proporcionar a ENAIRe todas las evidencias documentales relacionadas con la seguridad que le sean solicitadas a lo largo de la prestación del servicio.	(1)	(2)	(3)
RSG3. Requisitos para la supervisión de seguridad	RSG3.1. El proveedor exterior se deberá someter, cuando se le solicite, a auditorías o inspecciones de seguridad por parte de ENAIRe, o de quién ésta designe.	(1)	(2)	(3)
RSG4. Requisitos para corrección de desviaciones detectadas	RSG4.1. A solicitud de ENAIRe, el proveedor exterior deberá llevar a la práctica las medidas correctivas que sean necesarias para subsanar desviaciones detectadas en los requisitos de seguridad exigibles al servicio.	(1) Explicar cómo se garantizará el requisito	(2)	N/A

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

RSG	DESCRIPCIÓN	EVIDENCIA DE CUMPLIMIENTO / FASE		
		OFERTA	PREVIO INICIO	EJECUCIÓN
	RSG4.2. El proveedor exterior deberá documentar la implantación de las medidas correctivas y proporcionar a ENAIRe las nuevas evidencias de cumplimiento de los Requisitos de Seguridad o las evidencias actualizadas según sea necesario.	(1) Explicar cómo se garantizará el requisito	(2)	(3) - Evidencias de implantación de medidas de mitigación - Nuevas evidencias (o evidencias actualizadas) de cumplimiento de Requisitos, si fueran necesarias
	RSG4.3. En el caso de que el proveedor exterior sea un proveedor de servicios de navegación aérea o un gestor aeroportuario y siempre que se identifique la necesidad de implantación de medidas de mitigación adicionales respecto a un servicio prestado por un proveedor exterior, se realizará un análisis objetivo de necesidad, conveniencia y viabilidad técnica y económica para alcanzar un acuerdo respecto a su implantación. En caso de que las partes no alcancen un acuerdo, ENAIRe remitirá la discrepancia a la AESA, de acuerdo con lo establecido por ésta al efecto (AES Aeronautical Telecommunications ICAO Annex 11 - Guidelines for Safety Management Systems for Air Navigation Services - Part 3: Implementation of Safety Management Systems, Paragraph 3.3.3).	(1) Explicar cómo se garantizará el requisito	(2)	(3) - Análisis sobre las medidas de mitigación adicionales - Acuerdo sobre implantación de nuevas medidas / Remisión de discrepancia a AESA
RSG5. Requisitos para el traslado de responsabilidad es a terceros	RSG5.1. El proveedor exterior será responsable de trasladar y hacer cumplir los requisitos de seguridad que le sean aplicables tanto a su propio personal como a los trabajadores de sus contratas o subcontratas y de cualesquier otras empresas o entidades que tengan algún tipo de contacto formal o de colaboración con el proveedor exterior para el servicio que va a proporcionar a ENAIRe, así como de obtener las evidencias de cumplimiento correspondientes.	(1) Explicar cómo se garantizará el requisito	(2) Se completará este requisito con el siguiente	(3)

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

RSG	DESCRIPCIÓN	EVIDENCIA DE CUMPLIMIENTO / FASE		
		OFERTA	PREVIO INICIO	EJECUCIÓN
RSG6. Requisitos de competencia mínima del personal	<p>RSG6.1. El proveedor exterior deberá garantizar que todo el personal asignado al servicio, incluyendo las nuevas incorporaciones, tiene los conocimientos mínimos necesarios en materia de seguridad operacional. Para ello deberá evidenciar, mediante registro de entrega de documentación con acuse de recibo o similar, que todo el personal asignado al servicio objeto del contacto formal expediente ha recibido la documentación de seguridad operacional establecida, en función de la naturaleza de este, y que se detalla en las "Fichas de divulgación de seguridad operacional de servicios exteriores GEN y COM"</p> <p><i>Nota: En el apartado 7 de este anexo se adjuntan las Fichas de divulgación indicadas.</i></p>	(1) Explicar cómo se garantizará el requisito	- Registros de entrega de documentación con "Recibí" del personal asignado al servicio	- Actualización de estos registros si se incorpora al listado nuevo personal
	<p>RSG6.2. El proveedor exterior deberá garantizar que el personal destinado al servicio exterior ha recibido la formación adecuada y es competente para el desempeño de la tarea asignada, según lo que se haya establecido al efecto en el contacto formal.</p>	(1)	<ul style="list-style-type: none"> - Descripción de la competencia de los medios humanos destinados al servicio exterior - Títulos, carnés, acreditaciones, Registros de formación - Acreditación de competencia del personal 	(3) - Actualización de estos registros si se incorpora al listado nuevo personal
	<p>RSG6.3. El proveedor exterior deberá garantizar que cualquier nueva incorporación es formada adecuadamente y que todo el personal destinado al servicio continúa siendo competente para el desempeño de la tarea asignada a lo largo del periodo de prestación.</p>	(1) Explicar cómo se garantizará el requisito	(2)	- Actualización de estos registros si se incorpora al listado nuevo personal
	<p>RSG6.4. El proveedor exterior deberá mantener los registros apropiados sobre la formación y competencia de su personal.</p>	(1) Explicar cómo se garantizará el requisito	(2)	- Registros actualizados (en ENAIRe o en el proveedor)

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

RSG	DESCRIPCIÓN	EVIDENCIA DE CUMPLIMIENTO / FASE		
		OFERTA	PREVIO INICIO	EJECUCIÓN
RSG7. Requisitos acerca de la condición física y mental del personal	RSG7.1. El proveedor exterior deberá establecer los criterios médicos del personal que garantice que éste es "APTO" para realizar las tareas asignadas sin poner en riesgo la provisión segura de los servicios responsabilidad de ENAIRE, así como identificar las condiciones físicas y/o mentales bajo las cuales su personal será considerado "no apto" para realizar las tareas que tiene asignadas. Estos aspectos deberán venir determinados por su Servicio de Medicina del Trabajo, ya sea propio o ajeno. Por defecto se tomarán los "Protocolos de vigilancia sanitaria específica de los trabajadores" del Ministerio de Sanidad, Asuntos Sociales e Igualdad.	(1)	- Certificación de que los Procedimientos de vigilancia de la salud psicofísica aplicados están basados en los publicados por el Ministerio de Sanidad, Asuntos Sociales e Igualdad	N/A
	RSG7.2. El proveedor exterior deberá establecer los procedimientos de retirada/sustitución/relevo cuando un trabajador que realice tareas de seguridad presente una condición física y/o mental que lo incapacite para realizar las tareas que tiene asignadas.	(1) Explicar cómo se garantizará el requisito	- Procedimientos de Retirada / sustitución / Relevo del personal	N/A
	RSG7.3. El proveedor exterior deberá remitir a la unidad responsable de ENAIRE, al inicio del expediente, un listado con el resultado del Reconocimiento Médico Obligatorio en término de aptitud (APTO/NO APTO) del personal que realiza tareas de seguridad. Además, deberá mantener un registro con este listado actualizado y enviarlo al responsable de ENAIRE en caso de que se produzca algún cambio en el personal asignado al servicio y, en todo caso, remitirlo anualmente mientras se mantenga el contacto formal, o en plazos inferiores si así lo estima oportuno el responsable de ENAIRE.	(1)	- Listado con resultado del Reconocimiento Médico Obligatorio en términos de aptitud (APTO/NO APTO) de todo el personal asignado al servicio	- Registros actualizados (en ENAIRE o en el proveedor) - Registros de envío a ENAIRE de las actualizaciones del listado

