

SSA – SYSTEM SAFETY ASSESSMENT

SWAL – SOFTWARE ASSURANCE LEVEL

DT-A-25X-GRALD-001-SFTY-00-S-00

REGISTRO DE MODIFICACIONES

|  |  |  |  |
| --- | --- | --- | --- |
| Edición | Revisión | Fecha | Modificación |
| 1.0 |  | 28/02/17 | Versión inicial |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

ÍNDICE

[1. OBJETO 7](#_Toc476297098)

[1.1. ALCANCE 7](#_Toc476297099)

[1.2. ESTRUCTURA 7](#_Toc476297100)

[1.3. DOCUMENTOS DE REFERENCIA 8](#_Toc476297101)

[1.4. ABREVIATURAS 10](#_Toc476297102)

[2. DESCRIPCIÓN DEL SISTEMA 12](#_Toc476297103)

[2.1. Arquitectura HW 15](#_Toc476297104)

[2.2. Arquitectura SW 17](#_Toc476297105)

[3. PROCESO DE EVALUACIÓN DE LA SEGURIDAD 20](#_Toc476297106)

[4. ANALISIS FUNCIONAL DE AMENAZAS (FHA) 26](#_Toc476297107)

[4.1. INTRODUCCIÓN 26](#_Toc476297108)

[4.2. IDENTIFICACIÓN DE LAS FUNCIONES 26](#_Toc476297109)

[4.3. IDENTIFICACION DE LAS AMENAZAS 33](#_Toc476297110)

[4.4. IDENTIFICACION DE LOS EFECTOS 34](#_Toc476297111)

[4.5. IDENTIFICACIÓN DE ACCIONES DE MITIGACIÓN 37](#_Toc476297112)

[4.6. PROBABILIDAD 40](#_Toc476297113)

[4.7. SEVERIDAD 42](#_Toc476297114)

[4.8. PROCESO DE ASIGNACIÓN SWAL 47](#_Toc476297115)

[4.9. TABLAS RESULTANTES DEL ANÁLISIS 50](#_Toc476297116)

[5. CARPETA DE SEGURIDAD SOFTWARE (SSF) 106](#_Toc476297117)

[5.1. PARTE 1: ENTORNO 106](#_Toc476297118)

[5.1.1. DESCRIPCION DEL SISTEMA 106](#_Toc476297119)

[5.1.2. ENTORNO OPERACIONAL 106](#_Toc476297120)

[5.1.3. LISTADO DE HERRAMIENTAS 106](#_Toc476297121)

[5.2. Parte 2: Contexto de la Garantía de la Seguridad SW 108](#_Toc476297122)

[5.2.1. Regulación aplicable 108](#_Toc476297123)

[5.2.2. Estándares aplicables 109](#_Toc476297124)

[5.2.3. Análisis y Mitigación de Riesgos 110](#_Toc476297125)

[5.3. Parte 3: Proceso de Garantía de la Seguridad SW 112](#_Toc476297126)

[5.3.1. Plan de Gestión de la Seguridad 112](#_Toc476297127)

[5.3.2. Revisión del PLAN 114](#_Toc476297128)

[5.3.3. Listado de documentación 115](#_Toc476297129)

[5.4. Parte 4: Requisitos de Seguridad 116](#_Toc476297130)

[5.4.1. Listado de Requisitos de Seguridad del SOFTWARE 116](#_Toc476297131)

[5.5. Parte 5: Modificaciones de Software 119](#_Toc476297132)

[5.5.1. Gestión de Cambios 119](#_Toc476297133)

[5.5.2. Gestión de Incidencias 120](#_Toc476297134)

[5.5.3. Retirada, desinstalación de Software 123](#_Toc476297135)

[5.6. Parte 6: COTS 124](#_Toc476297136)

[5.6.1. Plan de Garantía y conformidad para COTS 124](#_Toc476297137)

[5.7. Parte 7: Garantías 126](#_Toc476297138)

[5.7.1. Garantía de herramientas 126](#_Toc476297139)

[5.7.2. Asignación de SWAL y monitorización 126](#_Toc476297140)

[5.7.3. Auditorias y revisiones 128](#_Toc476297141)

[5.7.4. Formación 132](#_Toc476297142)

[5.7.5. Requisitos SOFTWARE 133](#_Toc476297143)

[5.7.6. Matriz de trazabilidad 133](#_Toc476297144)

[5.7.7. Funciones no deseadas 135](#_Toc476297145)

[5.7.8. Satisfacción de requisitos 136](#_Toc476297146)

[5.7.9. Gestión de la configuración 138](#_Toc476297147)

[5.7.10. Plan de desarrollo del Software 138](#_Toc476297148)

[5.7.11. Mantenimiento 138](#_Toc476297149)

[5.7.12. Verificación 140](#_Toc476297150)

[5.7.13. Calidad 142](#_Toc476297151)

[5.7.14. Garantía de que el SW es aceptablemente seguro 142](#_Toc476297152)

[6. TRAZABILIDAD DE REQUISITOS 143](#_Toc476297153)

ÍNDICE DE FIGURAS

[Fig. 1 Arquitectura Hardware. Diagrama General de Bloques 15](#_Toc476297154)

[Fig. 2 Arquitectura Software. Diagrama General 17](#_Toc476297155)

[Fig. 3 Proceso de Evaluación de la Seguridad 21](#_Toc476297156)

[Fig. 4 Diagrama de Estados para peticiones tipo “incidencia” 120](#_Toc476297157)

[Fig. 5 Datos a introducir en una incidencia. 122](#_Toc476297158)

ÍNDICE DE TABLAS

[Tabla 1. Relación Módulos Hardware y Módulos Software 19](#_Toc476297159)

[Tabla 2. Estructura de carpetas para un desarrollo software 22](#_Toc476297160)

[Tabla 3. Estructura de carpetas para un desarrollo software con garantía de seguridad 24](#_Toc476297161)

[Tabla 4. Relación entre Funciones y Módulos Software 32](#_Toc476297162)

[Tabla 5. Amenazas y Efectos. 36](#_Toc476297163)

[Tabla 6. Amenazas y Mitigaciones. 39](#_Toc476297164)

[Tabla 7. Niveles de Severidad 46](#_Toc476297165)

[Tabla 8. Relación de SWAL con la probabilidad y severidad de los fallos 47](#_Toc476297166)

[Tabla 9. SWAL creciente. Probabilidad y severidad. 48](#_Toc476297167)

[Tabla 10. Comunicaciones Tierra / Aire – Transmisión 57](#_Toc476297168)

[Tabla 11. Comunicaciones Tierra / Aire – Recepción 65](#_Toc476297169)

[Tabla 12. Comunicaciones Tierra / Aire – Retransmisión 73](#_Toc476297170)

[Tabla 13. Comunicaciones Tierra / Aire – Redundancia Servicio 81](#_Toc476297171)

[Tabla 14. Comunicaciones Tierra / Tierra – Acceso Directo / Acceso Indirecto 89](#_Toc476297172)

[Tabla 15. Comunicaciones Tierra / Tierra – Acceso Instantáneo 97](#_Toc476297173)

[Tabla 16. Comunicaciones Tierra / Tierra – Servicios Suplementarios 105](#_Toc476297174)

[Tabla 17. Herramientas Desarrollo Software 107](#_Toc476297175)

[Tabla 18. Plan de Gestión de la Seguridad 113](#_Toc476297176)

[Tabla 19. Evidencias para el cumplimiento de SWAL 148](#_Toc476297177)

# OBJETO

Este documento describe los procesos previstos para garantizar el Nivel de Aseguramiento Software (SWAL) para los módulos software del producto ULISES V5000I de DF NÚCLEO.

## ALCANCE

El alcance del documento incluye todos los aspectos procedimentales, técnicos y de calidad que en el contexto del producto ULISES V5000I son necesarios para garantizar el cumplimiento SWAL.

## ESTRUCTURA

El cuerpo central del documento contiene los siguientes apartados:

* Descripción del Sistema. En concreto una descripción de la arquitectura hardware, una descripción de la arquitectura software y la relación entre los módulos hardware y software.
* Proceso de Evaluación de la Seguridad. Breve descripción de esta metodología y su relación con el ciclo de vida de un sistema.
* Análisis Funcional de Amenazas (FHA). El objeto de este análisis es la identificación del SWAL.
* Carpeta de Seguridad del Software (SSF). Este apartado sigue la estructura propuesta en la ED-153. Contiene una lista de evidencias o referencias a las mismas.
* Trazabilidad de requisitos. Este apartado es un resumen del presente documento.

## DOCUMENTOS DE REFERENCIA

* ED-153 “Guidelines for ANS Software Assurance” Agosto 2009.
* Material guia para la garantia del software. AENA. A111b-09-GUI-01-3.2. Noviembre 2013.
* Investigación de accidentes e incidentes de aviación. Anexo 13 al Convenio sobre Aviación Civil Internacional. Julio 2001.
* ESARR 6. Software in ATM Functional Systems, ed.2.0. Mayo 2010.
* ESARR 4. Risk Assessment and mitigation in ATM, ed.1.0. Abril 2001.
* Air Navigation System SAFETY ASSESSMENT METHODOLOGY. SAF.ET1.ST03.1000-MAN-01-00. Edición 2.1. Octubre 2006.
* SAM PART I. Functional Hazard Assessment. SAF.ET1.ST03.1000-MAN-01-01-00. Edición 2.1. Octubre 2006.
* SAM PART II. Preliminary System Safety Assessment. SAF.ET1.ST03.1000-MAN-01-02-00. Edición 2.1. Octubre 2006.
* SAM PART III. System Safety Assessment. SAF.ET1.ST03.1000-MAN-01-03-00. Edición 2.1. Octubre 2006.
* SAM PART IV. Annexes. SAF.ET1.ST03.1000-MAN-01-04. Edición 2.1. Octubre 2006.
* “ANS Software Lifecycle” SAF.ET1.ST03.1000-REP-01-00. Edición 3.0. Diciembre 2005
* “Recommendations for A.N.S. software” SAF.ET1.ST03.1000.GUI-01-00. Edición 1.0. Diciembre 2005.
* ED-136 “VoIP ATM System Operational and Technical Requirements”.
* ED-137 “INTEROPERABILITY STANDARDS FOR VOIP ATM COMPONENTS. VOLUME 1: RADIO.
* ED-137 “INTEROPERABILITY STANDARDS FOR VOIP ATM COMPONENTS. VOLUME 2: TELEPHONE.
* ED-137 “INTEROPERABILITY STANDARDS FOR VOIP ATM COMPONENTS. VOLUME 3: EUROPEAN LEGACY TELEPHONE INTERWORKING.
* ED-137 “INTEROPERABILITY STANDARDS FOR VOIP ATM COMPONENTS. VOLUME 4: RECORDING.
* ED-137 “INTEROPERABILITY STANDARDS FOR VOIP ATM COMPONENTS. VOLUME 5: SUPERVISION.
* ED-138 “Network Requirements and Performances for VoIP ATM Systems”. Part 1: Network Specification.
* ED-138 “Network Requirements and Performances for VoIP ATM Systems”. Part 2: Network Design Guideline.
* ED-139 “Qualification tests for VoIP ATM Components and Systems”.
* P07005 Control del Diseño y Desarrollo.
* P07005AC\_GUIA ELABORACION ERS CON UML-EA.
* P07005AD. RedMine. Guia de Utilizacion.
* P07008 Investigación, innovación y Vigilancia Tecnológica.
* P07023 Industrialización.
* P04001 Gestion de la Documentacion y de los Registros.
* P07007 Procedimiento General de Compras.
* P06001 Formacion y Toma de Conciencia.
* P08002 Auditorías internas de Calidad y Medio Ambiente.

## ABREVIATURAS

En este documento se utilizan las siguientes abreviaturas:

* **AD –** Acceso Directo.
* **ANS –** Air Navigation Systems.
* **ATM –** Air Traffic Management.
* **ATS –** Air Traffic System.
* **BC –** Batería Central.
* **BL –** Batería Local.
* **BSS –** Best Signal Selection.
* **CPU -** Central Processing Unit.
* **COTS -** Commercial Off-The-Shelf.
* **FHA -** Functional Hazard Assessment.
* **FXO –** Foreign Exchange Office.
* **FXS –** Foreign Exchange Subscriber.
* **HTTP –** Hypertext Transfer Protocol.
* **HW –** Hardware.
* **IP –** Internet Protocol.
* **LAN –** Local Area Network.
* **L/C - -**Línea Caliente.
* **LCEN –** Línea Caliente Exterior Normalizada.
* **NBX –** Node Box.
* **NTP –** Network Time Protocol.
* **PABX –** Private Automatic Branch Exchange.
* **PSSA -** Preliminary System Safety Assesment.
* **PTT –** Push To Talk.
* **QoS –** Quality of Service.
* **RTP –** Real-time Transport Protocol.
* **RX –** Reception.
* **SACTA -** Sistema de Automatización para Control del Tráfico Aéreo.
* **SAM -** Safety Assessment Methodology.
* **SCV –** Sistema de Comunicaciones Vocales.
* **SDP –** Session Description Protocol.
* **SIP –** Session Initiation Protocol.
* **SNMP –** Simple Network Management Protocol.
* **SOAP –** Simple Object Access Protocol.
* **SSA -** System Safety Assesment.
* **SSAS -** Software Safety Assurance System.
* **SSF -** Software Safety Folder.
* **SW –** Software.
* **SWAL -** Software Assurance Level.
* **T / A –** Tierra / Aire.
* **T / T –** Tierra / Tierra.
* **TX –** Transmission.
* **VoIP –** Voice over Internet Protocol.
* **WAN –** Wide Area Network.
* **WG –** Working Group.

# DESCRIPCIÓN DEL SISTEMA

ULISES V5000I es un sistema de control y gestión de comunicaciones de voz y datos, construido sobre tecnología IP, que permite y facilita comunicaciones orales entre aeronaves y Centros y/o Torres de Control. De igual forma suministra otros servicios adicionales que garantizan la seguridad del Control de Tránsito Aéreo.

Este sistema de comunicaciones de voz, consta de un conjunto de componentes que pueden agruparse en los siguientes subsistemas:

* Subsistema de Comunicaciones Radio Tierra / Aire.
* Subsistema de Comunicaciones Telefónicas Tierra / Tierra.
* Subsistema de Configuración, Supervisión y Mantenimiento.

Este producto constituye un sistema nativo IP ya que se diseñó desde el inicio en el marco del WG-67 al que contribuye DF NÚCLEO. Es por tanto un producto que cumple las normativas ED-136, ED-137, ED-138 y ED-139 de EUROCAE con capacidad de gestionar todas las posiciones de control operativas y todos los recursos de comunicaciones asignados.

ULISES V5000I ofrece ventajas relevantes como las siguientes:

* Solución completa SCV extremo-extremo IP.
* Solución de todos los recursos ATM redundante en pasarela y en red IP.
* Arquitectura distribuida de todo el sistema.
* Interoperabilidad con otros SCVs ya que ha sido diseñado de acuerdo a estándares de EUROCAE.
* Tiene en cuenta parámetros de calidad de servicio QoS.
* Permite desplazar las pasarelas hasta las proximidades de los recursos.
* El número de recursos únicamente viene dado por el ancho de banda disponible.
* Posibilidad de comunicaciones encriptadas y securizadas.
* Facilidad de configuración y reconfiguración del sistema.
* La Configuración y Supervisión, basada en una arquitectura de servicios WEB que se puede realizar desde un navegador comercial.

En cuanto a sistema de control de comunicaciones, el sistema ULISES V5000I, posibilita el acceso de operadores a distintos medios de transmisión, que de forma resumida, describimos a continuación:

Comunicaciones Tierra / Aire:

* Implementando la interfaz de audio y control que permite la utilización de las funciones de transmisión y recepción, a distintos equipos radio para diferentes bandas de frecuencia. Incluye equipos radio LEGACY (a través de pasarelas) y equipos radio VoIP (ED137B-1).
* Gestión de frecuencias desplazadas (BSS, CLIMAX).
* Maneja diferentes modos de redundancia de equipos radio:
  + MAIN / STANDBY con gestión externa.
  + MAIN / SATNDBY con gestión interna (solo en equipos radio IP).
  + Configuración M+N. Para equipamientos radio IP, según ED137B (1,5).