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

RSG	DESCRIPCIÓN	EVIDENCIA DE CUMPLIMIENTO / FASE		
		OFERTA	PREVIO INICIO	EJECUCIÓN
RSG8. Requisitos adicionales para personal ATSEP y personal de servicios auxiliares con supervisión directa de personal técnico, o de ingeniería, de ENAIRe que disponga de conocimientos en materia de seguridad operacional	RSG8.1. El proveedor exterior deberá garantizar, mediante los registros apropiados, que el personal destinado al servicio es el necesario y suficiente para asegurar una cobertura y la continuidad del servicio contratado, de acuerdo a lo establecido en el contacto formal.	(1) Explicar cómo se garantizará el requisito	(2) Análisis justificativo de las necesidades cuantitativas y cualitativas del personal para asegurar la cobertura y continuidad del servicio contratado	(2) Registros actualizados (en ENAIRe o en el proveedor exterior) con el personal asignado efectivamente al servicio
RSG10. Requisitos sobre niveles de garantía de seguridad del SW (SWAL)	RSG10.1. El proveedor exterior deberá asegurar que el software incluido en el suministro cumple con los niveles de garantía de seguridad del SW (SWAL) solicitados por ENAIRe de acuerdo con su SSAS (ver RSE2). Alternativamente, y en caso necesario, el proveedor exterior presentará una propuesta justificada de reasignación de SWAL en base a la arquitectura propuesta del sistema y teniendo en cuenta el SWAL solicitado en primera instancia. Esta propuesta deberá ser aceptada por ENAIRe.	(1) Explicar cómo se garantizará el requisito	(2)	- Evidencias específicas (ver RSE2.1 y RSE2.2) - Informe de garantía de cumplimiento de SWAL
	RSG10.2. El proveedor exterior garantizará la independencia entre elementos SW con diferente SWAL asignado o bien demostrará el cumplimiento del SWAL más crítico para todos los elementos SW relacionados entre sí.	(1) Explicar cómo se garantizará el requisito	(2)	- Evidencias específicas (ver RSE2.1 y RSE2.2) - Informe de garantía de cumplimiento de SWAL
	RSG10.3. El proveedor exterior entregará las evidencias solicitadas por ENAIRe en las fases especificadas, para demostrar los niveles de garantía de seguridad del SW de acuerdo con su SSAS (ver RSE2)	(1) Explicar cómo se garantizará el requisito	(2)	- Evidencias específicas (ver RSE2.1 y RSE2.2) - Informe de garantía de cumplimiento de SWAL

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

RSG	DESCRIPCIÓN	EVIDENCIA DE CUMPLIMIENTO / FASE		
		OFERTA	PREVIO INICIO	EJECUCIÓN
RSG12. Requisitos para la puesta y/o retirada de operación de equipos (HW y SW) relacionados con la seguridad	RSG12.1. El proveedor exterior deberá proporcionar una descripción de las actividades a llevar a cabo para la puesta en operación y/o retirada del equipamiento (HW y SW) relacionado con la seguridad, incluyendo las correspondientes a la fase de transición si fuera necesaria.	(1) Explicar cómo se garantizará el requisito	(2)	- Plan de transición y/o puesta en operación y/o retirada del servicio
	RSG12.2. El proveedor exterior proporcionará el soporte técnico necesario para que ENAIRE elabore el análisis y mitigación de riesgos de la transición y/o puesta en operación y/o retirada del equipamiento conforme a sus procedimientos.	(1) Explicar cómo se garantizará el requisito	(2)	- Análisis y mitigación de riesgos de la transición y/o puesta en operación y/o retirada del servicio (en el ámbito de competencia del proveedor exterior)
	RSG12.3. El proveedor exterior implantará las medidas de mitigación que se deriven del análisis y mitigación de riesgos de la transición y/o puesta en operación y/o retirada dentro de su ámbito de competencia, proporcionando las evidencias correspondientes que le sean solicitadas por ENAIRE.	(1) Explicar cómo se garantizará el requisito	(2)	- Evidencias de implantación de medidas de mitigación derivadas del análisis de la transición y/o puesta en operación y/o retirada del servicio.
RSG14. Requisitos para la coordinación de actividades con impacto en seguridad	RSG14.1. Antes del inicio del servicio, ENAIRE y el proveedor exterior deberán establecer formalmente procedimientos de coordinación para las actividades del proveedor que puedan afectar a la seguridad de los servicios ATM, CNS y/o AIS prestados por ENAIRE. Estos procedimientos de coordinación incluirán, si procede, procedimientos de comunicación de cambios significativos de una parte que puedan afectar a la otra, así como los mecanismos de colaboración para la gestión de dichos cambios.	(1) Explicar cómo se garantizará el requisito	(2) Procedimientos de coordinación	(3) Evidencia de la aplicación de los procedimientos de Coordinación
	RSG14.2. El proveedor exterior deberá garantizar que, cuando las actividades se realicen en emplazamientos con equipos relacionados con la seguridad que se encuentren en servicio, su personal no actuará sobre estos equipos sin la supervisión directa o la autorización de ENAIRE.	(1) Explicar cómo se garantizará el requisito	(2) - Procedimientos de coordinación - Registros de entrega al personal	(3)

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

RSG	DESCRIPCIÓN	EVIDENCIA DE CUMPLIMIENTO / FASE		
		OFERTA	PREVIO INICIO	EJECUCIÓN
RSG15. Requisitos para la gestión de intervenciones planificadas en el servicio	RSG15.1. El proveedor exterior coordinará con ENAIRE las intervenciones planificadas en el servicio y las llevará a cabo de acuerdo con lo establecido en los procedimientos de coordinación establecidos entre ambos.	(1) Explicar cómo se garantizará el requisito	(2)	(3) - Registros de cumplimiento de procedimientos de coordinación - Actas de reuniones de coordinación Comunicaciones (e-mail o similar) de coordinación de actividades
	RSG15.2. Antes de cualquier intervención planificada en el servicio que pudiera producir interrupciones o degradaciones en los servicios ATM/CNS, y a partir de la información suministrada por el proveedor exterior, ENAIRE analizará su impacto en seguridad y coordinará la implantación, tanto por parte del proveedor como por ENAIRE, de las medidas de mitigación necesarias. El proveedor exterior documentará el proceso de análisis de seguridad y guardará registro de las evidencias.	(1) Explicar cómo se garantizará el requisito	(2)	(3) - Análisis de seguridad de las intervenciones planificadas - Evidencias de implantación de medidas de mitigación
RSG16. Requisitos para la gestión de incidencias de seguridad en el servicio	RSG16.1. El proveedor exterior deberá comunicar de inmediato a ENAIRE las incidencias en el servicio prestado que puedan afectar a los servicios ATS o CNS bajo su responsabilidad.	(1) Explicar cómo se garantizará el requisito	(2)	(3)
	RSG16.2. El proveedor exterior deberá disponer de un sistema de detección, registro y resolución de incidencias cuyos datos e informes deberán ser accesibles por ENAIRE.	(1) Explicar cómo se garantizará el requisito	(2) Descripción del sistema de registro y resolución de incidencias	(3) Registro de incidencias
	RSG16.3. El proveedor exterior deberá comprometerse a colaborar en la investigación de incidencias registradas por ENAIRE que pudieran tener un origen en los servicios prestados por aquél, aportando todos los datos que le sean solicitados.	(1) Explicar cómo se garantizará el requisito	(2)	(3)

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

RSG	DESCRIPCIÓN	EVIDENCIA DE CUMPLIMIENTO / FASE		
		OFERTA	PREVIO INICIO	EJECUCIÓN
	RSG 16.4. El proveedor exterior será responsable de la redacción de los informes de investigación de incidencias relativos a sus servicios, de la elaboración de propuestas de recomendaciones y del seguimiento de la implantación de las acciones correctivas asociadas.	(1) Explicar cómo se garantizará el requisito	(2)	(3) - Informes de investigación de incidencias - Informes de seguimiento de recomendaciones y acciones correctivas
	RSG16.5. El proveedor exterior se comprometerá a difundir al personal asignado al servicio dentro de su propia organización las lecciones aprendidas derivadas de las investigaciones de las incidencias.	(1) Explicar cómo se garantizará el requisito	(2)	(3) Registros de difusión de lecciones aprendidas

6.3. Requisitos de Seguridad Específicos (RSE)

RSE	DESCRIPCIÓN	EVIDENCIA DE CUMPLIMIENTO / FASE		
		OFERTA	PREVIO INICIO	EJECUCIÓN
RSE1. Requisitos de Seguridad del Producto	RSE1.1 El proveedor exterior deberá garantizar que las modificaciones a realizar en el Sistema de Comunicaciones Voz (SCV) de los Aeropuertos de Santiago, Bilbao, Tenerife Norte y Tenerife Sur no degradarán ninguna de las funcionalidades del Sistema de Comunicaciones existentes.	(1) Explicar cómo se garantizará el requisito	(2)	Descripción en el Análisis de Seguridad (Safety) o en documento independiente
	RSE1.2 El proveedor exterior deberá garantizar que las modificaciones a realizar en el Sistema de Comunicaciones Voz (SCV) del Aeropuertos de Santiago, Bilbao, Tenerife Norte y Tenerife Sur no afectarán al funcionamiento de los sistemas adyacentes.	(1) Explicar cómo se garantizará el requisito	(2)	Análisis y mitigación de riesgos de la puesta en operación/transición/migración del servicio (en el ámbito de competencia del proveedor exterior)

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

RSE	DESCRIPCIÓN	EVIDENCIA DE CUMPLIMIENTO / FASE		
		OFERTA	PREVIO INICIO	EJECUCIÓN
RSE2. Requisitos de Seguridad del Software (SW)	<p>RSE2.1. El proveedor exterior deberá garantizar, para aquellas tareas del ciclo de vida del SW bajo su responsabilidad, <u>asociadas al desarrollo de la interfaz SCV-SACTA</u>, desde que se decide producir o modificar un producto hasta su retirada del servicio si fuera el caso, incluyendo el desarrollo, operación y mantenimiento, como mínimo, un nivel de garantía del software igual a 4 (SWAL 4), tomando como referencia el documento de EUROCAE ED-153 "Guidelines for ANS Software Safety Assurance", agosto 2009 y de acuerdo a lo indicado en los requisitos RSG10 y RSE2.2.</p>	<p>(1) Explicar cómo se garantizará el requisito</p>	(2)	Las indicadas en el RSE2.2
	<p>RSE2.2 El proveedor exterior deberá proporcionar las evidencias necesarias para demostrar el cumplimiento del SWAL 4 para el SW <u>asociado al desarrollo de la interfaz SCV-SACTA</u>, desarrollando la documentación necesaria o identificando en qué documento/s se encuentran los <u>contenidos recogidos en el punto 6.3.1</u> de este documento.</p> <p><i>Nota: El alcance y contenido de los puntos listados en el punto 6.3.1 estarán acordados con el cliente. La definición del contenido de cada punto se iniciará con la antelación suficiente para estar documentado antes del inicio de la fase que le corresponda.</i></p>	<p>(1) Explicar cómo se garantizará el requisito para cada uno de los contenidos del 6.3.1</p>	(2)	Evidencias específicas completadas y actualizadas ante cualquier cambio. En el Análisis de Seguridad (Safety) o en documentación independiente

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

6.3.1. Requisitos de Garantía del Software (SW)

RSE2.2 El proveedor exterior deberá proporcionar las evidencias necesarias para demostrar el cumplimiento del **SWAL 4** para el SW asociado al desarrollo de la interfaz SCV-SACTA, desarrollando la documentación necesaria o identificando en qué documento/s se encuentran los siguientes contenidos obtenidos de la Instrucción para la Garantía de la Seguridad del Software de ENAIRe [5] y de expertos en seguridad (safety), que provienen del estándar de EUROCAE ED-153 [11].

Algunos de los contenidos son responsabilidad del proveedor de servicios, ENAIRe, pero para desarrollarlos es necesario que el proveedor exterior proporcione determinadas evidencias, por eso se indican todos los contenidos necesarios. Aun así, los contenidos que son responsabilidad plena de ENAIRe, de los que no es necesario que el proveedor exterior proporcione ninguna evidencia se han marcado en *gris y cursiva*:

1. Descripción del Software y del entorno (Referencia del ED-153: 3.1.1, 3.1.2).

Incluir una definición del propósito del Software, sus funciones e interfaces, los escenarios y modos de operación, sus relaciones con las funciones del Sistema, así como el entorno, tanto físico como operacional, en el que será utilizado.

2. Identificación del Marco Aplicable (Referencia del ED-153: 3.1.3, 3.1.4).

Identificar la reglamentación aplicable, *así como los procedimientos internos de la organización*.

3. Planificación de la evaluación Safety del Software (Referencia del ED-153: 3.2.x, 3.5.x).

Establecer una planificación para acometer la evaluación de la seguridad operacional del software que contemple: enfoque, entregables, responsabilidades, esquemas de clasificación de riesgos, definición de objetivos de seguridad, métodos de identificación de amenazas.

Revisar e incluir planificación para su aprobación cuando sea necesario.

Distribuir la planificación para conocimiento y aplicación de las partes implicadas. Documentar los resultados de la evaluación safety del software, control de configuración y distribuirla para conocimiento y aplicación de las partes implicadas.

4. Identificación de los requisitos de seguridad del software (Referencia del ED-153: 3.3x, 3.1.5, 3.6.x).

Identificar fallos potenciales del SW, considerando todos los posibles modos de fallo y la secuencia de eventos que llevan a la ocurrencia de cada fallo. Evaluar los efectos de la ocurrencia de los fallos.

Identificar las amenazas del SW, añadiéndolas a las amenazas del sistema identificadas en el proceso de análisis y mitigación de riesgos.

Identificar requisitos de seguridad software, requisitos completos, describiendo el comportamiento funcional en modos nominal y degradado, el rendimiento en tiempo, la capacidad, la exactitud, el uso de recursos HW, la robustez y la tolerancia a la sobrecarga, según proceda.

Los Requisitos de Seguridad del Software serán correctos y completos, y deben dar cumplimiento a los Objetivos de Seguridad del Sistema. El Software no contendrá ninguna función que afecte negativamente a la seguridad.

Realizar la asignación de Niveles de Garantía del Software (SWAL). Se ha desarrollado un Material Guía donde se define una metodología de asignación [5].

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

5. Validación, Verificación y Garantía del proceso de evaluación Safety del Software (Referencia del ED-153: 3.4.x).

Verificar que los Requisitos de Seguridad del Software especifican el comportamiento funcional en modos nominal y degradado, el rendimiento en tiempo, la capacidad, la exactitud, el uso de recursos HW, la robustez y la tolerancia a la sobrecarga.

Verificar que son completos, correctos y consistentes con los efectos de las amenazas y con los Objetivos de Seguridad asociados.

Comprobar que se ha seguido la planificación establecida para la Evaluación Safety del Software, indicando las desviaciones encontradas.

6. Criterios de aceptación del producto (Referencia del ED-153: 4.1.7, 7.2.1).

Definir la estrategia y criterios, de acuerdo con el SWAL asignado, bajo los que se aceptará el producto SW entregado por el suministrador, incluyendo el acuerdo con el suministrador para la monitorización de los aspectos relacionados con la garantía de seguridad del software.

Para productos COTS o software no desarrollado o reutilizado, definir la estrategia y criterios para la adquisición, aceptación, verificación y gestión de configuración.

Esta estrategia y criterios deberán proporcionar confianza suficiente en que el software puede explotarse de una manera totalmente segura.

7. Especificación de requisitos (Referencia del ED-153: 4.3.1, 4.3.2, 4.3.4, 4.3.5, 4.3.6, 4.3.13, 4.3.14, 4.3.15, 4.4.5, 7.2.4, 7.2.6).

Especificar los requisitos de los sistemas, relacionándolos con las funciones, interfaces, necesidades de usuario, necesidad de mantenimiento, restricciones de diseño y validación. Los requisitos estarán distribuidos en los distintos elementos del sistema (equipos, personas y procedimientos).

Especificar los requisitos del software según punto 4.

Asegurar la trazabilidad de los requisitos del software con los requisitos del sistema, hasta el nivel de diseño necesario. Para productos COTS, asegurar que se satisface la especificación de los requisitos del software.

Especificar requisitos derivados, para prevenir que las funciones no deseadas del COTS afecten al resto del sistema.

8. Planificación de procesos (Referencia del ED-153: 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1).

Elaborar una planificación para las actividades del **Proceso de Desarrollo del Sistema y del Software**, que contemple como mínimo: definición de estándares aplicables, métodos y herramientas y responsabilidades asociadas con el desarrollo y la verificación de los requisitos.

Describir el entorno de desarrollo: métodos, procedimientos y/o herramientas y/o plataformas HW seleccionadas para la realización del desarrollo.

Se deberá seleccionar una herramienta para la gestión de la especificación de requisitos.

Elaborar una planificación del **Proceso de Operación** que aborde la comprobación de que el Software se ejecuta en el entorno de operación especificado, la necesidad de soporte o formación y los procedimientos de operación y monitorización.

Elaborar una planificación del **Proceso de Documentación**, que identifique la documentación que se elaborará durante el ciclo de vida del Software. La elaboración, modificación, distribución y producción de la documentación seguirá requisitos definidos, y estarán sujetas a Control de la Configuración.

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

Elaborar una planificación del **Proceso de Gestión de la Configuración**, indicando actividades, procedimientos, programación, herramientas y responsabilidades.

Elaborar una planificación del **Proceso de Verificación del Software**, indicando las actividades de verificación en las diferentes fases del Software, recursos a utilizar, responsabilidades, criterios de aprobación, métodos, programación y distribución de la documentación de salida del proceso a las partes implicadas.

Elaborar una planificación del **Proceso de Gestión y Resolución de Incidencias**, que gestione los problemas detectados en los productos Software (también para COTS) y en los procesos y actividades relacionados.