Comunicaciones Tierra / Tierra:

* Con llamada previa (Telefonía), habilitando el acceso a líneas y elementos de los siguientes tipos:
  + Líneas analógicas a 2 hilos dedicadas. Interfaces BL y BC.
  + Líneas analógicas a 2 Hilos FXS/FXO.
  + Líneas analógicas a 4 Hilos con señalización ATS-R2.
  + Líneas analógicas a 4 Hilos con señalización ATS-N5.
  + Líneas digitales EUROISDN de Acceso Básico Lado Abonado.
  + Teléfonos IP.
  + Abonados de Centralitas IP.
* Sin llamada previa. Línea Caliente (L/C):
  + Líneas analógicas a 4 hilos con señalización en banda compatible con AENA-LCEN.
  + Conexiones de acceso instantáneo VoIP según ED137B-3.

Comunicaciones Internas:

* Enlaces entre puestos con o sin llamada previa.

Interfaces a sistemas externos.

* Interfaz a SACTA (Sistema de Automatización para Control del Tráfico Aéreo).
* Interfaz a sistemas de sincronización externos.
* Posibilidad de Conexión a Sistemas Similares.
* Conexión a SCV’s compatibles ED-137/2B a través de redes ATM-VoIP.
* Conexión a Nodos Remotos de emplazamientos radio, compatibles ED-137/1B a través de redes ATM-VoIP.
* Conexión a subsistemas de Grabación de Comunicaciones de voz a través de redes ATM-VoIP según ED-137/4B.
* Conexiones de Datos a Estaciones de Supervisión Externas compatibles con ED-137/5B a través de redes ATM-VoIP.

Desde el aspecto tecnológico y de diseño el SCV ULISES V5000I, presenta grandes ventajas ya que es un sistema basado en tecnología IP, por tanto incorpora las ventajas de este tipo de entorno como es la arquitectura distribuida, redundante y fácilmente ampliable. En su diseño, se han incorporado otras características que aseguran la posibilidad de modificar una configuración sin impacto en el servicio operacional. En la medida de lo posible, utiliza componentes estándar y comerciales (Commercial Off The Shelf – COTS).

## Arquitectura HW

La arquitectura HW de ULISES V5000I se representa en la siguiente figura:



1. Arquitectura Hardware. Diagrama General de Bloques

Los elementos que forman este diagrama, son los siguientes:

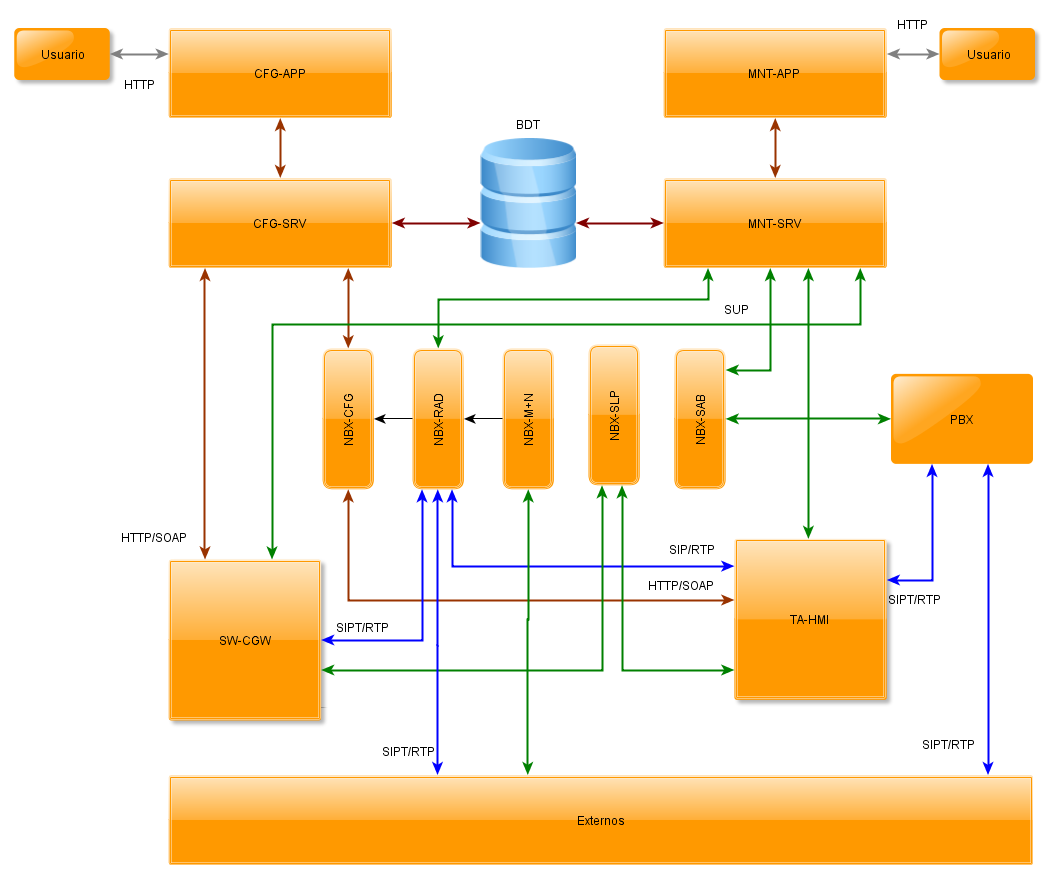
* Subsistema de Operador. Se refiere a los elementos que proporcionan el acceso a los recursos a los operadores del sistema. Como veremos posteriormente, están basados en hardware COTS.
* Subsistema de Gestión. Se refiere a los elementos en los que se reside la configuración y supervisión del sistema.
* Pasarelas a Recursos de Comunicaciones. Están formados por los elementos necesarios para ofrecer el acceso VoIP a los recursos de comunicaciones LEGACY (radio, líneas telefónicas, etc.) del ámbito local de la instalación.
* Elementos de Red Local y Firewall. Infraestructura de la red local (switches, routers, etc.). Los elementos Firewall, gestionan el control de acceso a esta red local de los elementos externos a la instalación.
* Sistemas Externos. Se refiere a aquellos sistemas, que aunque no son componentes del sistema SCV sí que son de ámbito local a la instalación, como puede ser el acceso al sistema SACTA, elementos de sincronismo en red, centralitas o teléfonos IP, etc.
* Pasarelas a Recurso de Comunicaciones Externos vía WAN. Se refiere a aquellos elementos que no son de ámbito local a la instalación y cuya conectividad se consigue mediante redes externas públicas o privadas. Esto incluye el acceso a emplazamientos remotos de equipos de radio, otros SCV IP, etc.

El sistema incorpora servicios de dualidad en varios de sus elementos:

* Dualidad en Servidores de Gestión.
* Dualidad en CPU en Pasarelas a Recursos de Comunicaciones.

## Arquitectura SW

La arquitectura SW de ULISES V5000I se representa en la siguiente figura:



1. Arquitectura Software. Diagrama General

Los elementos que componen este diagrama, son los siguientes:

* CFG-APP. Aplicación de configuración. Implementa los métodos y herramientas que posibilitan la configuración del sistema a los usuarios.
* CFG-SRV. Servicios de configuración. Implementan los procesos de intercambio y actualización de información de configuración entre los diferentes módulos y la Base de Datos.
* MANT-APP. Aplicación de Mantenimiento. Implementan los métodos y herramientas que se ofrecen al usuario de supervisión y mantenimiento y a la explotación del histórico asociado.
* MANT-SRV. Servicios de configuración. Implementan los procesos de intercambio y actualización de información de mantenimiento entre los diferentes módulos y la Base de Datos.
* BDT. Base de datos del sistema. Ofrece el soporte de almacenamiento y gestión de los datos de configuración y del histórico del sistema.
* NBX-CFG. Servicio centralizado de configuración. Ofrece la interfaz a la configuración del sistema y los procedimientos de distribución de la misma al resto de servicios centralizados y a las aplicaciones de operador.
* NBX-RAD. Servicio centralizado de radio. Mantiene las sesiones radio en las frecuencias de trabajo, tanto a equipos internos (pasarelas) como externos así como ofrece el servicio de operativa radio a las aplicaciones de operador.
* NBX-M+N. Servicio centralizado de gestión de equipos radio en configuración M+N. Supervisa la disponibilidad de los equipos radio manejados y gestiona las asignaciones de dichos equipos a las frecuencias controladas por el servicio centralizado de radio.
* NBX-SLP. Servicio centralizado de supervisión de líneas telefónicas internas PP. Se encarga de obtener la información operativa de las líneas telefónicas internas y distribuirlas a las aplicaciones de operador.
* NBX-SAB. Servicio centralizado de supervisión de abonados PBX. Se encarga de obtener la información operativa de los aboanados internos de PABX y distribuirla a las aplicaciones de operador.
* PABX. Proxy SIP. Gestiona la localización y gestión de sesiones de usuarios SIP del sistema, tanto internos como externos.
* SW-CGW. Paquete software de las Pasarelas. Integra el control de los diferentes protocolos de acceso de los recursos externos (Control Radio, ATS-R2, ATS-N5, LCEN, etc.) y la gestión de recursos de comunicaciones en la red.
* TA/HMI. Software de Operador. Integra el HMI de operación y el gestor de recursos audio.

La intercomunicación entre cada uno de estos módulos se establece mediante protocolos estándar, todos ellos encuadrados en la familia de protocolos IP:

* SIP/SDP. Utilizado para los procedimientos de señalización de las comunicaciones en concordancia con lo establecido por EUROCAE ED-137A/B.
* RTP. Utilizado para el intercambio de flujos de audio en concordancia con lo establecido por EUROCAE ED-137A/B.
* NTP. Utilizado para el intercambio de información de sincronismo interno y externo.
* SNMP. Utilizado para el intercambio de información de Supervisión y mantenimiento en concordancia con lo establecido en EUROCAE ED-137A/B.
* HTTP/SOAP. Utilizado para los procedimientos de implantación de configuraciones y para el acceso de las consolas de gestión de la configuración y mantenimiento a los servicios ofrecidos por el sistema.

La siguiente tabla muestra la relación entre los paquetes o módulos software y el hardware donde se ejecutan:

|  |  |  |  |
| --- | --- | --- | --- |
| Módulo HW  Módulo  Software | Subsistema de  Operador | Subsistema de  Gestión | Pasarelas (Gateways) |
| **CFG-APP** |  | X |  |
| **CFG-SRV** |  | X |  |
| **MANT-APP** |  | X |  |
| **MANT-SRV** |  | X |  |
| **BDT** |  | X |  |
| **NBX-CFG** | X |  |  |
| **NBX-RAD** | X |  |  |
| **NBX-M+N** | X |  |  |
| **NBX-SLP** | X |  |  |
| **NBX-SAB** | X |  |  |
| **PABX** |  | X |  |
| **SW-CGW** |  |  | X |
| **TA-HMI** | X |  |  |

1. Relación Módulos Hardware y Módulos Software

# PROCESO DE EVALUACIÓN DE LA SEGURIDAD

El proceso de evaluación de la seguridad (SAM) es una metodología que describe una secuencia de operaciones para evaluar la seguridad de los sistemas de navegación aérea (ANS).

Este proceso consiste en 3 pasos sucesivos:

* Análisis Funcional de amenazas (FHA).

¿Cuánta seguridad necesita el Sistema?

* Evaluación Preliminar de la Seguridad del Sistema (PSSA).

¿Cuánta seguridad tiene la arquitectura propuesta?

* Evaluación de la Seguridad del Sistema (SSA).

¿Cuánta seguridad tiene el Sistema implementado?

***Análisis Funcional de amenazas (FHA)***

El objeto de este análisis es la identificación del SWAL. La secuencia de tareas a realizar son las siguientes:

* Identificación de las funciones del sistema.
* Identificación de las amenazas potenciales.
* Identificación de los Efectos o Consecuencias de las Amenazas.
* Probabilidad.
* Severidad.
* Descripción de las medidas de mitigación.
* Identificación del SWAL

***Evaluación Preliminar de la Seguridad del Sistema (PSSA)***

Conociendo el diseño del sistema (su arquitectura hardware y software), en esta fase se analiza si dicho diseño tiene la seguridad requerida al sistema.

***Evaluación de la Seguridad del Sistema (SSA)***

Conociendo la implementación del sistema, el objetivo de esta fase es demostrar que el sistema implementado cumple con la seguridad requerida.

En la siguiente figura se muestra la relación entre el proceso de evaluación de la seguridad y el ciclo de vida del sistema.

DEFINICIÓN

DISEÑO

CICLO DE VIDA

DEL SISTEMA

PROCESO DE EVALUACIÓN

DE LA SEGURIDAD

IMPLEMENTACIÓN

MANTENIMIENTO

RETIRADA

FHA

PSSA

SSA

1. Proceso de Evaluación de la Seguridad

En la tabla siguiente se presenta la estructura típica de carpetas (o directorios) que se utilizan para un desarrollo. Para cada carpeta hay una indicación de su contenido.

|  |  |
| --- | --- |
| CARPETA | CONTENIDO |
| Especificación | Especificación de Requisitos Software |
| Lista de Casos de Prueba |
| Planificación | Plan de Calidad |
| Plan de Diseño y Desarrollo |
| Diseño | Diseño Básico |
| Diseño de Detalle |
| Resultados | Control de Configuración |
| Informes de Pruebas de Verificación |
| Informes de Pruebas de Validación |
| En paralelo a estas carpetas con documentación sobre el plan de calidad, se mantiene un repositorio donde se almacena:   * Doc: documentación del producto. * Bin: ejecutables del software. * Src: fuentes del software. |
| Registros | Revisión de Datos de Partida |
| Revisión de Diseño |
| Actas de Verificación |
| Actas de Validación |
| Seguimiento | Informe de Seguimiento |

1. Estructura de carpetas para un desarrollo software

En aquellos desarrollos en los que es requisito la garantía de la seguridad del software, se elaboran, además, los siguientes documentos:

***Evaluación Preliminar de la Seguridad del Sistema (PSSA)***

Este documento se elabora en la fase de diseño. Incluye:

* Descripción de la Arquitectura del Sistema. En concreto una descripción de la arquitectura hardware, una descripción de la arquitectura software y la relación entre los módulos hardware y software.
* Análisis Funcional de Amenazas (FHA). El objeto de este análisis es la identificación del SWAL.
* Carpeta de Seguridad del Software (SSF). Este apartado sigue la estructura propuesta en la ED-153. Contiene una lista de evidencias o referencias a las mismas.

Teniendo en cuenta que este documento se elabora en la actividad de diseño se entiende que algunos de los capítulos de la SSF todavía no presenten la evidencia correspondiente.

***Evaluación de la Seguridad del Sistema (SSA)***

Teniendo en cuenta que este documento se prepara con el sistema ya desarrollado, se entiende que la carpeta SSF ya puede hacer referencia a las evidencias correspondientes.

En concreto, incluye:

* Descripción de la Arquitectura del Sistema. En concreto una descripción de la arquitectura hardware, una descripción de la arquitectura software y la relación entre los módulos hardware y software.
* Análisis Funcional de Amenazas (FHA). El objeto de este análisis es la identificación del SWAL.
* Carpeta de Seguridad del Software (SSF). Este apartado sigue la estructura propuesta en la ED-153. Contiene una lista de evidencias o referencias a las mismas.

En la tabla siguiente se presenta la estructura típica de carpetas (o directorios) que se utilizan para un desarrollo con garantía de seguridad software. Para cada carpeta hay una indicación de su contenido.

|  |  |
| --- | --- |
| CARPETA | CONTENIDO |
| Especificación | Especificación de Requisitos Software |
| Lista de Casos de Prueba |
| Planificación | Plan de Calidad |
| Plan de Diseño y Desarrollo |
| Diseño | Diseño Básico |
| Diseño de Detalle |
| ***Evaluación Preliminar de la Seguridad del Sistema (PSSA)*** |
| Resultados | Control de Configuración |
| Informes de Pruebas de Verificación |
| Informes de Pruebas de Validación |
| ***Evaluación de la Seguridad del Sistema (SSA)*** |
| En paralelo a estas carpetas con documentación sobre el plan de calidad, se mantiene un repositorio donde se almacena:   * Doc: documentación del producto. * Bin: ejecutables del software. * Src: fuentes del software. |
| Registros | Revisión de Datos de Partida |
| Revisión de Diseño |
| Actas de Verificación |
| Actas de Validación |
| Seguimiento | Informe de Seguimiento |

1. Estructura de carpetas para un desarrollo software con garantía de seguridad

En el apartado 5 (Carpeta de Seguridad Software, SSF) se sigue la estructura de la norma ED-153 para facilitar el seguimiento de las evidencias.

# ANALISIS FUNCIONAL DE AMENAZAS (FHA)

## INTRODUCCIÓN

El objeto de este análisis es la identificación del SWAL.