9. Operación (Referencia del ED-153: 4.4.x, 4.5.2, 4.5.3).

Asegurar que el SW se está ejecutando en el entorno de operación especificado, utilizando los procedimientos definidos para ello.

Monitorizar el funcionamiento del software, con el rigor del SWAL asignado.

Confirmar, para aquellos cambios que se introduzcan en el Software en la fase de Mantenimiento, que se mantiene el SWAL asignado.

Asegurar que las actividades de Mantenimiento se realizan con el rigor adecuado al SWAL asignado.

10. Gestión de la configuración (Referencia del ED-153: 5.2.x, 7.2.8, 7.2.10).

Establecer un esquema, y aplicarlo, para la identificación del Software (también para COTS), de sus versiones, de su documentación, de las propuestas de cambio, de las incidencias reportadas.

Registrar y contabilizar los cambios de los elementos identificados.

Definir el proceso de liberación y restitución de versiones de Software (también para COTS) y de cualquier elemento sujeto a Gestión de la Configuración.

Asegurar la trazabilidad de los datos del ciclo de vida del software con la versión del software para la que se corresponden.

11. Verificación del Software (Referencia del ED-153: 5.4.3-13, 5.7.2).

Verificar que los requisitos del software son correctos y completos, que se satisfacen respecto al comportamiento funcional, la temporización, la consistencia externa e interna, las características HW de la plataforma de ejecución.

Verificar que la implementación del Software no contiene ninguna función que afecte negativamente a la seguridad.

Verificar la trazabilidad de los Requisitos del Sistema con los Requisitos del Software, hasta el nivel de diseño necesario, así como con las evidencias de verificación.

Verificar que los resultados de los procedimientos, casos y resultados del proceso de verificación son, hasta el nivel de diseño necesario, correctos, completos, y que se justifican las diferencias con lo esperado.

Verificar el proceso de liberación y restitución de versiones software.

12. Gestión y resolución de incidencias (Referencia del ED-153: 5.8.x, 7.2.9).

Documentar cada incidencia detectada en el Software (también para COTS) mediante un Informe, que recoja las actividades realizadas: investigación, análisis, resolución.

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

Analizar si una incidencia tiene impacto safety. Analizar si supone una inconsistencia en la previa asignación del SWAL. Analizar si existen acciones correctivas que mitiguen aceptablemente el impacto safety de las incidencias detectadas.

Realizar Gestión de la Configuración del Informe de Gestión de la Incidencia.

13. Contenidos adicionales (Referencia del ED-153: 3.0.9, 3.0.12, 3.0.17).

El presente documento y el material guía definen los distintos niveles de rigor e independencia con que deben satisfacerse las garantías de seguridad, de acuerdo con el SWAL asignado.

Ante cualquier modificación en el Software, debe aplicarse el SSAS y satisfacerse los objetivos y contenidos establecidos.

El SSAS proporciona, en sí mismo, el argumento de demostración de cumplimiento de los objetivos de seguridad, de acuerdo con el SWAL asignado.

7. Fichas de Divulgación en materia de Seguridad Operacional

A continuación, se adjuntan las fichas de divulgación en materia de Seguridad Operacional aplicables a este expediente, en concreto las fichas GEN y COM.

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

FICHA DE DIVULGACIÓN DE SEGURIDAD OPERACIONAL SERVICIOS EXTERIORES		GEN (1/5)
<h3><u>SEGURIDAD OPERACIONAL</u></h3> <p>La misión de ENAIRe es promover el desarrollo seguro, eficaz, y sostenible del transporte aéreo, otorgando <u>la más alta prioridad a la seguridad</u> en la provisión de los servicios de navegación aérea.</p> <p>Para ofrecer estos servicios se utilizan una serie de infraestructuras en tierra (edificios, equipos informáticos, equipos de telecomunicaciones, infraestructuras auxiliares de energía y climatización, etc.) para los que es fundamental una <u>correcta operación y mantenimiento</u>.</p> <p>La <u>formación</u> es un pilar importante para asegurar que las infraestructuras son correctamente gestionadas y mantenidas. La seguridad se puede ver comprometida si no se actúa con conocimiento y diligencia.</p> <p>Por tanto, el personal de otras empresas contratadas por ENAIRe:</p> <ul style="list-style-type: none">• debe ser consciente, en todo momento, del entorno especialmente sensible en el que se encuentra trabajando;• debe realizar su trabajo siguiendo fielmente las indicaciones técnicas y de seguridad del personal de ENAIRe;• debe tener en cuenta en todo momento la posible repercusión final de cualquier actuación que no esté previamente coordinada con el personal de ENAIRe;• en caso de producirse un error o de detectar una anomalía en el trabajo desempeñado, se deberá informar al personal de ENAIRe para que se puedan poner en marcha las medidas de seguridad necesarias con la mayor rapidez posible. <p>Todo ello con el objetivo final de que el trabajo desempeñado no produzca un efecto indeseado en la correcta operación y mantenimiento de las infraestructuras.</p>		

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

FICHA DE DIVULGACIÓN DE SEGURIDAD OPERACIONAL SERVICIOS EXTERIORES		GEN (2/5)
<u>GESTIÓN DE LA SEGURIDAD</u>		
El concepto actual de gestión de la seguridad tiene su fundamento en una serie de premisas:		
<ul style="list-style-type: none">• La eliminación de todos los accidentes e incidentes es imposible.• El riesgo y el error estarán presentes en todas las actividades y sistemas relacionados con una operación aérea.• Existen riesgos y errores que son asumibles, siempre que estén bajo control.		
De este modo, se define la gestión de la seguridad como la función encargada de mantener un estado en el que el riesgo de lesiones a las personas o daños a los bienes se reduce y se mantiene en un nivel tolerable, o por debajo del mismo (aceptable), por medio de un proceso continuo de identificación de amenazas y gestión de riesgos.		
▪ <u>Conceptos de amenaza y riesgo</u>		
Se denomina amenaza (hazard) a toda condición, evento o circunstancia que potencialmente pueda producir un accidente o afectar a la seguridad. Son sinónimos de amenaza (hazard) los términos <i>peligro, situación/evento peligroso y riesgo potencial</i> , aunque se recomienda la utilización de la primera nomenclatura.		
Se define el riesgo (<i>risk</i>) como la combinación de la probabilidad o frecuencia de aparición de un efecto perjudicial provocado por un hazard y la severidad de dicho efecto. Es importante recalcar la importancia de considerar siempre ambos factores (frecuencia y severidad), sobre todo a la hora de valorar la aceptabilidad de un riesgo.		
Aunque la probabilidad de ocurrencia de un efecto sea muy baja, el riesgo puede no ser aceptable, si sus consecuencias son muy severas. Por el contrario, un riesgo asociado a una amenaza de ocurrencia habitual podría ser aceptable si las consecuencias son menos graves.		
Los niveles de referencia para la seguridad, también llamados simplemente objetivos de seguridad, son los umbrales de aceptabilidad de los riesgos asociados a un entorno operacional específico.		
Los esquemas de clasificación del riesgo proporcionan un criterio de aceptación basado en valoraciones cuantitativas y cualitativas. La posibilidad de admitir un riesgo depende de la relación entre la frecuencia de ocurrencia de un efecto provocado por un hazard y la severidad de dicho efecto.		
En un proceso de gestión de la seguridad, los resultados obtenidos deben evaluarse periódicamente, con objeto de determinar la eficacia de las actividades desarrolladas en este sentido.		
Para ello, se usan una serie de indicadores, cuya naturaleza dependerá de los fenómenos estudiados, que permiten cuantificar - de manera objetiva – las prestaciones alcanzadas en materia de seguridad.		
En cada área de actuación concreta, los indicadores son contrastados con los niveles de referencia establecidos. Cuando se advierte que no se están cumpliendo los requerimientos previos, se ponen en marcha las acciones preventivas y/o correctivas pertinentes que solucionen las desviaciones detectadas.		
Un proceso de análisis y mitigación de riesgos es un conjunto de técnicas que permiten controlar y mantener los niveles de riesgo de un área de actividad determinada, dentro de los límites de aceptabilidad establecidos.		

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

FICHA DE DIVULGACIÓN DE SEGURIDAD OPERACIONAL SERVICIOS EXTERIORES		GEN (3/5)
<p>Dentro de los motivos desencadenantes de un accidente o incidente aéreo, es necesario considerar el concepto de responsabilidad organizativa, en el que se pueden encontrar errores en el diseño de los objetivos de empresa, en la estrategia de comunicación, en la formación del personal o en cualquier aspecto relacionado con la gestión de una determinada actividad.</p>		
<p>▪ <u>Sistema de Gestión de Seguridad (SGS)</u></p> <p>Un sistema de gestión de la seguridad (SGS) es un esquema organizativo y procedimental, mediante el que una organización realiza la gestión formal de la seguridad sobre las actividades desarrolladas.</p> <p>Los SGS constituyen el instrumento para la puesta en práctica de los conceptos fundamentales de gestión de la seguridad y se basan en los siguientes principios:</p> <ul style="list-style-type: none">• Establecimiento de unos criterios formales de actuación respecto a la seguridad y compromiso al más alto nivel organizativo.• Planteamiento de un enfoque sistémico de gestión, aplicable a todos los elementos (organizativos, técnicos, formativos, procedimentales, etc.) de la organización, así como a las posibles interferencias externas.• Desarrollo de procesos orientados a la mejora continua de la seguridad, que incluyan la identificación sistemática de deficiencias en el sistema y amenazas para la seguridad, así como el tratamiento adecuado de los riesgos detectados, a través de técnicas reactivas y proactivas.• Establecimiento de una estructura organizativa específica en la que se precisen las responsabilidades en materia de seguridad.• Disposición de una estructura documental que permita registrar el funcionamiento y los resultados del sistema.• Instauración de una cultura de seguridad que difunda unos principios adecuados de actitud y responsabilidad en todos los miembros de la organización, dentro de un planteamiento orientado a aprender de los errores, y un entorno laboral de confianza, sin temor a medidas punitivas.		
<p>Requisitos para alcanzar la seguridad</p> <ul style="list-style-type: none">○ Competencia del personal: El personal de la organización debe alcanzar y mantener un nivel de capacitación adecuado, tanto en sus funciones específicas, como en aquéllas relacionadas con la seguridad. Para ello, la organización ha de disponer los procesos adecuados para la selección del personal y su adiestramiento.○ Niveles cuantificables de seguridad: A partir de los criterios especificados en la normativa correspondiente, la organización debe determinar unos niveles cuantificables de seguridad para los servicios que proporciona. Asimismo, se dispondrán los medios y los procedimientos necesarios para garantizar su cumplimiento.○ Análisis de seguridad: La implantación de nuevos servicios o sistemas, así como su modificación, requerirá un proceso previo de análisis y mitigación de riesgos. Posteriormente, se efectuarán evaluaciones periódicas de seguridad durante la vida útil de dichos servicios y sistemas, de modo que cualquier cambio sustancial o situación de riesgo detectada implicará la realización de un nuevo análisis.		
<p>Requisitos para mantener la seguridad</p> <ul style="list-style-type: none">○ Notificación y tratamiento de incidencias: La organización ha de definir procedimientos que faciliten la comunicación inmediata, por parte del personal, de cualquier evento o circunstancia que pueda comprometer la seguridad. Si tienes conocimiento de una incidencia de seguridad, notifícalo. Dichas incidencias deberán ser analizadas con el único fin de determinar las medidas correctoras/preventivas que eviten su repetición.○ Inspecciones y auditorías de seguridad: La organización debe examinar los servicios suministrados y realizar auditorías periódicas de los procesos relacionados con la seguridad, con objeto de verificar el cumplimiento de los requisitos establecidos y recomendar mejoras, cuando sea necesario.		

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

FICHA DE DIVULGACIÓN DE SEGURIDAD OPERACIONAL SERVICIOS EXTERIORES		GEN (4/5)
<ul style="list-style-type: none">○ Formación en seguridad: La organización ha de proporcionar programas de instrucción y cursos de refresco para garantizar que el personal mantenga actualizados los conocimientos y las habilidades necesarias para desempeñar sus funciones de manera acorde a los requisitos de seguridad.○ Seguimiento de la seguridad: La organización debe disponer métodos de observación que permitan detectar, con antelación suficiente, tendencias negativas en los procesos relacionados con la seguridad, que impidan conseguir o mantener los niveles fijados.○ Gestión documental de la seguridad: La información relacionada con los procesos de gestión de la seguridad debe documentarse y archivarse adecuadamente. El registro de las acciones realizadas y los resultados obtenidos, permitirá valorar las prestaciones del sistema y las acciones necesarias para su perfeccionamiento. Dentro del ciclo mencionado, los datos y resultados obtenidos en la fase de mantenimiento de la seguridad permitirán evaluar el estado de sistema y actualizar los objetivos a alcanzar, en un proceso de mejora continuo. <p>■ <u>Cultura de seguridad</u></p> <p>La cultura de seguridad es la forma en la que la seguridad es percibida, valorada y priorizada por una organización. En términos más formales, es el producto de los valores individuales y de grupo, actitudes, responsabilidades y patrones de comportamiento que determinan el compromiso, modelo y competencia de la gestión de la seguridad en una organización. El enfoque de la cultura de seguridad en una organización es responsabilidad de su personal directivo y tiene un impacto directo en el resultado de la gestión de seguridad, ya que conforma la disposición del personal respecto a la misma. Una cultura de seguridad positiva es aquélla en la que la seguridad tiene carácter prioritario y todas las decisiones se toman teniendo en cuenta las repercusiones para la misma. También se requiere la conciencia de que una estrategia adecuada para la seguridad precisa la involucración de cada uno de los miembros de la organización, a todos los niveles. Asimismo, se necesita un compromiso firme de la dirección con estos principios, garantizando el desarrollo de acciones para su implementación, desarrollo, difusión y seguimiento.</p>		

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

FICHA DE DIVULGACIÓN DE SEGURIDAD OPERACIONAL SERVICIOS EXTERIORES		GEN (5/5)
<u>SERVICIOS Y SUMINISTROS RELATIVOS AL EQUIPAMIENTO DE LOS SISTEMAS CNS/ATM O SISTEMAS AUXILIARES (GENERAL)</u>		
<p>Desde el punto de vista de la seguridad operacional, los objetivos principales en los servicios o suministros relativos al equipamiento de los sistemas CNS/ATM o sistemas auxiliares son:</p> <ol style="list-style-type: none">1. Tratar de evitar al máximo la ocurrencia de deficiencias o periodos de carencia no programados en el equipamiento del sistema de Navegación Aérea.2. Tratar de restablecer lo más rápidamente posible el equipamiento sistema de comunicaciones a su estado operativo normal cuando éste haya sufrido algún tipo de degradación.		
<p><u>Riesgos Funcionales:</u></p> <p>El riesgo es la combinación entre la probabilidad de ocurrencia de un efecto perjudicial inducido por un evento no deseado y la gravedad de ese efecto.</p> <p>Como consecuencia del ejercicio de sus funciones y responsabilidades, el personal relacionado con los servicios y suministros relativos al equipamiento de los sistemas CNS/ATM o sistemas auxiliares deberá implantar las medidas para evitar, detectar y corregir los eventos no deseados, de forma que no haya repercusiones en la capacidad para proporcionar servicios de NA o deterioro de los mismos.</p>		
<p><u>Riesgos en Actuaciones:</u></p> <p><u>Coordinaciones:</u></p> <p>Las actuaciones a realizar en las instalaciones y equipamiento deberán estar previamente coordinadas con los responsables de dichas instalaciones, elaborándose las planificaciones y documentación aplicable con objeto de evitar y/o mitigar los riesgos que pudieran producirse en el propio servicio o en los colindantes.</p>		
<p><u>Notificación</u></p> <p>El personal relacionado con los servicios y suministros relativos al equipamiento de los sistemas CNS/ATM o sistemas auxiliares (así como en cualquier otro ámbito de Navegación Aérea) deberá notificar cualquier situación que considere peligrosa o con impacto real o potencial en la seguridad del servicio, tales como la no realización o planificación inadecuada de tareas programadas, sucesos técnicos que hayan tenido impacto en la operación o el servicio proporcionado, etc.</p>		