Las tareas a realizar serán las siguientes:

* Identificación de las funciones del sistema
* Identificación de las amenazas potenciales
* Identificación de los Efectos o Consecuencias de las Amenazas
* Probabilidad
* Severidad.
* Establecer las medidas de mitigación.
* Identificación del SWAL

## IDENTIFICACIÓN DE LAS FUNCIONES

ULISES V5000I es un sistema de control y gestión de comunicaciones de voz y datos, construido sobre tecnología IP, que permite y facilita comunicaciones orales entre aeronaves y Centros y/o Torres de Control. De igual forma suministra otros servicios adicionales que garantizan la seguridad del Control de Tránsito Aéreo.

Este sistema de comunicaciones de voz, consta de un conjunto de funciones sobre las que se va a realizar este análisis funcional de amenazas:

* Comunicaciones Tierra / Aire
  + Transmisión.
  + Recepción
  + Retransmisión
  + Redundancia Servicio (M+N)
* Comunicaciones Tierra / Tierra
  + Acceso directo / acceso indirecto
  + Acceso instantáneo
  + Servicios Suplementarios

Una breve descripción de estas funciones:

* Comunicaciones Tierra / Aire -Transmisión.

Esta facilidad, permite que el audio del operador sea enviado por la frecuencia radio a los elementos a la escucha. Los detalles de esta operación son los siguientes:

* Se activa el mando PTT.
* Se inhiben los circuitos de recepción en el operador correspondientes a todas las frecuencias asignadas en Transmisión / Recepción.
* Se direcciona la señal del micrófono a las interfaces de las frecuencias seleccionadas en Transmisión / Recepción.
* La situación continúa hasta que el mando de PTT se desactiva.
* Comunicaciones Tierra / Aire - Recepción.

Esta facilidad habilita la escucha en el puesto de las transmisiones de audio efectuadas en las frecuencias asignadas por las aeronaves u otros operadores. Las señales recibidas de cada una de las frecuencias asignadas en Recepción, se mezclan y ofrecen al operador bien en altavoz, bien en casco bien en una mezcla de ambas (un grupo en altavoz, un grupo en cascos).

Al pulsar PTT y transmitir por uno o más canales, se inhibirá la recepción por esos canales en la posición que active el PTT y sólo en ésta.

* Comunicaciones Tierra / Aire - Retransmisión.

Esta función permite establecer grupos de frecuencias (Grupos de Retransmisión) donde se ejecutan procedimientos de retransmisión:

La señal recibida por el sistema en una frecuencia, es transmitida por las demás frecuencias que componen el grupo.

* Una frecuencia concreta, sólo puede estar en un grupo de retransmisión.
* Esta señal recibida es presentada en recepción a los operadores.
* La transmisión de operador en el grupo se efectúa a todas las frecuencias que lo componen.

Esta función se accede desde las posiciones radio. Desde estas, el usuario puede:

* Establecer hasta 4 grupos de retransmisión de hasta 20 frecuencias cada uno.
* Deshacer grupos de retransmisión establecidos.
* Comunicaciones Tierra / Aire – Redundancia Servicio.

El sistema incorpora un gestor para la configuración M+N de equipos radio, tanto en transmisión como en recepción de forma que:

* Si existen N frecuencias de trabajo, existen N equipos en transmisión / recepción asignados a dichas frecuencias de trabajo como equipos ‘Principales’ que SOLO podrán operar en su Frecuencia.
* Existen M equipos de Transmisión/Recepción (normalmente M<N), en reserva. Estos equipos pueden sustituir a cualquier equipo configurado como principal, ante el fallo del mismo.
* La conmutación se realiza de forma ‘automática’ y de modo ‘transparente’ al operador final.
* Siempre que, para una determinada frecuencia de trabajo, el equipo (TX o RX) designado como principal para la frecuencia se encuentre disponible el sistema se asegura que será el utilizado para esa frecuencia de trabajo.
* Para el caso de Fallo de equipo estando todos los equipos de reserva ocupados, el sistema implementa un esquema de priorización que determina que frecuencia de trabajo se queda sin recurso (hasta que se solucionen los fallos presentes).
* La gestión de este módulo está integrada en el sistema de gestión del propio SCV.
* La supervisión de los equipos radio está integrada el sistema de Supervisión e Históricos del SCV.

Este módulo es aplicable a equipos radio que:

* Presentan una interfaz de operación según ED137B-1
* Exponen su estado operativo (NORMAL – FALLO), preferiblemente a través de SNMP compatible con ED137B-5.
* Pueden ser SINTONIZADOS, desde una aplicación externa (en este caso ULISES V 5000).
* Los equipos pueden ser Transmisores o Receptores.
* Comunicaciones Tierra / Tierra - Acceso directo / acceso indirecto

El servicio de Acceso Directo (AD) permitirá el inicio, aceptación y fin de llamada mediante una única operación, presionando un pulsador con enclavamiento del panel de acceso telefónico. La comunicación se establecerá entre dos posiciones previamente asignadas y convenientemente etiquetadas, por lo que tanto el llamante como el llamado estarán claramente identificados.

El servicio de Acceso Indirecto, es aquel que permite establecer la comunicación entre dos usuarios cualesquiera, utilizando para ello un dial numérico o alfa-numérico y finalizan la llamada presionando un pulsador destinado al efecto.

El sistema proporciona una facilidad, aplicable a la gestión del servicio de acceso indirecto, por medio de la cual, redirecciona los datos y la gestión de la llamada a una posición de acceso directo especial. Tanto la señalización como la operación de esta tecla es análoga a cualquier otra posición AD. Esta facilidad se utiliza tanto para llamadas salientes como para llamadas entrantes.

Relacionado con el servicio de acceso indirecto, el sistema implementa una cola de entre 3 y 20 llamadas que permite almacenar llamadas entrantes no atendidas, llamadas retenidas, etc., identificadas de modo que el usuario reconoce fácilmente su origen y estado. Las llamadas en cola se pueden atender tanto automáticamente, con el método FIRST-IN-FIRST-OUT, como de manera manual seleccionando la siguiente llamada que se desea atender.

* Comunicaciones Tierra / Tierra - Acceso instantáneo

El servicio de Acceso instantáneo o de Línea Caliente (L/C) es un circuito telefónico directo punto a punto, sin aceptación por parte del llamado entre dos únicas posiciones predeterminadas, donde las acciones de selección de línea y de establecer comunicación se realizan simultáneamente al presionar el llamante un pulsador de L/C, permitiendo la transmisión de audio al llamado sin necesidad de acción alguna por la parte receptora. Los pulsadores son inestables (sin enclavamiento).

* Comunicaciones Tierra / Tierra – Servicios suplementarios

El Subsistema telefónico implementa una serie de funciones telefónicas suplementarias que permiten a los usuarios realizar, recibir y gestionar llamadas telefónicas de diferentes formas. Estas funciones son las siguientes:

* Regulación del volumen de audio en cascos homogéneo para todas las líneas asignadas
* Control Zumbador de Llamadas Entrantes. Permite activar o desactivar la señalización acústica de la presencia de Llamadas Entrantes no atendidas.
* Paginación de controles AD. Las diferentes posiciones AD se organizan en páginas que el operador puede secuenciar para acceder a la posición deseada. Se señaliza la actividad en páginas ocultas.
* Teclado Alfanumérico. Para poder habilitar el servicio de llamada saliente por acceso indirecto el sistema dispone de una página desde donde se accede a un teclado telefónico avanzado. Permite la introducción de destino dígito a dígito, desde agenda de últimos números marcados o números memorizados.
* Retención (Puesta en espera). Esta función permite al usuario desconectar temporalmente una comunicación establecida, con el fin de llevar a cabo alguna otra operación telefónica y posteriormente volver a la llamada original. Mediante dicha función la llamada en curso será almacenada en una cola de llamadas para su posterior recuperación, identificada de manera que el usuario reconozca que se trata de una llamada puesta en espera.
* Transferencia. El sistema tiene capacidad para que un operador que tenga asignada una línea telefónica pueda transferir la llamada de esa línea a otro operador que no la tuviese asignada.
* Rellamada Automática (para Accesos Directos). Esta función permite al usuario habilitar al sistema para que automáticamente realice repeticiones de llamada a otro usuario configurado como Acceso Directo. El usuario podrá configurar el tiempo entre llamadas. El sistema avisa al usuario mediante indicación luminosa que esta opción se encuentra seleccionada.
* Escucha. Esta función permite a un usuario, siempre y cuando cuente con la necesaria autorización, escuchar las comunicaciones de otro u otros usuarios conectados al SCV.
* Prioridad. Esta función sólo está disponible en aquellos sistemas que soporten señalización con este servicio. Actualmente las señalizaciones que pueden prestar este servicio son R2 y N5. Esta función permite a un usuario obtener conexión incluso si todos los circuitos disponibles de una troncal están ocupados. El usuario puede asignar un nivel de prioridad a la llamada antes de realizarla, o una vez realizada tras recibir el tono de congestión. Aquel circuito cuya llamada tenga la prioridad más baja será designado para ser liberado y un tono de aviso será emitido sobre la comunicación en curso para avisar a los usuarios de este circuito que la comunicación va a ser interrumpida. Después de un intervalo de tiempo predeterminado dicho circuito será liberado y la llamada con prioridad será establecida. El nivel de prioridad asignado a cada usurario es configurable a nivel de supervisión.
* Intrusión. Esta función sólo estará disponible en aquellos sistemas que soporten señalización con este servicio. Actualmente las señalizaciones que pueden prestar este servicio son R2 y N5. Esta función permite a un usuario llamante establecer comunicación con otro usuario ocupado irrumpiendo en una comunicación establecida entre el usuario llamado y un tercer usuario (no llamado). Si la intrusión se ha realizado con éxito, se establecerá una conferencia entre los tres usuarios. Cualquiera de los usuarios podrá salir de la conferencia simplemente colgando.

La siguiente tabla muestra la relación entre las funciones y los módulos software donde se ejecutan:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Módulo SW  Función | CFG  APP | CFG  SRV | MANT  APP | MANT  SRV | BDT | NBX  CFG | NBX  RAD | NBX  M+N | NBX  SLP | NBX  SAB | PABX | SW  CGW | TA  HMI |
| **Comunicaciones Tierra / Aire**  **Transmisión** | X | X | X | X | X | X | X | X |  |  |  | X | X |
| **Comunicaciones Tierra / Aire**  **Recepción** | X | X | X | X | X | X | X | X |  |  |  | X | X |
| **Comunicaciones Tierra / Aire**  **Retransmisión** | X | X | X | X | X | X | X | X |  |  |  | X | X |
| **Comunicaciones Tierra / Aire**  **Redundancia Servicio** | X | X | X | X | X | X | X | X |  |  |  | X | X |
| **Comunicaciones Tierra / Tierra**  **Acceso directo / acceso indirecto** | X | X | X | X | X | X |  |  | X | X | X | X | X |
| **Comunicaciones Tierra / Tierra**  **Acceso Instantáneo** | X | X | X | X | X | X |  |  | X | X | X | X | X |
| **Comunicaciones Tierra / Tierra**  **Servicios Suplementarios** | X | X | X | X | X | X |  |  | X | X | X | X | X |

1. Relación entre Funciones y Módulos Software

## IDENTIFICACION DE LAS AMENAZAS

Para que el ULISES V5000I cumpla las funciones comentadas en el apartado anterior, se han identificado las siguientes amenazas:

* *Especificación defectuosa*.
* *Diseño defectuoso*.
* *Validación defectuosa*.
* *Fallo HW en Operador* (módulo HW: Subsistema de Operador).
* *Fallo HW en Operador Gestor* (módulo HW: Subsistema de Operador. Activos los servicios de gestión).
* *Fallo HW en Pasarela* (módulo HW: Pasarela a Recursos de Comunicaciones).
* *Fallo HW en Gestión* (módulo HW: Subsistema de Gestión).
* *Fallo HW en LAN*.
* *Fallo SW en Operador* (módulo HW: Subsistema de Operador).
* *Fallo SW en Operador Gestor* (módulo HW: Subsistema de Operador. Activos los servicios de gestión).
* *Fallo SW en Pasarela* (módulo HW: Pasarela a Recursos de Comunicaciones).
* *Fallo SW en Gestión* (módulo HW: Subsistema de Gestión).

## IDENTIFICACION DE LOS EFECTOS

En este apartado se listan todos los efectos que pueden implicar las amenazas comentadas en el apartado anterior:

* *Funcionalidad no adecuada.*
* *Pérdida de comunicaciones t/a.*
* *Degradación de comunicaciones t/a.*
* *Pérdida de comunicaciones t/t.*
* *Degradación de comunicaciones t/t.*
* *Pérdida de servicios de re-configuración.*
* *Degradación de servicios de re-configuración.*
* *Pérdida de la supervisión del sistema.*
* *Degradación de la supervisión del sistema.*

Cada una de las amenazas identificadas con anterioridad puede implicar alguno de los efectos anteriores. La relación exhaustiva de amenazas y efectos se indica en la siguiente tabla:

|  |  |
| --- | --- |
| AMENAZA | EFECTO |
| *Especificación defectuosa* | *Funcionalidad no adecuada* |
| *Diseño defectuoso* | *Degradación de comunicaciones t/a* |
| *Degradación de comunicaciones t/t* |
| *Degradación de servicios de re-configuración* |
| *Degradación de la supervisión del sistema* |
| *Validación defectuosa* | *Degradación de comunicaciones t/a* |
| *Degradación de comunicaciones t/t* |
| *Degradación de servicios de re-configuración* |
| *Degradación de la supervisión del sistema* |
| *Fallo HW en Operador* | *Degradación de comunicaciones t/a* |
| *Degradación de comunicaciones t/t* |
| *Fallo HW en Operador Gestor* | *Pérdida de comunicaciones t/a* |
| *Degradación de comunicaciones t/a* |
| *Pérdida de comunicaciones t/t* |
| *Degradación de comunicaciones t/t* |
| *Fallo HW en Pasarela* | *Degradación de comunicaciones t/a* |
| *Degradación de comunicaciones t/t* |
| *Fallo HW en Gestión* | *Degradación de comunicaciones t/t* |
| *Pérdida de servicios de re-configuración* |
| *Degradación de servicios de re-configuración* |
| *Pérdida de la supervisión del sistema* |
| *Degradación de la supervisión del sistema* |
| *Fallo HW en LAN* | *Pérdida de comunicaciones t/a* |
| *Pérdida de comunicaciones t/t* |
| *Pérdida de servicios de re-configuración* |
| *Pérdida de la supervisión del sistema* |
| *Fallo SW en Operador* | *Degradación de comunicaciones t/a* |
| *Degradación de comunicaciones t/t* |
| *Fallo SW en Operador Gestor* | *Pérdida de comunicaciones t/a* |
| *Degradación de comunicaciones t/a* |
| *Degradación de comunicaciones t/t* |
| *Fallo SW en Pasarela* | *Degradación de comunicaciones t/a* |
| *Degradación de comunicaciones t/t* |
| *Fallo SW en Gestión* | *Degradación de comunicaciones t/t* |
| *Pérdida de servicios de re-configuración* |
| *Degradación de servicios de re-configuración* |
| *Pérdida de la supervisión del sistema* |
| *Degradación de la supervisión del sistema* |

1. Amenazas y Efectos.

En esta tabla falta filtrar por función. En las tablas resultantes del análisis se indicará, para cada función los efectos que le aplican.

## IDENTIFICACIÓN DE ACCIONES DE MITIGACIÓN

Tras producirse el evento, se aplicarán las medidas de mitigación, lo que dará lugar a que las consecuencias del evento (es decir, sus efectos) se puedan REDUCIR, CONTROLAR o ELIMINAR.