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

ENAIRe	FICHA DE DIVULGACIÓN DE SEGURIDAD OPERACIONAL SERVICIOS EXTERIORES	COM (1/2)
ÁREA DE COMUNICACIONES		
Desde el punto de vista de la seguridad operacional, los objetivos principales del mantenimiento del sistema de comunicaciones aeronáuticas son:		
<ol style="list-style-type: none">1. Tratar de evitar al máximo la ocurrencia de deficiencias o períodos de carencia no programados en el sistema de comunicaciones aeronáuticas.2. Tratar de restablecer lo más rápidamente posible el sistema de comunicaciones a su estado operativo normal cuando éste haya sufrido algún tipo de degradación.		
<u>Riesgos Funcionales:</u>		
El riesgo es la combinación entre la probabilidad de ocurrencia de un efecto perjudicial inducido por un evento no deseado y la gravedad de ese efecto.		
En el ámbito de comunicaciones, se identifican con carácter general los siguientes eventos no deseados (amenazas):		
Función de Comunicaciones con Aeronaves (CAT)		
AMENAZA	COMENTARIOS	
Pérdida total de comunicaciones con todas las aeronaves	Esta amenaza se produce cuando se pierden todas las frecuencias disponibles en todos los objetos de responsabilidad de torre a través del equipamiento principal.	
Pérdida parcial de comunicaciones con todas las aeronaves	Esta amenaza surge cuando se produce una pérdida total de comunicaciones en un único objeto de responsabilidad de la torre. Es decir, no está disponible ni la frecuencia principal ni la de emergencia, y no están operativos ni el transceptor fijo de la posición ni el transceptor portátil de la torre.	
Error detectado en las comunicaciones con las aeronaves	Esta amenaza surge ante la aparición de interferencias o cualquier otro problema asociado al equipamiento que provoque una degradación de la calidad con la que se reciben las comunicaciones entre el controlador y el piloto.	
Error no detectado en la comunicación con las aeronaves	Esta amenaza surge ante la aparición de interferencias o cualquier otro problema asociado al equipamiento que provoque una degradación de la calidad con la que se reciben las comunicaciones y que provoque malentendidos entre controlador y piloto.	
Amenazas detectadas: CAT – Comunicaciones con Aeronaves		

Requisitos de Seguridad (Safety) – Interfaz SCV-SACTA

FICHA DE DIVULGACIÓN DE SEGURIDAD OPERACIONAL SERVICIOS EXTERIORES		COM (2/2)
--	--	--------------

Función de Comunicaciones con colaterales y Agentes Externos (CTT)

AMENAZA	COMENTARIOS
Pérdida total o parcial de comunicaciones con otras dependencias ATS	Esta amenaza surge ante la aparición de interferencias o cualquier otro problema asociado al equipamiento que provoque una degradación de la calidad con la que se reciben las comunicaciones y que provoque malentendidos entre los controladores de la TWR y las dependencias colaterales (APPs y/o ACCs).
Error sin detectar de comunicaciones con otras dependencias ATS	Esta amenaza surge ante la posible aparición de interferencias u otros problemas asociados al equipamiento que provoque una degradación de la calidad con la que se reciben las comunicaciones y que provoque malentendidos entre los controladores de la TWR y las dependencias colaterales (APPs y/o ACCs).
Pérdida o errores de comunicaciones con otros agentes externos	Esta amenaza engloba todas las posibles incidencias relativas a las comunicaciones de la TWR con cualquier agente externo (vehículos en tierras, aeropuerto, oficina de meteorología, etc.), es decir exceptuando tanto a las aeronaves como a las dependencias colaterales. Se contemplan tanto pérdidas totales o parciales como degradación de las comunicaciones.

Amenazas detectadas: CTT - Comunicaciones con colaterales y Agentes Externos

La severidad de los efectos de una amenaza dependerá del contexto y debe ser evaluada por los expertos operativos y técnicos relacionados directamente con ese sistema.

Como consecuencia del ejercicio de sus funciones y responsabilidades, el personal en el ámbito de comunicaciones deberá implantar las medidas para evitar, detectar y corregir, los eventos no deseados citados con anterioridad, de forma que no haya repercusiones en la capacidad para proporcionar servicios de NA o deterioro de los mismos.

Riesgos en Actuaciones:**Coordinaciones:**

Las actuaciones a realizar en las instalaciones y equipamiento deberán estar previamente coordinadas con los responsables de dichas instalaciones, elaborándose las planificaciones y documentación aplicable con objeto de evitar y/o mitigar los riesgos que pudieran producirse en el propio servicio o en los colindantes.

Notificación

El personal que trabaja en el ámbito de comunicaciones (así como en cualquier otro ámbito de Navegación Aérea) deberá notificar cualquier situación que considere peligrosa o con impacto real o potencial en la seguridad del servicio, tales como la no realización o planificación inadecuada de tareas programadas, sucesos técnicos que hayan tenido impacto en la operación o el servicio proporcionado, etc.

Pliego de Prescripciones Técnicas:

Desarrollo e implantación de Interfaz SCV-SACTA en Torres con Servicio de Aproximación

ANEXO IV

Requisitos de Interoperabilidad (UE) 2018/1139

División de Comunicaciones

Código: DSIS-13-DTC-045-3.0

Elaborado: 09/03/2020

Página: 1/8

Requisitos de Interoperabilidad – División de Comunicaciones

Aprobaciones del documento

Elaborado por:	Revisado por:	Aprobado por:
Visado en Internav	Visado en Internav	Visado en Internav
Luis Miguel Pérez Montes <i>Seguridad (safety) y Verificación A.T. Externa ISDEFE</i>	Aurora Sánchez Barro <i>Jefe Departamento Sistemas Comunicaciones T/A</i>	Manuel García Martín <i>Jefe División Comunicaciones</i>
Silvia Alonso Barril <i>Seguridad (safety) y Verificación A.T. Externa ISDEFE</i>	Ángel Crespo Pérez <i>Jefe Departamento Comunicaciones T/T</i>	

Control de Cambios

En la siguiente tabla figuran al menos las tres últimas modificaciones efectuadas en el presente documento.

Edición	Fecha	Páginas afectadas	Cambios
3.0	09/03/2020	4, 6 y 7	Incorporación del reglamento (UE) Nº 2018/1139.
2.0	07/05/2018	Todas	Actualización formato ENAIRe. Actualizar y ampliar listado normativa. Incluir ejemplos de evidencias en el punto 5.
1.0	10/05/2013	Todas	Creación del documento.

Hoja de Control de Documentación Impresa

Edición	Fecha de Entrada en Vigor	Responsable de la Impresión	Fecha de Impresión	Páginas Impresas	Firma

Esta hoja de control garantiza que la copia del documento en papel se corresponde con el documento contenido en el gestor documental de ENAIRe vigente en el momento de la impresión. En caso de que esta hoja de control no esté cumplimentada se considerará que la copia en papel es meramente informativa pudiendo no corresponder con la versión en vigor del documento.

Formato empleado: A14-09-PL-001-3.0

Requisitos de Interoperabilidad – División de Comunicaciones

ÍNDICE

1. Objeto.....	4
2. Ámbito de Aplicación	4
3. Documentación de Referencia y Normativa aplicable	4
4. Requisitos de Interoperabilidad (RIOP)	5
5. Proceso de Verificación	6
1. Diseño global.....	7
2. Desarrollo e integración del sistema.....	7
3. Integración operacional del sistema.....	8
4. Disposiciones sobre Mantenimiento.....	8

Requisitos de Interoperabilidad – División de Comunicaciones

1. Objeto

El objeto de éste documento es determinar los requisitos de interoperabilidad (RIOP) que deben incluirse en los Pliegos de Prescripciones Técnicas de la División de Comunicaciones así como la definición de las evidencias que el potencial proveedor exterior deberá proporcionar para demostrar el cumplimiento de los requisitos de interoperabilidad establecidos.

De este modo, se da cumplimiento al Reglamento (CE) Nº 552/2004 y (UE) Nº 2018/1139 de Interoperabilidad, siguiendo el material guía de Eurocontrol [2].

2. Ámbito de Aplicación

El ámbito de aplicación del presente documento son los expedientes de suministro de la División de Comunicaciones en los que se incluyan elementos HW y/o SW que vayan a utilizarse en los Sistemas de Navegación Aérea de ENAIRe.

3. Documentación de Referencia y Normativa aplicable

Documentación Interna – ENAIRe

[1]	S22-07-PES-001-5.0 Procedimiento Verificación CE de Sistemas.
-----	---

Documentación Externa – Reglamentos y Estándares aplicables

[2]	Reglamento (CE) Nº 552/2004, relativo a la interoperabilidad de la red europea de gestión del tránsito aéreo. Nota: Este reglamento está derogado por el (UE) 2018/1139, excepto los artículos 4,5,6,6 bis y 7 y los anexos III y IV, que seguirán aplicándose a más tardar hasta el 12/09/2023.
[3]	Reglamento (UE) Nº 2018/1139 , sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de la Unión Europea para la Seguridad Aérea y por el que se modifican los Reglamentos (CE) Nº 2111/2005, (CE) Nº 1008/2008, (UE) Nº 996/2010, (CE) Nº 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) Nº 552/2004 y (CE) Nº 216/2008 del Parlamento Europeo y del Consejo y el Reglamento (CEE) Nº 3922/91 del Consejo. Nota: Este reglamento entró en vigor el 24/07/2018. Se aplica en ENAIRe desde enero 2020.
[4]	Reglamento (CE) Nº 1032/2006, por el que se establecen requisitos para los sistemas automáticos de intercambio de datos de vuelo a efectos de notificación, coordinación y transferencia de vuelos entre dependencias de control del tránsito aéreo.
[5]	Reglamento (CE) Nº 633/2007, por el que se establecen requisitos para la aplicación de un protocolo de transferencia de mensajes de vuelo utilizado a efectos de notificación, coordinación y transferencia de vuelos entre dependencias de control del tránsito aéreo.
[6]	Reglamento (CE) Nº 29/2009, por el que se establecen requisitos relativos a los servicios de enlace de datos para el cielo único europeo.

Requisitos de Interoperabilidad – División de Comunicaciones

[7]	Reglamento (CE) Nº 30/2009, por el que se modifica el Reglamento CE Nº 1032/2006 en los requisitos para los sistemas automáticos de intercambio de datos de vuelo que dan soporte a los servicios de enlace de datos.
[8]	Reglamento (EU) Nº 73/2010, por el que se establecen requisitos relativos a la calidad de los datos aeronáuticos y la información aeronáutica para el cielo único europeo.
[9]	Reglamento (EU) Nº 283/2011, por el que se modifica el Reglamento CE Nº 633/2007 en lo que atañe a las disposiciones transitorias a las que se refiere el artículo 7.
[10]	Reglamento (EU) Nº 1206/2011, por el que se establecen los requisitos en materia de identificación de aeronaves para la vigilancia del cielo único europeo.
[11]	Reglamento (EU) Nº 1207/2011, por el que se establecen requisitos de rendimiento e interoperabilidad de la vigilancia del cielo único europeo.
[12]	Reglamento EU Nº 1079/2012, por el que se establecen requisitos de separación entre canales de voz para el Cielo Único Europeo.
[13]	Reglamento (EU) Nº 657/2013, que modifica el Reglamento de Ejecución (UE) Nº 1079/2012 por el que se establecen requisitos de separación entre canales de voz para el Cielo Único Europeo.
[14]	Reglamento (EU) Nº 1029/2014, que modifica el Reglamento (UE) Nº 73/2010 por el que se establecen requisitos relativos a la calidad de los datos aeronáuticos y la información aeronáutica para el cielo único europeo.
[15]	Reglamento (EU) Nº 716/2014, relativo al establecimiento del Proyecto Piloto Común destinado a respaldar la ejecución del Plan Maestro de Gestión del Tránsito Aéreo Europeo.
[16]	Reglamento (EU) Nº 1028/2014, que modifica el Reglamento de Ejecución (UE) Nº 1207/2011, por el que se establecen los requisitos de rendimiento e interoperabilidad de la vigilancia del cielo único europeo.
[17]	Reglamento (EU) Nº 310/2015, que modifica el Reglamento (CE) Nº 29/2009 por el que se establecen requisitos relativos a los servicios de enlace de datos para el cielo único europeo y deroga el Reglamento de Ejecución (UE) Nº 441/2014.
[18]	Eurocontrol-GUID-137. Guidelines on conformity assessment for the interoperability Regulation of the SES, v3.0.

4. Requisitos de Interoperabilidad (RIOP)

Antes de su entrada en servicio, cualquier sistema requerido por ENAIRe para respaldar las funciones y servicios listados en el punto 3.1 del Anexo VIII del Reglamento (UE) 2018/1139 (en particular los servicios de Comunicaciones), deberá satisfacer los Requisitos Esenciales para los Servicios de Navegación Aérea (SNA), en concreto los definidos en el Anexo VIII, punto 3 (3.1, 3.2, 3.3 y 3.4) del Reglamento (UE) 2018/1139.

Para satisfacer esta Reglamentación aplicable, ENAIRe deberá someter cada uno de sus sistemas a un proceso de verificación del cumplimiento de los requisitos de interoperabilidad, previo a su entrada en servicio. Para cada expediente los sistemas a verificar serán los definidos en el propio PPT y en las Especificaciones Técnicas adjuntas al mismo.

Requisitos de Interoperabilidad – División de Comunicaciones

Un sistema puede dividirse en componentes, entendidos éstos como partes constituyentes del mismo. Debido a que en la Reglamentación de interoperabilidad aplicable no se define ningún componente, a excepción del componente “Transmisor/Receptor” definido en el Artículo 4.7 del Reglamento (EU) Nº 1079/2012, se considerará de forma general asimilable el sistema a un solo componente. No obstante, para cada expediente, se podrá utilizar la definición de componentes de que disponga el oferente, previa aprobación por parte de ENAIRe.

A continuación se listan los requisitos de interoperabilidad (RIOP) que deberá cumplir el potencial proveedor exterior:

RIOP1. Los componentes objeto del presente pliego de prescripciones técnicas deberán ir acompañados de una Declaración CE de Conformidad (DoC) o de Idoneidad para el Uso (DSU) según se indica en el Reglamento (CE) Nº 552/2004 (artículo 5.1, todavía en vigor).

Nota: para la elaboración de estos documentos se recomienda utilizar las plantillas definidas por Eurocontrol (<http://www.eurocontrol.int/conformity>)

RIOP2. El fabricante, su representante autorizado o el proveedor exterior, según aplique, deberá garantizar y declarar, mediante la Declaración CE de Conformidad (DoC) o de Idoneidad para el Uso (DSU), que ha aplicado las disposiciones establecidas en los requisitos esenciales y en las correspondientes medidas de ejecución en materia de interoperabilidad según se indica en el Reglamento (CE) Nº 552/2004 (artículo 5.2, todavía en vigor) y se expone en este documento.

Nota: La definición de los componentes se acordará con el adjudicatario del expediente.

Nota: Considerar los requisitos esenciales del reglamento en vigor, (UE) 2018/1139 (Anexo VIII punto 3).

RIOP3. El proveedor exterior proporcionará toda la documentación necesaria relativa al equipamiento objeto del expediente, para que antes de la entrada en servicio de los sistemas, ENAIRe pueda elaborar la declaración CE de verificación de los sistemas que confirme el cumplimiento de los requisitos de interoperabilidad establecidos en la reglamentación aplicable y que se detallan en el punto 3 de este documento.

5. Proceso de Verificación

El proceso de verificación tendrá como resultado final dos documentos elaborados por ENAIRe, cuyo contenido se define en el Anexo IV (Sistemas) del Reglamento (CE) Nº 552/2004 (**el anexo IV sigue en vigor**) y que son:

- Una Declaración CE de Verificación (DoV).
- Un Expediente Técnico (ET) anexo a la misma: que contendrá la documentación y evidencias aportadas por el contratista en las diferentes fases de la verificación.

Las fases de verificación son las definidas en el **Anexo IV (Sistemas) del (CE) Nº 552/2004 (el anexo IV sigue en vigor)**, mencionado y son:

Requisitos de Interoperabilidad – División de Comunicaciones

1. Diseño global.

Para verificar que el diseño del sistema da cumplimiento a los requisitos de interoperabilidad aplicables al mismo, el contratista deberá demostrar que en el diseño se ha tenido en cuenta una determinada documentación de referencia. Para ello, deberá aportar la Declaración CE de Conformidad (DoC) o Declaración CE de Idoneidad para el Uso (DSU) del o los componente/s que constituyen el sistema, junto con las evidencias que demuestren la trazabilidad entre los requisitos de interoperabilidad aplicables y la documentación de referencia.

Esta documentación de referencia debería ser al menos la utilizada en la redacción de las Especificaciones Técnicas del sistema referenciadas en el PPT. Es obligatorio entregar las evidencias del cumplimiento con los requisitos derivados de la documentación de OACI y/o EUROCAE, y altamente recomendable entregar las evidencias del cumplimiento en la fase de diseño de los requisitos derivados de las Especificaciones de ENAIRe y otros organismos internacionales especificados en el Pliego.

El oferente incluirá en la oferta aquellas evidencias de cumplimiento que disponga contra cualquier reglamentación mencionada en el párrafo anterior. El contratista, tras acordarlo con ENAIRe, entregará las evidencias documentales de cumplimiento de los requisitos acordados en la fase de diseño.

Además, en aquellos casos en que sea aplicable, se deberá presentar la etiqueta CE de cumplimiento de las Directivas RTT&E relacionadas en la documentación aplicable en el PPT.