* *Revisiones de requisitos.*
* *Revisiones de diseño.*
* *Pruebas de validación.*
* *Traslado de funciones entre terminales.*
* *Redundancia y conmutación automática del servicio NBX.*
* *Redundancia en CPU y en la tarjeta de interface en las pasarelas.*
* *Dualidad en el servidor.*
* *Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes).*
* *Duplicidad de LAN.*
* *Pruebas unitarias del SW.*

Para cada una de las amenazas identificadas con anterioridad puede aplicar alguna de las acciones de mitigación anteriores. La relación exhaustiva de amenazas y mitigaciones se indica en la siguiente tabla:

|  |  |
| --- | --- |
| AMENAZA | MITIGACIÓN |
| *Especificación defectuosa* | *Revisiones de requisitos* |
| *Diseño defectuoso* | *Revisiones de diseño* |
| *Validación defectuosa* | *Pruebas de validación* |
| *Fallo HW en Operador* | *Traslado de funciones entre terminales* |
| *Fallo HW en Operador Gestor* | *Traslado de funciones entre terminales* |
| *Redundancia y conmutación automática del servicio NBX* |
| *Fallo HW en Pasarela* | *Redundancia en CPU y en la tarjeta de interface en las pasarelas* |
| *Fallo HW en Gestión* | *Dualidad en el servidor* |
| *Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes)* |
| *Fallo HW en LAN* | *Duplicidad de LAN* |
| *Fallo SW en Operador* | *Traslado de funciones entre terminales* |
| *Pruebas unitarias del SW* |
| *Pruebas de validación* |
| *Fallo SW en Operador Gestor* | *Traslado de funciones entre terminales* |
| *Redundancia y conmutación automática del servicio NBX* |
| *Pruebas unitarias del SW* |
| *Pruebas de validación* |
| *Fallo SW en Pasarela* | *Redundancia en CPU y en la tarjeta de interface en las pasarelas* |
| *Pruebas unitarias del SW* |
| *Pruebas de validación* |
| *Fallo SW en Gestión* | *Dualidad en el servidor* |
| *Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes)* |
| *Pruebas unitarias del SW* |
| *Pruebas de validación* |

1. Amenazas y Mitigaciones.

En esta tabla falta filtrar por función. En las tablas resultantes del análisis se indicará, para cada función las mitigacioness que le aplican.

## PROBABILIDAD

Para cada rama del árbol Función-Amenaza-Efecto se asigna una probabilidad.

La ED-153 propone las siguientes definiciones:

* *Muy probable (MP)*: no existen medidas de mitigación efectivas e independientes.
  + El número y eficiencia de las medidas de mitigación no se consideran suficientes para confiar en rebajar el nivel de SWAL.
  + El número y eficiencia de las medidas de mitigación pueden considerarse suficientes desde un punto de vista individual, sin embargo los criterios de aislamiento se encuentran seriamente dañados (modo común de fallo).
  + Las medidas de mitigación no están probadas todavía ni está previsto que se prueben en el futuro.
  + La complejidad o novedad de las medidas de mitigación sugieren no confiar lo suficiente en ellas (análisis de la complejidad y completitud cuestionable).
  + Aunque existen medidas de mitigación, no se puede contar con ellas.
* *Probable (P)*: existen medidas de mitigación efectivas y aisladas.
  + Al menos se demuestra una medida de mitigación efectiva y aislada.
  + El número de medidas de mitigación es reducido pero la eficiencia de las mismas es significativa.
  + Exite un número de medidas de mitigación aisladas que tienen una eficiencia moderada.
* *Improbable (I)*: existen medidas de mitigación aisladas y muy efectivas.
  + El número de medidas de mitigación es limitado pero la eficiencia de las mismas es muy significativa.
  + Existen un número significativo de medidas de mitigación aisladas con una eficiencia significativa.
* *Muy improbable (MI)*: existen medidas de mitigación aisladas y extremadamente eficientes.
  + El número de medidas de mitigación es limitado pero la eficiencia de las mismas es extremadamente significativa.
  + Existe un número muy significativo de medidas de mitigación aisladas que tienen una eficiencia significativa.
  + Existe un número significativo de mediadas de mitigación aisladas que tienen una eficiencia muy significativa.

## SEVERIDAD

Para cada rama del árbol Función-Amenaza-Efecto se asigna una severidad.

Esta severidad asignada podrá ser:

1 Más severo. Accidente.

2 Incidente serio.

3 Incidente mayor.

4 Incidente significativo.

5 Menos severo. Sin efecto sobre la seguridad.

**Conceptos de accidente e incidente de aviación**

El Anexo 13 al Convenio de Aviación Civil Internacional esta dedicado a la investigación de accidentes e incidentes de aviación.

Dada la trascendencia de estos conceptos, los incluimos a continuación tal y como figuran definidos en ese documento.

*Accidente.*

*Todo suceso, relacionado con la utilización de una aeronave, que ocurre dentro del período comprendido entre el momento en que una persona entra a bordo de la aeronave, con intención de realizar un vuelo, y el momento en que todas las personas han desembarcado, durante el cual:*

*a) cualquier persona sufre lesiones mortales o graves a consecuencia de:*

*— hallarse en la aeronave, o*

*— por contacto directo con cualquier parte de la aeronave, incluso las partes que se hayan desprendido de la aeronave, o*

*— por exposición directa al chorro de un reactor, excepto cuando las lesiones obedezcan a causas naturales, se las haya causado una persona a sí misma o hayan sido causadas por otras personas o se trate de lesiones sufridas por pasajeros clandestinos escondidos fuera de las áreas destinadas normalmente a los pasajeros y la tripulación; o*

*b) la aeronave sufre daños o roturas estructurales que:*

*— afectan adversamente su resistencia estructural, su performance o sus características de vuelo; y*

*— que normalmente exigen una reparación importante o el recambio del componente afectado,*

*excepto por falla o daños del motor, cuando el daño se limita al motor, su capó o sus accesorios; o por daños limitados en las hélices, extremos de ala, antenas, neumáticos, frenos o carenas, pequeñas abolladuras o perforaciones en el revestimiento de la aeronave; o*

*c) la aeronave desaparece o es totalmente inaccesible.*

*Nota 1.— Para uniformidad estadística únicamente, toda lesión que ocasione la muerte dentro de los 30 días contados a partir de la fecha en que ocurrió el accidente, está clasificada por la OACI como lesión mortal.*

*Nota 2.— Una aeronave se considera desaparecida cuando se da por terminada la búsqueda oficial y no se han localizado los restos.*

*Incidente.*

*Todo suceso relacionado con la utilización de una aeronave, que no llegue a ser un accidente, que afecte o pueda afectar la seguridad de las operaciones.*

*Nota.— En el Manual de notificación de accidentes/incidentes (Doc 9156) figura una lista de los tipos de incidentes de especial interés para la Organización de Aviación Civil Internacional en sus estudios de prevención de accidentes.*

*Incidente grave.*

*Incidente en el que intervienen circunstancias que indican que casi ocurrió un accidente.*

*Nota 1.— La diferencia entre accidente e incidente grave estriba solamente en el*

*resultado.*

*Nota 2.— Hay ejemplos de incidentes graves en el Adjunto C del Anexo 13 y en el Manual de notificación de accidentes/incidentes (Doc 9156).*

**Criterios para la evaluación de la severidad de un efecto**

Se entiende por severidad de un peligro su potencialidad de causar, o conducir a que se produzca, un accidente o incidente con daños personales o materiales. Normalmente es muy difícil demostrar una relación causa/efecto directa, por lo que deben considerarse los efectos del fallo sobre otros elementos del sistema (personas, procedimiento y equipos). Estos efectos a considerar sobre otros elementos son:

* Efectos sobre la tripulación de la aeronave (ej. Sobrecarga, habilidad de realizar su función, etc.).
* Efectos sobre los controladores aéreos (ej. Sobrecarga, habilidad de realizar su función, etc.).
* Efectos sobre la funcionalidad de la aeronave.
* Efecto sobre la funcionalidad de los sistemas de tierra.
* Efectos sobre la habilidad de proveer servicios seguros de gestión de tráfico aéreo (ej. Magnitud de la pérdida o corrupción de los servicios y/o funciones de gestión de tráfico aéreo).

Para evaluar el nivel de severidad de estos efectos se emplea la clasificación de la tabla siguiente, tomada de las definiciones de ESSAR4.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Clase de Severidad** | **1**  **(más severo)** | **2** | **3** | **4** | **5**  **(menos severo)** |
| Efecto sobre las operaciones | Accidentes | Incidente  serio | Incidente mayor | Incidente significativo | Sin efecto inmediato sobre la seguridad |
| Ejemplos | Uno o más accidentes catastróficos  Una o más colisiones en el aire  Una o más colisiones en tierra  Uno o más vuelos controlados a pista  Pérdida total de control de vuelo | Gran reducción en la separación sin que ni la tripulación ni el controlador sean capaces de controlar la situación  Uno o más aviones desviados de su ruta de tal modo que se requiere una maniobra brusca para evitar una colisión | Gran reducción en la separación pero con la tripulación o el controlador capaces de controlar la situación  Reducción menor en la separación sin que ni la tripulación ni el controlador sean capaces de controlar la situación totalmente | Aumento de la sobrecarga de la tripulación o del controlador aéreo o degradar ligeramente la capacidad funcional de habilitar el sistema CNS  Reducción menor en la separación pero la tripulación o el controlador son capaces de controlar la situación | No hay situaciones peligrosas |

1. Niveles de Severidad

## PROCESO DE ASIGNACIÓN SWAL

En el siguiente apartado aparecen las tablas resultantes del análisis funcional de las amenazas para el ULISES V5000I.

Para cada rama del árbol Función-Amenaza-Efecto-Mitigación se asigna un SWAL para una combinación de probalidad y severidad.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Severidad  Probabilidad | 1 | 2 | 3 | 4 |
| **Muy Probable** | SWAL1 | SWAL2 | SWAL3 | SWAL4 |
| **Probable** | SWAL2 | SWAL3 | SWAL3 | SWAL4 |
| **Improbable** | SWAL3 | SWAL3 | SWAL4 | SWAL4 |
| **Muy Improbable** | SWAL4 | SWAL4 | SWAL4 | SWAL4 |

1. Relación de SWAL con la probabilidad y severidad de los fallos

El valor SWAL asignado a un equipo será el SWAL más crítico de los módulos que lo componen. Todos los módulos SWAL de dicho equipo deben ser desarrollados como si tuviesen dicho SWAL.

El SWAL asignado proporciona una medida uniforme de cómo el software es definido, desarrollado, puesto en operación y retirado (aseguramiento del proceso) y una medida de la habilidad del producto para funcionar como se esperaba (aseguramiento del producto).

La siguiente tabla muestra, para valores de SWAL crecientes, las parejas resultantes de probabilidad y severidad.

|  |  |  |
| --- | --- | --- |
| SWAL | PROBABILIDAD | SEVERIDAD |
| SWAL1 | Muy Probable | 1 |
| SWAL2 | Probable | 1 |
| Muy Probable | 2 |
| SWAL3 | Improbable | 1 |
| Probable | 2 |
| Improbable | 2 |
| Muy Probable | 3 |
| Probable | 3 |
| SWAL4 | Muy Improbable | 1 |
| Muy Improbable | 2 |
| Improbable | 3 |
| Muy Improbable | 3 |
| Muy Probable | 4 |
| Probable | 4 |
| Improbable | 4 |
| Muy Improbable | 4 |

1. SWAL creciente. Probabilidad y severidad.

Lógicamente, será función del nivel SWAL asignado a un producto las exigencias requeridas en el proceso de evaluación de la seguridad (detalle de descripción, verificación, evidencias…).

## 

## TABLAS RESULTANTES DEL ANÁLISIS

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Función | Amenaza | Efecto | Probabilidad | Severidad | Mitigación | SWAL |
| Comunicaciones Tierra / Aire – Transmisión | Especificación defectuosa | Funcionalidad no adecuada | Improbable | 3 | * Revisión de requisitos | 4 |
| Diseño defectuoso | degradación de comunicaciones t/a | Improbable | 3 | * Revisión de diseño | 4 |
| degradación de servicios de re-configuración | Improbable | 3 | * Revisión de diseño | 4 |
| degradación de la supervisión del sistema | Improbable | 3 | * Revisión de diseño | 4 |
| Validación defectuosa | degradación de comunicaciones t/a | Improbable | 3 | * Pruebas de validación | 4 |
| degradación de servicios de re-configuración | Improbable | 3 | * Pruebas de validación | 4 |
| degradación de la supervisión del sistema | Improbable | 3 | * Pruebas de validación | 4 |
| Fallo HW en Operador | degradación de comunicaciones t/a | Improbable | 3 | * Traslado de funciones entre terminales | 4 |
| Fallo HW en Operador Gestor | perdida de comunicaciones t/a | Improbable | 3 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| degradación de comunicaciones t/a | Improbable | 3 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| Fallo HW en Pasarela | degradación de comunicaciones t/a | Improbable | 3 | * Redundancia en CPU y en la tarjeta de interface en las pasarelas | 4 |
| Fallo HW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de la supervisión del sistema |  | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| Fallo HW en LAN | perdida de comunicaciones t/a | Muy Improbable | 3 | * Duplicidad de lan | 4 |
| perdida de servicios de re-configuración | Muy Improbable | 3 | * Duplicidad de lan | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 3 | * Duplicidad de lan | 4 |
| Fallo SW en Operador | degradación de comunicaciones t/a | Improbable | 3 | * Pruebas de validación * Traslado de funciones entre terminales * Pruebas unitarias del sw | 4 |
| Fallo SW en Operador Gestor | perdida de comunicaciones t/a | Muy Improbable | 3 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| degradación de comunicaciones t/a | Muy Improbable | 3 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| Fallo SW en Pasarela | degradación de comunicaciones t/a | Improbable | 3 | * Pruebas de validación * Redundancia en CPU y en la tarjeta de interface en las pasarelas * Pruebas unitarias del sw | 4 |
| Fallo SW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de la supervisión del sistema | Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |

1. Comunicaciones Tierra / Aire – Transmisión

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Función | Amenaza | Efecto | Probabilidad | Severidad | Mitigación | SWAL |
| Comunicaciones Tierra / Aire – Recepción | Especificación defectuosa | Funcionalidad no adecuada | Improbable | 3 | * Revisión de requisitos | 4 |
| Diseño defectuoso | degradación de comunicaciones t/a | Improbable | 3 | * Revisión de diseño | 4 |
| degradación de servicios de re-configuración | Improbable | 3 | * Revisión de diseño | 4 |
| degradación de la supervisión del sistema | Improbable | 3 | * Revisión de diseño | 4 |
| Validación defectuosa | degradación de comunicaciones t/a | Improbable | 3 | * Pruebas de validación | 4 |
| degradación de servicios de re-configuración | Improbable | 3 | * Pruebas de validación | 4 |
| degradación de la supervisión del sistema | Improbable | 3 | * Pruebas de validación | 4 |
| Fallo HW en Operador | degradación de comunicaciones t/a | Improbable | 3 | * Traslado de funciones entre terminales | 4 |
| Fallo HW en Operador Gestor | perdida de comunicaciones t/a | Improbable | 3 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| degradación de comunicaciones t/a | Improbable | 3 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| Fallo HW en Pasarela | degradación de comunicaciones t/a | Improbable | 3 | * Redundancia en CPU y en la tarjeta de interface en las pasarelas | 4 |
| Fallo HW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de la supervisión del sistema | Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| Fallo HW en LAN | perdida de comunicaciones t/a | Muy Improbable | 3 | * Duplicidad de lan | 4 |
| perdida de servicios de re-configuración | Muy Improbable | 3 | * Duplicidad de lan | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 3 | * Duplicidad de lan | 4 |
| Fallo SW en Operador | degradación de comunicaciones t/a | Improbable | 3 | * Pruebas de validación * Traslado de funciones entre terminales * Pruebas unitarias del sw | 4 |
| Fallo SW en Operador Gestor | perdida de comunicaciones t/a | Muy Improbable | 3 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| degradación de comunicaciones t/a | Muy Improbable | 3 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| Fallo SW en Pasarela | degradación de comunicaciones t/a |  | 3 |  | 4 |
| Fallo SW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de la supervisión del sistema | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |

1. Comunicaciones Tierra / Aire – Recepción

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Función | Amenaza | Efecto | Probabilidad | Severidad | Mitigación | SWAL |
| Comunicaciones Tierra / Aire – Retransmisión | Especificación defectuosa | Funcionalidad no adecuada | Improbable | 3 | * Revisión de requisitos | 4 |
| Diseño defectuoso | degradación de comunicaciones t/a | Improbable | 3 | * Revisión de diseño | 4 |
| degradación de servicios de re-configuración | Improbable | 3 | * Revisión de diseño | 4 |
| degradación de la supervisión del sistema | Improbable | 3 | * Revisión de diseño | 4 |
| Validación defectuosa | degradación de comunicaciones t/a | Improbable | 3 | * Pruebas de validación | 4 |
| degradación de servicios de re-configuración | Improbable | 3 | * Pruebas de validación | 4 |
| degradación de la supervisión del sistema | Improbable | 3 | * Pruebas de validación | 4 |
| Fallo HW en Operador | degradación de comunicaciones t/a | Improbable | 3 | * Traslado de funciones entre terminales | 4 |
| Fallo HW en Operador Gestor | perdida de comunicaciones t/a | Improbable | 3 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| degradación de comunicaciones t/a | Improbable | 3 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| Fallo HW en Pasarela | degradación de comunicaciones t/a | Improbable | 3 | * Redundancia en CPU y en la tarjeta de interface en las pasarelas | 4 |
| Fallo HW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de la supervisión del sistema | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| Fallo HW en LAN | perdida de comunicaciones t/a | Muy Improbable | 3 | * Duplicidad de lan | 4 |
| perdida de servicios de re-configuración | Muy Improbable | 3 | * Duplicidad de lan | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 3 | * Duplicidad de lan | 4 |
| Fallo SW en Operador | degradación de comunicaciones t/a | Improbable | 3 | * Pruebas de validación * Traslado de funciones entre terminales * Pruebas unitarias del sw | 4 |
| Fallo SW en Operador Gestor | perdida de comunicaciones t/a | Muy Improbable | 3 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| degradación de comunicaciones t/a | Muy Improbable | 3 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| Fallo SW en Pasarela | degradación de comunicaciones t/a | Improbable | 3 | * Pruebas de validación * Redundancia en CPU y en la tarjeta de interface en las pasarelas * Pruebas unitarias del sw | 4 |
| Fallo SW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de la supervisión del sistema | Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |

1. Comunicaciones Tierra / Aire – Retransmisión

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Función | Amenaza | Efecto | Probabilidad | Severidad | Mitigación | SWAL |
| Comunicaciones Tierra / Aire – Redundancia Servicio | Especificación defectuosa | Funcionalidad no adecuada | Improbable | 3 | * Revisión de requisitos | 4 |
| Diseño defectuoso | degradación de comunicaciones t/a | Improbable | 3 | * Revisión de diseño | 4 |
| degradación de servicios de re-configuración | Improbable | 3 | * Revisión de diseño | 4 |
| degradación de la supervisión del sistema | Improbable | 3 | * Revisión de diseño | 4 |
| Validación defectuosa | degradación de comunicaciones t/a | Improbable | 3 | * Pruebas de validación | 4 |
| degradación de servicios de re-configuración | Improbable | 3 | * Pruebas de validación | 4 |
| degradación de la supervisión del sistema | Improbable | 3 | * Pruebas de validación | 4 |
| Fallo HW en Operador | degradación de comunicaciones t/a | Improbable | 3 | * Traslado de funciones entre terminales | 4 |
| Fallo HW en Operador Gestor | perdida de comunicaciones t/a | Improbable | 3 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| degradación de comunicaciones t/a | Improbable | 3 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| Fallo HW en Pasarela | degradación de comunicaciones t/a | Improbable | 3 | * Redundancia en CPU y en la tarjeta de interface en las pasarelas | 4 |
| Fallo HW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de la supervisión del sistema | Muy Improbable | 3 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| Fallo HW en LAN | perdida de comunicaciones t/a | Muy Improbable | 3 | * Duplicidad de lan | 4 |
| perdida de servicios de re-configuración | Muy Improbable | 3 | * Duplicidad de lan | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 3 | * Duplicidad de lan | 4 |
| Fallo SW en Operador | degradación de comunicaciones t/a | Improbable | 3 | * Pruebas de validación * Traslado de funciones entre terminales * Pruebas unitarias del sw | 4 |
| Fallo SW en Operador Gestor | perdida de comunicaciones t/a | Muy Improbable | 3 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| degradación de comunicaciones t/a | Muy Improbable | 3 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| Fallo SW en Pasarela | degradación de comunicaciones t/a | Improbable | 3 | * Pruebas de validación * Redundancia en CPU y en la tarjeta de interface en las pasarelas * Pruebas unitarias del sw | 4 |
| Fallo SW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de la supervisión del sistema | Muy Improbable | 3 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |

1. Comunicaciones Tierra / Aire – Redundancia Servicio

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Función | Amenaza | Efecto | Probabilidad | Severidad | Mitigación | SWAL |
| Comunicaciones Tierra / Tierra – Acceso Directo / Acceso Indirecto | Especificación defectuosa | Funcionalidad no adecuada | Improbable | 4 | * Revisión de requisitos | 4 |
| Diseño defectuoso | degradación de comunicaciones t/t | Improbable | 4 | * Revisión de diseño | 4 |
| degradación de servicios de re-configuración | Improbable | 4 | * Revisión de diseño | 4 |
| degradación de la supervisión del sistema | Improbable | 4 | * Revisión de diseño | 4 |
| Validación defectuosa | degradación de comunicaciones t/t | Improbable | 4 | * Pruebas de validación | 4 |
| degradación de servicios de re-configuración | Improbable | 4 | * Pruebas de validación | 4 |
| degradación de la supervisión del sistema | Improbable | 4 | * Pruebas de validación | 4 |
| Fallo HW en Operador | degradación de comunicaciones t/t | Improbable | 4 | * Traslado de funciones entre terminales | 4 |
| Fallo HW en Operador Gestor | perdida de comunicaciones t/t | Improbable | 4 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| degradación de comunicaciones t/t |  | 4 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| Fallo HW en Pasarela | degradación de comunicaciones t/t |  | 4 | * Redundancia en CPU y en la tarjeta de interface en las pasarelas | 4 |
| Fallo HW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 4 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 4 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 4 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de la supervisión del sistema | Muy Improbable | 4 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| Fallo HW en LAN | perdida de comunicaciones t/t | Muy Improbable | 4 | * Duplicidad de lan | 4 |
| perdida de servicios de re-configuración | Muy Improbable | 4 | * Duplicidad de lan | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 4 | * Duplicidad de lan | 4 |
| Fallo SW en Operador | degradación de comunicaciones t/t | Improbable | 4 | * Pruebas de validación * Traslado de funciones entre terminales * Pruebas unitarias del sw | 4 |
| Fallo SW en Operador Gestor | perdida de comunicaciones t/t | Muy Improbable | 4 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| degradación de comunicaciones t/t | Muy Improbable | 4 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| Fallo SW en Pasarela | degradación de comunicaciones t/t | Improbable | 4 | * Pruebas de validación * Redundancia en CPU y en la tarjeta de interface en las pasarelas * Pruebas unitarias del sw | 4 |
| Fallo SW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 4 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 4 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 4 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de la supervisión del sistema | Muy Improbable | 4 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |

1. Comunicaciones Tierra / Tierra – Acceso Directo / Acceso Indirecto

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Función | Amenaza | Efecto | Probabilidad | Severidad | Mitigación | SWAL |
| Comunicaciones Tierra / Tierra – Acceso Instantáneo | Especificación defectuosa | Funcionalidad no adecuada | Improbable | 4 | * Revisión de requisitos | 4 |
| Diseño defectuoso | degradación de comunicaciones t/t | Improbable | 4 | * Revisión de diseño | 4 |
| degradación de servicios de re-configuración | Improbable | 4 | * Revisión de diseño | 4 |
| degradación de la supervisión del sistema | Improbable | 4 | * Revisión de diseño | 4 |
| Validación defectuosa | degradación de comunicaciones t/t | Improbable | 4 | * Pruebas de validación | 4 |
| degradación de servicios de re-configuración | Improbable | 4 | * Pruebas de validación | 4 |
| degradación de la supervisión del sistema | Improbable | 4 | * Pruebas de validación | 4 |
| Fallo HW en Operador | degradación de comunicaciones t/t | Improbable | 4 | * Traslado de funciones entre terminales | 4 |
| Fallo HW en Operador Gestor | perdida de comunicaciones t/t | Improbable | 4 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| degradación de comunicaciones t/t | Improbable | 4 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| Fallo HW en Pasarela | degradación de comunicaciones t/t | Improbable | 4 | * Redundancia en CPU y en la tarjeta de interface en las pasarelas | 4 |
| Fallo HW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 4 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 4 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 4 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de la supervisión del sistema | Muy Improbable | 4 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| Fallo HW en LAN | perdida de comunicaciones t/t | Muy Improbable | 4 | * Duplicidad de lan | 4 |
| perdida de servicios de re-configuración | Muy Improbable | 4 | * Duplicidad de lan | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 4 | * Duplicidad de lan | 4 |
| Fallo SW en Operador | degradación de comunicaciones t/t | Improbable | 4 | * Pruebas de validación * Traslado de funciones entre terminales * Pruebas unitarias del sw | 4 |
| Fallo SW en Operador Gestor | perdida de comunicaciones t/t | Muy Improbable | 4 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| degradación de comunicaciones t/t | Muy Improbable | 4 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| Fallo SW en Pasarela | degradación de comunicaciones t/t | Improbable | 4 | * Pruebas de validación * Redundancia en CPU y en la tarjeta de interface en las pasarelas * Pruebas unitarias del sw | 4 |
| Fallo SW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 4 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 4 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 4 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de la supervisión del sistema | Muy Improbable | 4 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |

1. Comunicaciones Tierra / Tierra – Acceso Instantáneo

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Función | Amenaza | Efecto | Probabilidad | Severidad | Mitigación | SWAL |
| Comunicaciones Tierra / Tierra – Servicios Suplementarios | Especificación defectuosa | Funcionalidad no adecuada | Improbable | 4 | * Revisión de requisitos | 4 |
| Diseño defectuoso | degradación de comunicaciones t/t | Improbable | 4 | * Revisión de diseño | 4 |
| degradación de servicios de re-configuración | Improbable | 4 | * Revisión de diseño | 4 |
| degradación de la supervisión del sistema | Improbable | 4 | * Revisión de diseño | 4 |
| Validación defectuosa | degradación de comunicaciones t/t | Improbable | 4 | * Pruebas de validación | 4 |
| degradación de servicios de re-configuración | Improbable | 4 | * Pruebas de validación | 4 |
| degradación de la supervisión del sistema | Improbable | 4 | * Pruebas de validación | 4 |
| Fallo HW en Operador | degradación de comunicaciones t/t | Improbable | 4 | * Traslado de funciones entre terminales | 4 |
| Fallo HW en Operador Gestor | perdida de comunicaciones t/t | Improbable | 4 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| degradación de comunicaciones t/t | Improbable | 4 | * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX | 4 |
| Fallo HW en Pasarela | degradación de comunicaciones t/t | Improbable | 4 | * Redundancia en CPU y en la tarjeta de interface en las pasarelas | 4 |
| Fallo HW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 4 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 4 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 4 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| degradación de la supervisión del sistema | Muy Improbable | 4 | * Dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) | 4 |
| Fallo HW en LAN | perdida de comunicaciones t/t | Muy Improbable | 4 | * Duplicidad de lan | 4 |
| perdida de servicios de re-configuración | Muy Improbable | 4 | * Duplicidad de lan | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 4 | * Duplicidad de lan | 4 |
| Fallo SW en Operador | degradación de comunicaciones t/t | Improbable | 4 | * Pruebas de validación * Traslado de funciones entre terminales * Pruebas unitarias del sw | 4 |
| Fallo SW en Operador Gestor | perdida de comunicaciones t/t | Muy Improbable | 4 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| degradación de comunicaciones t/t | Muy Improbable | 4 | * Pruebas de validación * Traslado de funciones entre terminales * Redundancia y conmutacion automatica del servicio NBX * Pruebas unitarias del sw | 4 |
| Fallo SW en Pasarela | degradación de comunicaciones t/t | Improbable | 4 | * Pruebas de validación * Redundancia en CPU y en la tarjeta de interface en las pasarelas * Pruebas unitarias del sw | 4 |
| Fallo SW en Gestión | perdida de servicios de re-configuración | Muy Improbable | 4 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de servicios de re-configuración | Muy Improbable | 4 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| perdida de la supervisión del sistema | Muy Improbable | 4 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |
| degradación de la supervisión del sistema | Muy Improbable | 4 | * Pruebas de validación * dualidad en el servidor * Modo de funcionamiento sin servidor (se aseguran las comunicaciones existentes) * Pruebas unitarias del sw | 4 |

1. Comunicaciones Tierra / Tierra – Servicios Suplementarios

# CARPETA DE SEGURIDAD SOFTWARE (SSF)

## PARTE 1: ENTORNO

### DESCRIPCION DEL SISTEMA

Una breve descripción del sistema se encuentra en el apartado 2 de este documento. Se lleva a cabo una descripción de la arquitectura a nivel hardware y software.

Esta descripción se considera suficiente para desarrollar posteriormente el análisis funcional de amenazas.

Una descripción más precisa se encuentra en los documentos:

* ***JIN12001. P07005U. Documento de Diseño Basico.***
* ***JIN12001. P07005U. Documento de Diseño Detalle.***

Estos documentos están redactados siguiendo el procedimiento ***P07005 Procedimiento para el Control del Diseño y Desarrollo***.

### ENTORNO OPERACIONAL

Aunque algo del entorno se encuentra en el apartado 2 de este documento, el detalle se encuentra en los documentos:

* ***JIN12001. P07005U. Documento de Diseño Basico.***
* ***JIN12001. P07005U. Documento de Diseño Detalle.***

Estos documentos están redactados siguiendo el procedimiento ***P07005 Procedimiento para el Control del Diseño y Desarrollo***.

### LISTADO DE HERRAMIENTAS

En nuestro procedimiento ***P07005 Procedimiento para el Control del Diseño y Desarrollo*** se establece que dentro de las actividades de planificación de un proyecto se elabora el Plan de Desarrollo.

Este Plan de Desarrollo debe contener información relativa a las herramientas a utilizar en dicho desarrollo.

En el documento ***JIN12001.P07005D.Plan de Diseño y Desarrollo*** aparecen las herramientas que aplican en este desarrollo. En concreto para el software son:

|  |  |  |
| --- | --- | --- |
| APLICACIÓN | HERRAMIENTA | DESCRIPCION |
| DESARROLLO SOFTWARE | Visual Studio 2010 | Entorno Desarrollo Windows |
| Linux GNU gcc | Entorno Desarrollo LINUX |
| Enterprise Architect | Diseño UML |
| Documentación | Microsoft Office 2010 | Suite Informática |
| ProjectLibre 1.5.3 | Planificación |

1. Herramientas Desarrollo Software

## Parte 2: Contexto de la Garantía de la Seguridad SW

### Regulación aplicable

* ED-153 “Guidelines for ANS Software Assurance” Agosto 2009.
* Material guia para la garantia del software. AENA. A111b-09-GUI-01-3.2. Noviembre 2013.
* Investigación de accidentes e incidentes de aviación. Anexo 13 al Convenio sobre Aviación Civil Internacional. Julio 2001.
* ESARR 6. Software in ATM Functional Systems, ed.2.0. Mayo 2010.
* ESARR 4. Risk Assessment and mitigation in ATM, ed.1.0. Abril 2001.
* Air Navigation System SAFETY ASSESSMENT METHODOLOGY. SAF.ET1.ST03.1000-MAN-01-00. Edición 2.1. Octubre 2006.
* SAM PART I. Functional Hazard Assessment. SAF.ET1.ST03.1000-MAN-01-01-00. Edición 2.1. Octubre 2006.
* SAM PART II. Preliminary System Safety Assessment. SAF.ET1.ST03.1000-MAN-01-02-00. Edición 2.1. Octubre 2006.
* SAM PART III. System Safety Assessment. SAF.ET1.ST03.1000-MAN-01-03-00. Edición 2.1. Octubre 2006.
* SAM PART IV. Annexes. SAF.ET1.ST03.1000-MAN-01-04. Edición 2.1. Octubre 2006.
* “ANS Software Lifecycle” SAF.ET1.ST03.1000-REP-01-00. Edición 3.0. Diciembre 2005
* “Recommendations for A.N.S. software” SAF.ET1.ST03.1000.GUI-01-00. Edición 1.0. Diciembre 2005.
* P07005 Control del Diseño y Desarrollo.
* P07005AC\_GUIA ELABORACION ERS CON UML-EA.
* P07005AD. RedMine. Guia de Utilizacion.
* P07008 Investigación, innovación y Vigilancia Tecnológica.
* P07023 Industrialización.
* P04001 Gestion de la Documentacion y de los Registros.
* P07007 Procedimiento General de Compras.
* P06001 Formacion y Toma de Conciencia.
* P08002 Auditorías internas de Calidad y Medio Ambiente.