A modo de resumen, y de cara a ayudar al cumplimiento del requisito RIOP3, se incluyen a continuación un listado ejemplo de las evidencias requeridas para esta fase:

- Declaración CE de Conformidad (DoC) o Declaración CE de Idoneidad para el Uso del o los componentes (DSU) que constituyen el sistema, junto con las evidencias que demuestren la trazabilidad entre los requisitos de interoperabilidad aplicables y la documentación de referencia.
- Documentación de características técnicas del sistema o de diseño del sistema (HW y SW).
- Documentación de seguridad pertinente (HW y SW).
- Documentación de disponibilidad y fiabilidad del sistema.
- Informe de análisis de interferencias (para sistemas T/A, si se considera necesario).
- Certificado o Declaración CE de Conformidad (DoC) con la Directiva 2014/53/UE sobre la comercialización de equipos radioeléctricos del componente.

2. Desarrollo e integración del sistema.

Para verificar que el sistema se ha desarrollado e integrado teniendo en cuenta los requisitos de interoperabilidad aplicables al mismo, el contratista deberá presentar evidencias que demuestren la trazabilidad entre estos requisitos de interoperabilidad aplicables y las pruebas de integración del sistema (FAT-Factory Acceptance Test).

A modo de resumen, y de cara a ayudar al cumplimiento del requisito RIOP3, se incluyen a continuación un listado ejemplo de las evidencias requeridas para esta fase:

- Protocolos de pruebas en fábrica y/o maqueta (FAT).

Requisitos de Interoperabilidad – División de Comunicaciones

- Registro de pruebas FAT y/o maqueta (en caso de que el fabricante no las proporcione, el proveedor exterior deberá realizarlas en sus instalaciones).
- Protocolos de pruebas de Validación (para sistemas T/A y SCV desplegados por el Departamento de Comunicaciones de Sistemas Tierra/Aire).
- Registro de resultados del protocolo de pruebas de Validación o informe de validación.
- Protocolos de pruebas de Integración (para sistemas T/A y SCV desplegados por el Departamento de Comunicaciones de Sistemas Tierra/Aire).
- Registro de resultados del protocolo de pruebas de Integración.

3. Integración operacional del sistema.

Para verificar que el sistema se ha integrado en su entorno operacional teniendo en cuenta los requisitos de interoperabilidad aplicables al mismo, el contratista deberá presentar evidencias que demuestren la trazabilidad entre estos requisitos de interoperabilidad aplicables y las pruebas de integración operacional del sistema en emplazamiento (SAT-Site Acceptance Test) y, si son aplicables, las pruebas de verificación en vuelo.

A modo de resumen, y de cara a ayudar al cumplimiento del requisito RIOP3, se incluyen a continuación un listado ejemplo de las evidencias requeridas para esta fase:

- Protocolos de pruebas en emplazamiento (SAT).
- Registro de pruebas SAT.
- Protocolos de pruebas de Aceptación (para sistemas T/A y SCV desplegados por el Departamento de Comunicaciones de Sistemas Tierra/Aire).
- Registro de resultados del protocolo de pruebas de Aceptación y/o informe de validación.

4. Disposiciones sobre Mantenimiento.

Para verificar que en la elaboración de los procedimientos de mantenimiento del sistema se han tenido en cuenta los requisitos de interoperabilidad aplicables al mismo, el contratista deberá presentar evidencias que demuestren la trazabilidad entre estos requisitos de interoperabilidad aplicables y los manuales de mantenimiento y de operación del sistema.

Con el fin de demostrar que toda la documentación presentada ha sido suficientemente revisada, se presentará un certificado ISO 9001 y la evidencia de que bajo este certificado se dispone de un procedimiento de elaboración y revisión de la documentación de mantenimiento y operación.

A modo de resumen, y de cara a ayudar al cumplimiento del requisito RIOP3, se incluyen a continuación un listado ejemplo de las evidencias requeridas para esta fase:

- Certificado ISO 9001, del Integrador y fabricantes de los sistemas.
- Manuales de usuario, operación y de mantenimiento.

PRESUPUESTO DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACION DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

Elaborado: 14/05/2020

Página: 1/4

**PRESUPUESTO DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE
INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN**

Índice

1. PRESUPUESTO.....	3
2. REQUISITOS DE LA PROPOSICIÓN ECONÓMICA.....	4

PRESUPUESTO DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

1. Presupuesto

Partida	Ref. PPT	Denominación	P.Total
1		DESARROLLO PROXY SACTA - SCV	
1.1		Desarrollo y validación PROXY para Interfaz SACTA-SCV según ANEXOS 1 y 2 al PPT	145.000,00 €
		SUBTOTAL	145.000,00 €
2		SERVICIOS ASOCIADOS AEROPUERTO TENERIFE NORTE	
2.1		Instalación, pruebas y puesta en servicio según ANEXO 1 al PPT	48.400,00 €
2.2		Documentación según ANEXO 1 al PPT	18.130,00 €
2.3		Formación según ANEXO 1 al PPT	5.250,00 €
2.4		Asistencia técnica según ANEXO 1 al PPT	3.100,00 €
		SUBTOTAL	74.880,00 €
3		SERVICIOS ASOCIADOS AEROPUERTO TENERIFE SUR	
3.1		Instalación, pruebas y puesta en servicio según ANEXO 1 al PPT	48.400,00 €
3.2		Documentación según ANEXO 1 al PPT	18.130,00 €
3.3		Formación según ANEXO 1 al PPT	5.250,00 €
3.4		Asistencia técnica según ANEXO 1 al PPT	3.100,00 €
		SUBTOTAL	74.880,00 €
4		SERVICIOS ASOCIADOS AEROPUERTO BILBAO	
4.1		Instalación, pruebas y puesta en servicio según ANEXO 1 al PPT	48.400,00 €
4.2		Documentación según ANEXO 1 al PPT	18.130,00 €
4.3		Formación según ANEXO 1 al PPT	5.250,00 €
4.4		Asistencia técnica según ANEXO 1 al PPT	3.100,00 €
		SUBTOTAL	74.880,00 €
5		SERVICIOS ASOCIADOS AEROPUERTO SANTIAGO	
5.1		Instalación, pruebas y puesta en servicio según ANEXO 1 al PPT	48.400,00 €
5.2		Documentación según ANEXO 1 al PPT	18.130,00 €
5.3		Formación según ANEXO 1 al PPT	5.250,00 €
5.4		Asistencia técnica según ANEXO 1 al PPT	3.100,00 €
		SUBTOTAL	74.880,00 €
		TOTAL	444.520,00 €

El importe límite del presente expediente asciende a CUATROCIENTOS CUARENTA Y CUATRO MIL QUINIENTOS VEINTE EUROS (444.520,00 €), impuestos no incluidos.

Cualquier versión impresa o en soporte informático, total o parcial de este documento, se considera como copia no controlada y siempre debe ser contrastada con su versión vigente en el Gestor Documental de ENAIRe.

PRESUPUESTO DEL EXPEDIENTE DE ASISTENCIA PARA EL DESARROLLO E IMPLANTACIÓN DE INTERFAZ SCV-SACTA EN TORRES CON SERVICIO DE APROXIMACIÓN

2. Requisitos de la proposición económica

En la Proposición Económica se presentará un Presupuesto Desglosado con una relación de los capítulos en que se listarán los conjuntos y subconjuntos que constituyen los sistemas a suministrar e instalar y los servicios asociados a realizar. Es de obligado cumplimiento que en la oferta se desglose en partidas unitarias, todos y cada uno de los elementos y equipos que integran el suministro, indicando la cantidad de unidades a suministrar.

En la Proposición Económica se desglosará una partida económica específica para la Formación. Se deberán detallar los importes unitarios de cada uno de los cursos, documentaciones, materiales, instructores y demás gastos de esta partida.

Los precios ofertados resultarán contractuales, una vez realizada la adjudicación.

Realizado por:

SANCHEZ
BARRO
AURORA -
08977040W

Fdo.: Aurora Sánchez Barro

Firmado digitalmente por SANCHEZ
BARRO AURORA - 08977040W
Nombre de reconocimiento (DN):
c=ES
serialNumber=IDCES-08977040W,
givenName=AURORA, sn=SANCHEZ
BARRO, cn=SANCHEZ BARRO
AURORA - 08977040W
Fecha: 2020.05.14 11:10:42 +02'00'

Aprobado por:

García
Martín,
Manuel
Fdo.: Manuel García Martín

Firmado digitalmente por García
Martín, Manuel
Nombre de reconocimiento (DN):
dc=es, dc=nav, dc=na, dc=lean,
ou=Direccion de Sistemas,
ou=Division Comunicaciones,
cn=García Martín, Manuel,
email=mangarcia@enaire.es
Fecha: 2020.05.14 17:21:53 +02'00'