### Estándares aplicables

* ED-153 “Guidelines for ANS Software Assurance” Agosto 2009.
* Material guia para la garantia del software. AENA. A111b-09-GUI-01-3.2. Noviembre 2013.
* Investigación de accidentes e incidentes de aviación. Anexo 13 al Convenio sobre Aviación Civil Internacional. Julio 2001.
* ESARR 6. Software in ATM Functional Systems, ed.2.0. Mayo 2010.
* ESARR 4. Risk Assessment and mitigation in ATM, ed.1.0. Abril 2001.
* Air Navigation System SAFETY ASSESSMENT METHODOLOGY. SAF.ET1.ST03.1000-MAN-01-00. Edición 2.1. Octubre 2006.
* SAM PART I. Functional Hazard Assessment. SAF.ET1.ST03.1000-MAN-01-01-00. Edición 2.1. Octubre 2006.
* SAM PART II. Preliminary System Safety Assessment. SAF.ET1.ST03.1000-MAN-01-02-00. Edición 2.1. Octubre 2006.
* SAM PART III. System Safety Assessment. SAF.ET1.ST03.1000-MAN-01-03-00. Edición 2.1. Octubre 2006.
* SAM PART IV. Annexes. SAF.ET1.ST03.1000-MAN-01-04. Edición 2.1. Octubre 2006.
* “ANS Software Lifecycle” SAF.ET1.ST03.1000-REP-01-00. Edición 3.0. Diciembre 2005
* “Recommendations for A.N.S. software” SAF.ET1.ST03.1000.GUI-01-00. Edición 1.0. Diciembre 2005.

### Análisis y Mitigación de Riesgos

El documento, ***JIN12001.PSSA,*** está en la carpeta de Diseño. Es la fase de Evaluación Preliminar de la Seguridad del Sistema. Incluye:

* Descripción de la Arquitectura del Sistema. En concreto una descripción de la arquitectura hardware, una descripción de la arquitectura software y la relación entre los módulos hardware y software.
* Análisis Funcional de Amenazas (FHA). El objeto de este análisis es la identificación del SWAL. La secuencia de tareas a realizar son las siguientes:
  + Identificación de las funciones del sistema.
  + Identificación de las amenazas potenciales.
  + Identificación de los Efectos o Consecuencias de las Amenazas.
  + Probabilidad.
  + Severidad.
  + Descripción de las medidas de mitigación.
  + Identificación del SWAL
* Carpeta de Seguridad del Software (SSF). Este apartado sigue la estructura propuesta en la ED-153. Contiene una lista de evidencias o referencias a las mismas.

Teniendo en cuenta que este documento se elabora en la actividad de diseño se entiende que algunos de los capítulos de la SSF todavía no presenten la evidencia correspondiente.

En la carpeta de Resultados, está el presente documento ***JIN12001.SSA***. Es la fase de Evaluación de la Seguridad del Sistema. Teniendo en cuenta que este documento se prepara con el sistema ya desarrollado, se entiende que la carpeta SSF ya puede hacer referencia a las evidencias correspondientes.

En concreto, incluye:

* Descripción de la Arquitectura del Sistema. En concreto una descripción de la arquitectura hardware, una descripción de la arquitectura software y la relación entre los módulos hardware y software.
* Análisis Funcional de Amenazas (FHA). El objeto de este análisis es la identificación del SWAL. La secuencia de tareas a realizar son las siguientes:
  + Identificación de las funciones del sistema.
  + Identificación de las amenazas potenciales.
  + Identificación de los Efectos o Consecuencias de las Amenazas.
  + Probabilidad.
  + Severidad.
  + Descripción de las medidas de mitigación.
  + Identificación del SWAL
* Carpeta de Seguridad del Software (SSF). Este apartado sigue la estructura propuesta en la ED-153. Contiene una lista de evidencias o referencias a las mismas.

## Parte 3: Proceso de Garantía de la Seguridad SW

### Plan de Gestión de la Seguridad

En aquellos desarrollos en los que es requisito la garantía de la seguridad del software, se elaboran, además, los siguientes documentos:

***Evaluación Preliminar de la Seguridad del Sistema (PSSA)***

Este documento se elabora en la fase de diseño. Incluye:

* Descripción de la Arquitectura del Sistema. En concreto una descripción de la arquitectura hardware, una descripción de la arquitectura software y la relación entre los módulos hardware y software.
* Análisis Funcional de Amenazas (FHA). El objeto de este análisis es la identificación del SWAL.
* Carpeta de Seguridad del Software (SSF). Este apartado sigue la estructura propuesta en la ED-153. Contiene una lista de evidencias o referencias a las mismas.

Teniendo en cuenta que este documento se elabora en la actividad de diseño se entiende que algunos de los capítulos de la SSF todavía no presenten la evidencia correspondiente.

***Evaluación de la Seguridad del Sistema (SSA)***

Teniendo en cuenta que este documento se prepara con el sistema ya desarrollado, se entiende que la carpeta SSF ya puede hacer referencia a las evidencias correspondientes.

En concreto, incluye:

* Descripción de la Arquitectura del Sistema. En concreto una descripción de la arquitectura hardware, una descripción de la arquitectura software y la relación entre los módulos hardware y software.
* Análisis Funcional de Amenazas (FHA). El objeto de este análisis es la identificación del SWAL.
* Carpeta de Seguridad del Software (SSF). Este apartado sigue la estructura propuesta en la ED-153. Contiene una lista de evidencias o referencias a las mismas.

En la tabla siguiente se presenta la estructura típica de carpetas (o directorios) que se utilizan para un desarrollo con garantía de seguridad software. Para cada carpeta hay una indicación de su contenido. Está resaltada la documentación específica de garantía de seguridad software.

|  |  |
| --- | --- |
| CARPETA | CONTENIDO |
| Especificación | Especificación de Requisitos Software |
| Lista de Casos de Prueba |
| Planificación | Plan de Calidad |
| Plan de Diseño y Desarrollo |
| Diseño | Diseño Básico |
| Diseño de Detalle |
| ***Evaluación Preliminar de la Seguridad del Sistema (PSSA)*** |
| Resultados | Control de Configuración |
| Informes de Pruebas de Verificación |
| Informes de Pruebas de Validación |
| ***Evaluación de la Seguridad del Sistema (SSA)*** |
| En paralelo a estas carpetas con documentación sobre el plan de calidad, se mantiene un repositorio donde se almacena:   * Doc: documentación del producto. * Bin: ejecutables del software. * Src: fuentes del software. |
| Registros | Revisión de Datos de Partida |
| Revisión de Diseño |
| Actas de Verificación |
| Actas de Validación |
| Seguimiento | Informe de Seguimiento |

1. Plan de Gestión de la Seguridad

### Revisión del PLAN

El documento ***JIN1201.P07005E. Acta Revision Diseño*** se elabora examinando la documentación de diseño. Los objetivos de esta revisión son:

* La arquitectura diseñada tiene que describir completamente el sistema.
* Deben estar contemplados todos los requisitos.
* Tiene que desarrollarse una matriz de trazabilidad.
* El diseño tiene que ser verificable.
* El diseño tiene que contemplar las consideraciones de seguridad.

Dentro de la documentación de diseño está la Evaluación Preliminar de la Seguridad del Sistema ***(JIN12001.PSSA)*** que es uno de los documentos revisados en dicha acta.

Finalizada la fase de desarrollo se realizan las actividades de verificación y validación. Está disponible la Evaluación de la Seguridad del Sistema.

Como resultado de la verificación, se elabora el correspondiente “Informe de verificación”. El documento ***JIN12001.P07005Z.Informe de Pruebas de Verificacion*** contiene dicho informe.

Durante todo el proceso descrito, se ejecutan los correspondientes hitos de Revisión y Verificación que se hayan establecido en el Plan de Revisiones / Verificaciones establecido en la fase de Planificación. Cada hito de Revisión y Verificación debe dejar un registro en forma de Acta de Verificación. El documento ***JIN12001.P07005F.Acta Verificacion*** contiene dicha acta.

Como resultado de la validación, se elabora el correspondiente “Informe de validación”. El documento ***JIN12001.P07005Z.Informe de Pruebas de Validacion*** contiene dicho informe.

Durante todo el proceso descrito, se ejecutan los correspondientes hitos de Validación que se hayan establecido en el Plan de Validaciones establecido en la fase de Planificación. Cada hito de Validación debe dejar un registro en forma de Acta de Validación. El documento ***JIN12001.P07005G.Acta Validacion*** contiene dicha acta.

### Listado de documentación

Dentro de las actividades de planificación de un proyecto se elabora el Plan de Desarrollo.

El responsable de la edición de dicho documento es el Jefe de Proyecto. Se elabora a partir de la documentación existente en la carpeta de Especificación:

* Especificación de Requisitos Software.
* Lista de Casos de Prueba.

Este Plan de Desarrollo debe contener información relativa al Plan de Documentación de dicho desarrollo.

En el documento ***JIN12001.P07005D.Plan de Diseño y Desarrollo*** aparecen los documentos que aplican en este desarrollo.

## Parte 4: Requisitos de Seguridad

### Listado de Requisitos de Seguridad del SOFTWARE

* La empresa deberá garantizar, para aquellas tareas del ciclo de vida del SW bajo su responsabilidad, 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.
* La empresa deberá proporcionar las evidencias necesarias para demostrar el cumplimiento del SWAL 4, desarrollando la documentación necesaria o identificando en que documento/s se encuentran los siguientes contenidos:

a. Parte 1: Entorno.

* Descripción del Sistema (Ref. ED-153: 3.1.1, 3.1.2)
* Entorno operacional (Ref. ED-153: 3.1.1, 3.1.2)
* Listado de herramientas (Gestión de la configuración, de desarrollo) (Ref. ED-153: 4.3.9-12, 4.4.1, 5.1.x, 5.2.x, 5.4.1, 5.4.2, 5.8.1, 7.2.8, 7.2.10)

b. Parte 2: Contexto de la Garantía de la Seguridad SW.

* Regulación aplicable (Ref. ED-153: 3.1.3, 3.1.4)
* Estándares aplicables (Ref. ED-153: 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1)
* Análisis y Mitigación de Riesgos (Ref. ED-153: 3.0.9, 3.0.12, 3.0.17, 3.1.5, 3.3.x, 3.6.x)

c. Parte 3: Proceso de Garantía de la Seguridad SW.

* SMP: Plan de Gestión de la Seguridad (Safety) (Ref. ED-153: 3.2.x, 3.5.x)
* Revisión del SMP y listas de distribución del mismo, referencias a los mecanismos de mejora, validación y verificación (Ref. ED-153: 3.2.x, 3.4.x, 3.5.x, 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1)
* Listado de documentación y referencias a los procedimientos de documentación seguidos (Ref. ED-153: 3.2.x, 3.5.x, 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1)

d. Parte 4: Requisitos de Seguridad (Safety).

* Listado de Requisitos de Seguridad (Safety) del SW (Ref. ED-153: 3.0.2, 3.1.5, 3.3.x, 3.6.x, 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)

e. Parte 5: Modificaciones de Software.

* Gestión de Cambios (Ref. ED-153: 5.2.x, 7.2.8, 7.2.10)
* Gestión de Incidencias (Ref. ED-153: 5.2.x, 5.8.x, 7.2.8, 7.2.9, 7.2.10)
* Retirada, desinstalación de Software (Ref. ED-153: 4.4.x, 4.5.2, 4.5.3)

f. Parte 6: COTS.

* Plan de Garantía para COTS (CAP-COTS Assurance Plan). Adquisición, aceptación, verificación y gestión de configuración e incidencias para COTS (Ref. ED-153: 3.0.3, 4.1.7, 5.2.x, 5.8.x, 7.2.1, 7.2.8, 7.2.9, 7.2.10)
* Informe de Conformidad para COTS (CCR-COTS Comp. Report.). Especificación de requisitos derivados, y cumplimiento de la Garantía de la Seguridad del SW para COTS (Ref. ED-153: 3.0.2, 3.0.3, 3.0.13, 3.4.x, 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)

g. Parte 7: Garantías.

* Garantía de herramientas (Ref. ED-153: 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1)
* Asignación de SWAL y monitorización (Ref. ED-153: 3.0.5, 3.0.8, 3.0.11, 3.0.14, 3.0.15, 3.3.x, 3.1.5, 3.6.x, 4.1.7, 4.3.1, 4.3.2, 4.3.4, 4.3.5, 4.3.6, 4.3.9-12, 4.3.13, 4.3.14, 4.3.15, 4.4.1, 4.4.5, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1; 6.2.9; 6.2.12, 7.2.1, 7.2.4, 7.2.6)
* Auditorias y revisiones (Ref. ED-153: 3.0.9, 3.0.12, 3.0.17, 5.4.3-13, 5.7.2)
* Formación (Ref. ED-153: 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1)
* Requisitos correctos y completos (Ref. 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, 5.4.3-13, 5.7.2, 7.2.4, 7.2.6)
* Matriz de trazabilidad (Ref. ED-153: 3.0.3, 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, 5.4.3-13, 5.7.2, 7.2.4, 7.2.6)
* Funciones no deseadas (Ref. ED-153: 3.0.4, 3.1.5, 3.3.x, 3.6.x, 4.4.x, 4.5.2, 4.5.3, 5.4.3-13, 5.7.2, 5.8.x, 7.2.9)
* Satisfacción de requisitos (Ref. ED-153: 3.0.6, 3.4.x, 4.3.1, 4.3.2, 4.3.4, 4.3.5, 4.3.6, 4.3.9-15, 4.4.x, 4.5.2, 4.5.3, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.4.3-13, 5.7.2, 5.8.1, 7.2.4, 7.2.6)
* Gestión de la configuración (Ref. ED-153: 3.0.7, 4.3.9-12, 4.4.1, 5.1.x, 5.2.x, 5.4.1, 5.4.2, 5.8.1, 7.2.8, 7.2.10)
* Plan de desarrollo del Software (SDP) (Ref. ED-153: 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1)
* Mantenimiento (Ref. ED-153: 4.4.x, 4.5.2, 4.5.3)
* Verificación (Ref. ED-153: 3.0.10, 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.x, 4.5.2, 4.5.3, 5.4.3-13, 5.7.2, 7.2.4, 7.2.6)
* Calidad (Ref. ED-153: 5.4.3-13, 5.7.2)
* Garantía de que el SW es aceptablemente seguro (Ref. ED-153: 3.0.1, 3.0.9, 3.0.12, 3.0.17)

## Parte 5: Modificaciones de Software

### Gestión de Cambios

En el procedimiento ***P07005 Procedimiento para el Control del Diseño y Desarrollo*** se dice que, como resumen de la fase de desarrollo, se elaborará un documento de control de configuración, que incluya una parte para la gestión de cambios que refleje en el fututo las modificaciones introducidas en cada una de las versiones o revisiones del sistema.

Como resultado de la actividad de Pruebas y Verificación, se genera un conjunto revisado de los resultados de la fase de Desarrollo, acompañada por el correspondiente documento de control de configuración en el que se establecerá:

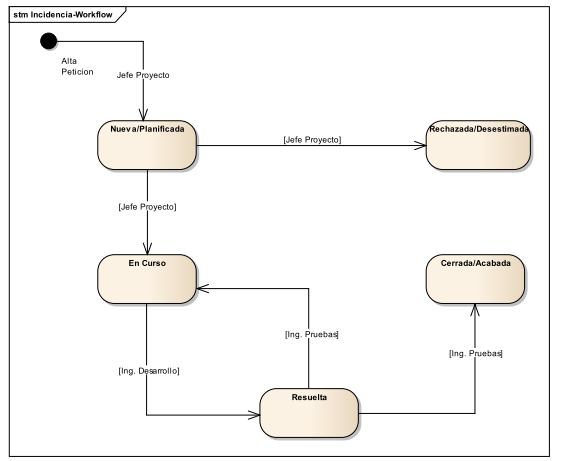
* Las modificaciones efectuadas respecto a la versión de entrada en la fase.
* Los componentes o módulos afectados por dichas modificaciones.

El documento ***JIN12001.P07005H.Control de Configuracion*** contiene dicho informe.

### Gestión de Incidencias

El procedimiento se implementa mediante la herramienta Redmine. La instrucción técnica ***P07005AD. RedMine. Guia de Utilizacion*** define como utilizar esta herramienta para la gestión de Proyectos e incidencias.

En la siguiente gráfica se presenta el flujo de trabajo que se sigue para el tratamiento de una incidencia.



1. Diagrama de Estados para peticiones tipo “incidencia”

Para la compresión de dicho diagrama de estados, se comentan algunas características de nuestra metodología.

Redmine es una aplicación web de gestión de proyectos multiplataforma de código abierto que nos permite llevar a cabo las tareas más comunes relacionadas con la asignación de tareas de desarrollo o mantenimiento entre los miembros de un equipo de trabajo.

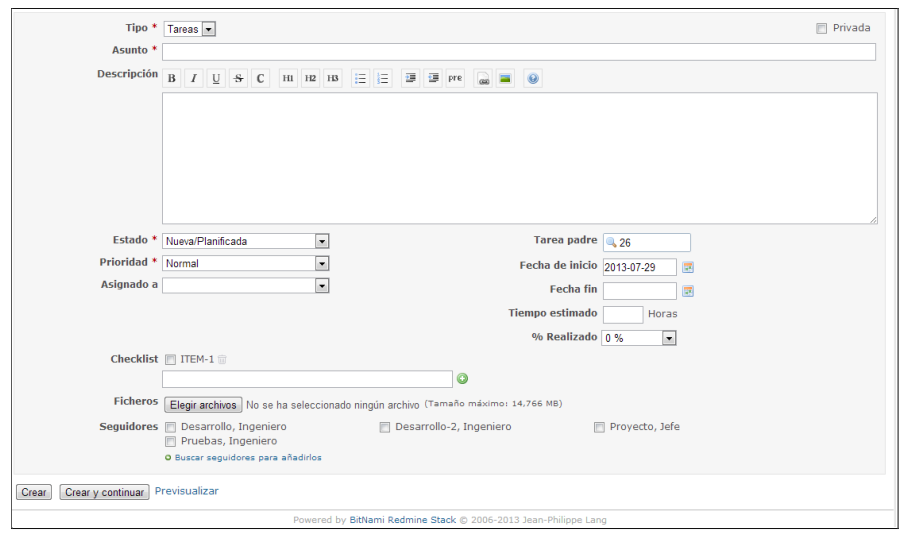
Al sistema se accede vía navegador WEB. Una vez realizado el “login”, en función del perfil del usuario, se presenta la información que cada usuario debe conocer y las opciones habilitadas a cada uno de ellos. Cada proyecto debe contar con los siguientes perfiles asignados:

* 1 Jefe de Proyecto.
* Ingenieros de Desarrollo.
* Ingenieros de Pruebas.

El jefe de proyecto asignado, tiene habilitados en la herramienta los siguientes procedimientos específicos:

* Planificación
  + Añadir Peticiones.
  + Borrar Peticiones.
  + Modificar o actualizar Peticiones.
* Seguimiento.
  + Actualizar datos.
  + Gestión de Peticiones.
  + Replanificación.
  + Registro de Trabajo.

Como ejemplo, se muestra una gráfica de datos a introducir en una incidencia.



1. Datos a introducir en una incidencia.

Las incidencias activas y asignadas a los ingenieros de desarrollo de un proyecto se muestran en la página personal de cada uno de ellos.

Sobre estas tareas, se pueden efectuar dos operaciones:

* Registro diario de los trabajos realizados.
* Dar por finalizada la tarea.

Las incidencias activas y asignadas a los ingenieros de pruebas de un proyecto se muestran en la página personal de cada uno de ellos.

Sobre estas tareas, se pueden efectuar dos operaciones:

* Registro diario de los trabajos realizados.
* Dar por finalizada la tarea.

### Retirada, desinstalación de Software

Uno de los resultados de la fase de Desarrollo es la documentación de Producto:

* Documentación de Diseño Mecánico.
* Documentación de Diseño Software.
* Documentación de Diseño Hardware.
* Esquema.
* Listas de Materiales.
* Código fuente.
* Manuales Técnicos.
* Manuales de Usuario.
* Guías de Instalación Software.
* …

En la Guía de Instalación Software también se aborda el procedimiento correcto de desinstalación.

## Parte 6: COTS

### Plan de Garantía y conformidad para COTS

La Dirección Técnica es la que define los módulos software a utilizar en un producto. La adquisición de los módulos COTS se realiza de acuerdo al documento ***P07007 Procedimiento General de Compras***.

En este caso el origen de la necesidad de compra es la introducción de un nuevo producto (otros posibles orígenes son: estructura, fábrica, producción, reparaciones, contratos…).

Independientemente del origen de la necesidad de compra, nuestro procedimiento define una serie de fases para este proceso:

* Solicitud de compra.
* Petición de ofertas procesadas por compras.
* Evaluación.
* Propuesta de adjudicación.
* Mesa de compras.
* Formalización de la compra.
* Gestión del pedido.
* Recepción del producto o servicio.
* Facturación.

El Plan de Calidad de un Desarrollo incluye tanto a los módulos software desarrollados como a los módulos sofwate COTS.

Uno de los resultados de la fase de Desarrollo es la documentación de Producto:

* Documentación de Diseño Mecánico.
* Documentación de Diseño Software.
* Documentación de Diseño Hardware.
* Esquema.
* Listas de Materiales.
* Código fuente.
* Manuales Técnicos.
* Manuales de Usuario.
* Guías de Instalación Software.
* …

En la guía de instalación software también se describiren detalladamente los módulos COTS: entorno operativo, versión, configuración, instalación…

## Parte 7: Garantías

### Garantía de herramientas

Dentro de las actividades de planificación de un proyecto se elabora el Plan de Desarrollo.

El responsable de la edición de dicho documento es el Jefe de Proyecto. Se elabora a partir de la documentación existente en la carpeta de Especificación:

* Especificación de Requisitos Software.
* Lista de Casos de Prueba.

Este Plan de Desarrollo debe contener información relativa a las herramientas a utilizar en dicho desarrollo.

En el documento ***JIN12001.P07005D.Plan de Diseño y Desarrollo*** aparecen las herramientas que aplican en este desarrollo.

### Asignación de SWAL y monitorización

El documento, ***JIN12001.PSSA,*** está en la carpeta de Diseño. Es la fase de Evaluación Preliminar de la Seguridad del Sistema. Incluye:

* Descripción de la Arquitectura del Sistema. En concreto una descripción de la arquitectura hardware, una descripción de la arquitectura software y la relación entre los módulos hardware y software.
* Análisis Funcional de Amenazas (FHA). El objeto de este análisis es la identificación del SWAL. La secuencia de tareas a realizar son las siguientes:
  + Identificación de las funciones del sistema.
  + Identificación de las amenazas potenciales.
  + Identificación de los Efectos o Consecuencias de las Amenazas.
  + Probabilidad.
  + Severidad.
  + Descripción de las medidas de mitigación.
  + Identificación del SWAL
* Carpeta de Seguridad del Software (SSF). Este apartado sigue la estructura propuesta en la ED-153. Contiene una lista de evidencias o referencias a las mismas.

Teniendo en cuenta que este documento se elabora en la actividad de diseño se entiende que algunos de los capítulos de la SSF todavía no presenten la evidencia correspondiente.

En la carpeta de Resultados, está el presente documento ***JIN12001.SSA***. Es la fase de Evaluación de la Seguridad del Sistema. Teniendo en cuenta que este documento se prepara con el sistema ya desarrollado, se entiende que la carpeta SSF ya puede hacer referencia a las evidencias correspondientes.

En concreto, incluye:

* Descripción de la Arquitectura del Sistema. En concreto una descripción de la arquitectura hardware, una descripción de la arquitectura software y la relación entre los módulos hardware y software.
* Análisis Funcional de Amenazas (FHA). El objeto de este análisis es la identificación del SWAL. La secuencia de tareas a realizar son las siguientes:
  + Identificación de las funciones del sistema.
  + Identificación de las amenazas potenciales.
  + Identificación de los Efectos o Consecuencias de las Amenazas.
  + Probabilidad.
  + Severidad.
  + Descripción de las medidas de mitigación.
  + Identificación del SWAL
* Carpeta de Seguridad del Software (SSF). Este apartado sigue la estructura propuesta en la ED-153. Contiene una lista de evidencias o referencias a las mismas.

### Auditorias y revisiones

El documento ***P07005 Procedimiento para el Control del Diseño y Desarrollo*** define cómo se realizan las auditorías y revisiones.

El documento ***JIN12001.P07005A.Revision de Datos de Partida*** se elabora examinando los requisitos y casos de prueba. Los objetivos de esta revisión son:

* Detectar los requisitos y posibles carencias de los mismos en la documentación de entrada que impidan dar continuidad al proceso de desarrollo.
* Revisar los requisitos funcionales y no funcionales, de producto, de calidad, de coste, de plazo, protección industrial e intelectual, etc…
* En caso de existir carencias deberán ser resueltas antes de proceder a la fase planificación.

El documento ***JIN1201.P07005E. Acta Revision Diseño*** se elabora examinando la documentación de diseño. Los objetivos de esta revisión son:

* La arquitectura diseñada tiene que describir completamente el sistema.
* Deben estar contemplados todos los requisitos.
* Tiene que desarrollarse una matriz de trazabilidad.
* El diseño tiene que ser verificable.
* El diseño tiene que contemplar las consideraciones de seguridad.

En la fase de Planificación, se elabora el Plan de Desarrollo. Dentro de dicho plan aparecen recogidos los planes de verificación y validación.

Las actividades de verificación se van a describir con más detalle en un apartado posterior (5.7.12).

Como resultado de la verificación, se elabora el correspondiente “Informe de verificación”. El documento ***JIN12001.P07005Z.Informe de Pruebas de Verificacion*** contiene dicho informe.

Durante todo el proceso descrito, se ejecutan los correspondientes hitos de Revisión y Verificación que se hayan establecido en el Plan de Revisiones / Verificaciones establecido en la fase de Planificación. Cada hito de Revisión y Verificación debe dejar un registro en forma de Acta de Verificación. El documento ***JIN12001.P07005F.Acta Verificacion*** contiene dicha acta.

Las actividades de validación se van a describir con más detalle en un apartado posterior (5.7.12).

Como resultado de la validación, se elabora el correspondiente “Informe de validación”. El documento ***JIN12001.P07005Z.Informe de Pruebas de Validacion*** contiene dicho informe.

Durante todo el proceso descrito, se ejecutan los correspondientes hitos de Validación que se hayan establecido en el Plan de Validaciones establecido en la fase de Planificación. Cada hito de Validación debe dejar un registro en forma de Acta de Validación. El documento ***JIN12001.P07005G.Acta Validacion***contiene dicha acta.

Por otra parte, el documento ***P08002 Auditorías internas de Calidad y Medio Ambiente*** tiene como objeto establecer la sistemática para llevar a cabo auditorías internas del Sistema de Gestión Integrado (calidad, medio ambiente, prevención de riesgos laborales, investigación, desarrollo e innovación…).

Este procedimiento tiene un capítulo dedicado a las auditorías de producto. Algunas de sus características más relevantes son:

* Es una evaluación independiente de la calidad del producto para determinar su aptitud de uso y su conformidad con las especificaciones.
* Las auditorías del producto sólo se realizarán bajo petición del cliente o por la Producción de I+D o de la Dirección Productiva (donde se ejecute el contrato).
* Se realizarán después de que se hayan completado las inspecciones. Los objetivos de una auditoría de producto son:
  + Estimación del nivel de calidad que es entregado a los clientes, reflejando los puntos de vista del usuario.
  + Evaluación de la efectividad de las decisiones de inspección al determinar la conformidad con las especificaciones.
  + Suministro de información útil para mejorar la calidad del producto y la efectividad de la inspección.
  + Suministro de un aseguramiento adicional más allá de las actividades de inspección.
* Idealmente, la auditoría del producto deberá comparar el resultado real en el servicio con las necesidades del usuario.
* Estas auditorías no están normalmente incluidas en el Plan de Contrato/Calidad.
* 5.4.6. El auditor, miembro del Departamento del SGI, anotará el resultado de la evaluación en el registro de formato P08002E “Informe de evaluación. Calidad del producto”.
* La auditoría se realizará tomando muestras del producto, siendo el tamaño de la muestra el que se determine en cada caso. Se ensayará el producto buscando la presencia o ausencia de defectos o fallos.
* Los defectos se clasificarán según su gravedad en: críticos, mayores y menores.
  + Defectos críticos: Son los que, en condiciones normales de uso, estén expuestos a causar lesiones personales o hagan al producto no apto para el servicio.
  + Defectos mayores: Son los que causan un fallo operativo que no pueda ser corregido “in situ”, provoquen un incremento del mantenimiento o reduzca la vida, causen un incremento de trabajos de instalación, o defectos importantes de aspecto o de acabado.
  + Defectos menores: Tengan un rendimiento por debajo de la norma, causen un pequeño incremento de los trabajos de instalación o defectos de aspecto o de acabado.
* Si se detecta/n defectos/s de cualquier tipo, se abrirá una No Conformidad y será objeto de análisis según el procedimiento P08004 “Control del producto no conforme. Reclamaciones. No conformidades. Acciones correctivas y preventivas”.

### Formación

El documento ***P06001 Formacion y Toma de Conciencia*** es el procedimiento general sobre formación. El objeto de este procedimiento es definir la sistemática utilizada por la Compañía para asegurar que su personal sea competente y posea la educación, formación, información, habilidades y experiencia apropiada para su puesto de trabajo y esté sensibilizado con aspectos relacionados con la seguridad y salud en el trabajo.

El documento ***P07023 Industrialización*** es el procedimiento que tiene como objeto definir la sistemática a seguir en DF NÚCLEO para la Industrialización de sus diseños y productos.

Este documento tiene un capítulo dedicado a la formación. Se explica que una vez finalizado el producto y toda su documentación asociada es necesaria la formación de las partes interesadas. La formación correrá a cargo de la Dirección Técnica, aunque alguna vez sea precisa la colaboración de Fábrica en determinados aspectos.

La formación puede ser interna o externa. La interna se refiere a la impartida por y para trabajadores de DF NÚCLEO.

Puede ocurrir que se precise impartir formación por trabajadores de DF NUCLEO a terceros (fabricantes, instaladores, subcontratistas de puesta en servicio y/o Mantenimiento, etc.).

Todo lo relativo a la formación interna, será gestionado a través del área de formación de la Dirección de Gestión del Talento, RR. HH y PRL, mientras que la formación a terceros será gestionada por el Área de Puesta en Servicio.

### Requisitos SOFTWARE

El documento ***JIN12001.P07005V.Especificacion de Requisitos Software*** (como su nombre indica) define la Especificación de Requisitos Software del producto.

Este documento está redactado siguiendo la instrucción técnica ***P07005AC Guía de Elaboración de Especificacion de Requisitos Software con UML-EA.***

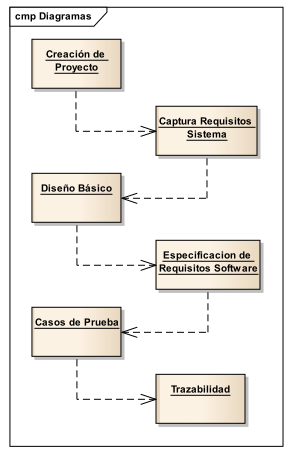
### Matriz de trazabilidad

El documento ***JIN12001.P07005V.Especificacion de Requisitos Software*** (citado en el apartado anterior) define la Especificación de Requisitos Software del producto.

En este documento, además de los requisitos software, se definen los casos de prueba y la matriz de trazabilidad entre requisitos y Casos de Prueba.

Dicho documento está redactado siguiendo la instrucción técnica ***P07005AC Guía de Elaboración de Especificacion de Requisitos Software con UML-EA.***

El proceso general para la elaboración de una especificación de requisitos software, utilizando el lenguaje UML y la herramienta EA, se presenta en el siguiente diagrama:



Por otra parte, el documento ***JIN12001. P07005U. Documento de Diseño Detalle*** utiliza también el lenguaje UML para definir la estructura de diseño. En este documento de diseño, se han considerado dos diagramas de los que dispone dicho lenguaje:

* Diagrama de Componentes (software), para modelar la estructura.
* Diagrama de Casos de uso, para modelar la funcionalidad.

Ambos diagramas se han desarrollado sobre la herramienta Enterprise Architect.

En este documento se define una matriz de trazabilidad entre el diseño básico y los requisitos, que se ha establecido en la herramienta UML entre Requisitos y Casos de Uso que modelan la funcionalidad exigida.

### Funciones no deseadas

Uno de los resultados de la fase de Desarrollo es la documentación de Producto:

* Documentación de Diseño Mecánico.
* Documentación de Diseño Software.
* Documentación de Diseño Hardware.
* Esquema.
* Listas de Materiales.
* Código fuente.
* Manuales Técnicos.
* Manuales de Usuario.
* Guías de Instalación Software.
* …

Para asegurar que el software se está ejecutando en el entorno de operación esplecificado, en la Guía de Instalación Software se describe con detalle cada uno de los procesos de instalación y configuración del entorno de operación.

### Satisfacción de requisitos

La satisfacción de los requisitos es un proceso que se va realizando a lo largo de todo el ciclo de vida del sistema.

En la primera carpeta (especificación), el documento ***JIN12001.P07005X.Lista de Casos de Prueba*** contiene un resumen de requisitos, un resumen de casos de prueba y la matriz de trazabilidad.

El documento ***JIN12001.P07005A.Revision de Datos de Partida*** se elabora examinando los requisitos y casos de prueba. Los objetivos de esta revisión son:

* Detectar los requisitos y posibles carencias de los mismos en la documentación de entrada que impidan dar continuidad al proceso de desarrollo.
* Revisar los requisitos funcionales y no funcionales, de producto, de calidad, de coste, de plazo, protección industrial e intelectual, etc…
* En caso de existir carencias deberán ser resueltas antes de proceder a la fase planificación.

En la tercera carpeta (diseño) se incluyen los documentos. ***JIN12001. P07005U. Documento de Diseño Basico, JIN12001. P07005U. Documento de Diseño Detalle*** y **JIN12001.PSSA**.

Finalizada la fase de diseño, el documento ***JIN1201.P07005E. Acta Revision Diseño*** se elabora examinando la documentación de diseño. Los objetivos de esta revisión son:

* La arquitectura diseñada tiene que describir completamente el sistema.
* Deben estar contemplados todos los requisitos.
* Tiene que desarrollarse una matriz de trazabilidad.
* El diseño tiene que ser verificable.
* El diseño tiene que contemplar las consideraciones de seguridad.

En la fase de Planificación, se elabora el Plan de Desarrollo. Dentro de dicho plan aparecen recogidos los planes de verificación y validación.

Las actividades de verificación se van a describir con más detalle en un apartado posterior (5.7.12).

Como resultado de la verificación, se elabora el correspondiente “Informe de verificación”. El documento ***JIN12001.P07005Z.Informe de Pruebas de Verificacion*** contiene dicho informe.

Durante todo el proceso descrito, se ejecutan los correspondientes hitos de Revisión y Verificación que se hayan establecido en el Plan de Revisiones / Verificaciones establecido en la fase de Planificación. Cada hito de Revisión y Verificación debe dejar un registro en forma de Acta de Verificación. El documento ***JIN12001.P07005F.Acta Verificacion*** contiene dicha acta.

Las actividades de validación se van a describir con más detalle en un apartado posterior (5.7.12).

Como resultado de la validación, se elabora el correspondiente “Informe de validación”. El documento ***JIN12001.P07005Z.Informe de Pruebas de Validacion*** contiene dicho informe.

Durante todo el proceso descrito, se ejecutan los correspondientes hitos de Validación que se hayan establecido en el Plan de Validaciones establecido en la fase de Planificación. Cada hito de Validación debe dejar un registro en forma de Acta de Validación. El documento ***JIN12001.P07005G.Acta Validacion***contiene dicha acta.

### Gestión de la configuración

En el procedimiento ***P07005 Procedimiento para el Control del Diseño y Desarrollo*** se dice que, como resumen de la fase de desarrollo, se elaborará un documento de control de configuración, que incluya una parte para la gestión de cambios que refleje en el fututo las modificaciones introducidas en cada una de las versiones o revisiones del sistema.

Como resultado de la actividad de Pruebas y Verificación, se genera un conjunto revisado de los resultados de la fase de Desarrollo, acompañada por el correspondiente documento de control de configuración en el que se establecerá:

* Las modificaciones efectuadas respecto a la versión de entrada en la fase.
* Los componentes o módulos afectados por dichas modificaciones.

El documento ***JIN12001.P07005H.Control de Configuracion*** contiene dicho informe.

### Plan de desarrollo del Software

El documento JIN12001.P07005D.Plan de Diseño y Desarrollo contiene el Plan de Desarrollo.

Este Plan de Desarrollo contiene información relativa a:

* Modelo de Ciclo de Vida del Proyecto.
* Métodos, Técnicas y Herramientas.
* Planificación de Detalle de Hitos y Tareas.
* Cuadro de Responsabilidades.
* Planes de Apoyo…

La elaboración de dicho Plan de Desarrollo está recogida en el procedimiento ***P07005 Procedimiento para el Control del Diseño y Desarrollo***.

### Mantenimiento

Las actividades de mantenimiento están contempladas en el ciclo de vida de un desarrollo. Los procedimientos ***P07005 Control del Diseño y Desarrollo*** y ***P07023 Industrialización*** abordan esta fase.

Se comenta que, si durante el ciclo de vida, se detectan fallos en el producto, éstos serán analizados por el respectivo Jefe de Producto, quien decidirá si el fallo afecta a la industrialización, en cuyo caso será dicho departamento el que solucione el problema generando cuantos documentos, listas y/o manuales hiciesen falta para finalizar la incidencia.

Si el Jefe de Proyecto tras analizar el mal funcionamiento del producto decide que es necesaria la modificación del mismo será el departamento de Desarrollo de la Dirección Técnica quien deba modificar el producto. En este caso puede ocurrir que el cambio suponga un coste extra no planificado, en cuyo caso la Dirección Técnica procederá a presentarlo al comité de Innovación siguiendo lo descrito en el procedimiento ***P07008 “Investigación, innovación y Vigilancia Tecnológica”***.

Las posibles mejoras o cambios del producto, serán analizadas en el Comité de Innovación y una vez aprobadas y desarrolladas serán industrializadas según lo expuesto en este procedimiento.

Las funciones de apoyo que la Dirección Técnica realiza a lo largo de la vida del producto son:

* Apoyo a Fábrica.
* Ayuda a reparaciones.
* Problemas de mantenibilidad.
* Evolución del producto.
* Validación de nuevos componentes.

### Verificación

El documento ***P07005 Procedimiento para el Control del Diseño y Desarrollo*** define cómo se realizan las actividades de verificación y validación.

En la fase de Planificación, se elabora el Plan de Desarrollo. Dentro de dicho plan aparecen recogidos los planes de verificación y validación.

**VERIFICACIÓN**

El propósito de la fase de pruebas y verificación es integrar los diferentes componentes software entre sí y con otros componentes, tales como hardware y/o software comercial, para producir un sistema completo que satisfaga las expectativas expresadas en los requisitos del sistema.

Bajo la responsabilidad del Jefe de Proyecto y el grupo de Desarrollo, se verifica, si los componentes o subsistemas interactúan correctamente a través de sus interfaces, tanto internas como externas, si cubren la funcionalidad establecida, y se ajustan a los requisitos especificados en las verificaciones correspondientes.

Esta fase, se ejecuta mediante una estrategia de regresión: Ejecutando los ciclos de pruebas, tantas veces como sea necesario hasta conseguir un sistema libre de fallos.

Como resultado de esta actividad, se genera un conjunto revisado de los resultados de la fase de Desarrollo, acompañada por el correspondiente documento de control de configuración en el que se establecerá:

* Las modificaciones efectuadas respecto a la versión de entrada en la fase.
* Los componentes o módulos afectados por dichas modificaciones.

Como resultado de la verificación, se elabora el correspondiente “Informe de verificación”. El documento ***JIN12001.P07005Z.Informe de Pruebas de Verificacion*** contiene dicho informe.

Durante todo el proceso descrito, se ejecutan los correspondientes hitos de Revisión y Verificación que se hayan establecido en el Plan de Revisiones / Verificaciones establecido en la fase de Planificación. Cada hito de Revisión y Verificación debe dejar un registro en forma de Acta de Verificación. El documento ***JIN12001.P07005F.Acta Verificacion*** contiene dicha acta.

**VALIDACION**

La fase de Validación tiene por objeto garantizar que el producto es adecuado al fin para el que se ha desarrollado.

Se entrará en la fase de validación una vez que el Jefe de Proyecto lo decida, valorando en particular la situación de las actividades de verificación.

La modalidad de validación depende de cada producto y de su contexto, y debe definirse en la Planificación del proyecto. La realización de las actividades de validación deberá hacerse conforme a las directrices de dicha Planificación.

Los criterios de validación se establecen en la fase de análisis (en el documento de casos de prueba) y se desarrollan en la fase de desarrollo a través del documento de protocolo de pruebas.

La responsabilidad de la validación de un producto es del grupo de validación, que se define en el establecimiento del Plan de Desarrollo (y sus posteriores revisiones).

Las actividades de validación, se realizan también con una estrategia de regresión, ejecutando diferentes ciclos de validación, hasta que el producto supere los criterios establecidos.

Como resultado de la validación, se elabora el correspondiente “Informe de validación”. El documento ***JIN12001.P07005Z.Informe de Pruebas de Validacion*** contiene dicho informe.

Durante todo el proceso descrito, se ejecutan los correspondientes hitos de Validación que se hayan establecido en el Plan de Validaciones establecido en la fase de Planificación. Cada hito de Validación debe dejar un registro en forma de Acta de Validación. El documento ***JIN12001.P07005G.Acta Validacion***contiene dicha acta.

### Calidad

El documento ***JIN12001.P07005B.Plan de Calidad*** contiene el Plan de Calidad de Desarrollo.

La elaboración de dicho Plan de Calidad está recogida en el procedimiento ***P07005 Procedimiento para el Control del Diseño y Desarrollo***.

En la fase de Planificación, se elaboran tanto el Plan de Desarrollo como el Plan de Calidad.

### Garantía de que el SW es aceptablemente seguro

En el capítulo 3 de este documento se ha descrito el Proceso de Evaluación de la Seguridad. La garantía de que el software es aceptablemente seguro radica en la verificación de que se han seguido todas las acciones allí descritas.

En este documento se han descrito las evidencias completas de nuestro sistema de aseguramiento de la seguridad software (SSAS).

# TRAZABILIDAD DE REQUISITOS

Este apartado es un resumen del presente documento. El objetivo es demostrar cómo el ULISES V5000I sigue el estándar de EUROCAE ED-153 “Guidelines for ANS Software Safety Assurance” en cuanto al aseguramiento de la seguridad del software.

En el apartado 5.4 de este documento se listan los requisitos de seguridad. Volviendo ahora sobre ellos cabe comentar lo siguiente:

* En el apartado 4 (Análisis Funcional de Amenazas, FHA) se asigna un SWAL 4 que coincide con el nivel exigido como requisito.
* En el apartado 5 (Carpeta de Seguridad Software, SSF) se sigue la estructura de la norma ED-153 para facilitar el seguimiento de las evidencias. La siguiente tabla resume dicho capítulo.

Las 2 primeras columnas hacen referencia a los requisitos de la norma ED-153.

Las 2 últimas columnas hacen referencia a las evidencias del ULISES V5000I. Hay evidencias que se generan en las primeras fases del desarrollo (definición y diseño) y están disponibles en el PSSA (Preliminary System Safety Assesment). Otras evidencias se generan en fases posteriores del ciclo de vida del sistema (implementación, mantenimiento, retirada) y, por lo tanto, no estarán completas hasta el SSA (System Safety Assesment).

|  |  |  |  |
| --- | --- | --- | --- |
| Parte | Ítem | Evidencia | |
| PSSA | SSA |
| Parte1: Entorno | Descripción del Sistema  (Ref. ED-153: 3.1.1, 3.1.2) | * (5.1.1) |  |
| Entorno operacional  (Ref. ED-153: 3.1.1, 3.1.2) | * (5.1.2) |  |
| Listado de herramientas  (Ref. ED-153: 4.3.9-12, 4.4.1, 5.1.x, 5.2.x, 5.4.1, 5.4.2, 5.8.1, 7.2.8, 7.2.10) | * (5.1.3) |  |
| Parte 2: Contexto de la garantía de la seguridad sw | Regulación aplicable  (Ref. ED-153: 3.1.3, 3.1.4) | * (5.2.1) |  |
| Estándares aplicables  (Ref. ED-153: 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1) | * (5.2.2) |  |
| Análisis y Mitigación de Riesgos  (Ref. ED-153: 3.0.9, 3.0.12, 3.0.17, 3.1.5, 3.3.x, 3.6.x) | * (5.2.3) | * (5.2.3) |
| Parte 3: Proceso de Garantía de la seguridad sw | Plan de Gestión de la Seguridad  (Ref. ED-153: 3.2.x, 3.5.x) | * (5.3.1) |  |
| Revisión del Plan  (Ref. ED-153: 3.2.x, 3.4.x, 3.5.x, 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1) | * (5.3.2) | * (5.3.2) |
| Listado de documentación  (Ref. ED-153: 3.2.x, 3.5.x, 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1) | * (5.3.3) |  |
| Parte 4: Requisitos Safety | Listado de Requisitos Safety  (Ref. ED-153: 3.0.2, 3.1.5, 3.3.x, 3.6.x, 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) | * (5.4.1) |  |
| Parte 5: Modificaciones de Software | Gestión de cambios  (Ref. ED-153: 5.2.x, 7.2.8, 7.2.10) |  | * (5.5.1) |
| Gestión de incidencias  (Ref. ED-153: 5.2.x, 5.8.x, 7.2.8, 7.2.9, 7.2.10) | * (5.5.2) |  |
| Parte 5: Modificaciones de Software | Retirada, desinstalación de Software  (Ref. ED-153: 4.4.x, 4.5.2, 4.5.3) |  | * (5.5.3) |
| Parte 6: COTS | Plan de Garantía para COTS  (Ref. ED-153: 3.0.3, 4.1.7, 5.2.x, 5.8.x, 7.2.1, 7.2.8, 7.2.9, 7.2.10) |  | * (5.6.1) |
| Informe de Conformidad para COTS  (Ref. ED-153: 3.0.2, 3.0.3, 3.0.13, 3.4.x, 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) |  | * (5.6.1) |
| Parte 7: Garantías | Garantía de herramientas  (Ref. ED-153: 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1) | * (5.7.1) |  |
| Asignación de SWAL y monitorización  (Ref. ED-153: 3.0.5, 3.0.8, 3.0.11, 3.0.14, 3.0.15, 3.3.x, 3.1.5, 3.6.x, 4.1.7, 4.3.1, 4.3.2, 4.3.4, 4.3.5, 4.3.6, 4.3.9-12, 4.3.13, 4.3.14, 4.3.15, 4.4.1, 4.4.5, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1; 6.2.9; 6.2.12, 7.2.1, 7.2.4, 7.2.6) | * (5.7.2) | * (5.7.2) |
| Parte 7: Garantías | Auditorias y revisiones  (Ref. ED-153: 3.0.9, 3.0.12, 3.0.17, 5.4.3-13, 5.7.2) | * (5.7.3) | * (5.7.3) |
| Formación  (Ref. ED-153: 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1) | * (5.7.4) |  |
| Requisitos correctos y completos  (Ref. 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, 5.4.3-13, 5.7.2, 7.2.4, 7.2.6) | * (5.7.5) |  |
| Matriz de trazabilidad  (Ref. ED-153: 3.0.3, 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, 5.4.3-13, 5.7.2, 7.2.4, 7.2.6) | * (5.7.6) |  |
| Funciones no deseadas  (Ref. ED-153: 3.0.4, 3.1.5, 3.3.x, 3.6.x, 4.4.x, 4.5.2, 4.5.3, 5.4.3-13, 5.7.2, 5.8.x, 7.2.9) |  | * (5.7.7) |
| Parte 7: Garantías | Satisfacción de requisitos  (Ref. ED-153: 3.0.6, 3.4.x, 4.3.1, 4.3.2, 4.3.4, 4.3.5, 4.3.6, 4.3.9-15, 4.4.x, 4.5.2, 4.5.3, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.4.3-13, 5.7.2, 5.8.1, 7.2.4, 7.2.6) | * (5.7.8) |  |
| Gestión de la configuración  (Ref. ED-153: 3.0.7, 4.3.9-12, 4.4.1, 5.1.x, 5.2.x, 5.4.1, 5.4.2, 5.8.1, 7.2.8, 7.2.10) |  | * (5.7.9) |
| Plan de desarrollo del SW  (Ref. ED-153: 4.3.9-12, 4.4.1, 5.1.x, 5.2.1, 5.4.1, 5.4.2, 5.8.1) | * (5.7.10) |  |
| Mantenimiento  (Ref. ED-153: 4.4.x, 4.5.2, 4.5.3) | * (5.7.11) |  |
| Verificación  (Ref. ED-153: 3.0.10, 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.x, 4.5.2, 4.5.3, 5.4.3-13, 5.7.2, 7.2.4, 7.2.6) |  | * (5.7.12) |
| Parte 7: Garantías | Calidad  (Ref. ED-153: 5.4.3-13, 5.7.2) | * (5.7.13) |  |
| Garantía de que sw es seguro  (Ref. ED-153: 3.0.1, 3.0.9, 3.0.12, 3.0.17) | * (5.7.14) | * (5.7.14) |

1. Evidencias para el cumplimiento de SWAL