| **Software Architecture & Design Verification Report** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Nombre del documento** | SAS\_CTV.docx  SAS\_Global.docx  SAS\_CTV.xlxs  ArquitecturaSW\_CTV.pptx  {{BBBB}} | **Código y versión** | {{FFFF}} | | |
| **Nombre del verificador** | {{AAAA}} | **Fecha** | {{DATE}} | **No revisión** | 1 |

| **Reqs.** | **Criterio de aceptación** | **Conforme/**  **No Conforme** | **Descripción de la Evidencia/Deficiencia** | **¿Es critica la desviación?** |
| --- | --- | --- | --- | --- |
| 7.3.4.42 | Después de que se hayan establecido las Especificaciones de Arquitectura, Interfaz y Diseño del Software, la verificación debe recoger: | | | |
| a) | La coherencia interna de las Especificaciones de Arquitectura | Conforme | Hay evidencia de revisiones (MinRev\_SAS CTV) de la Especificación de Arquitectura del Software para corroborar la coherencia interna del componente “{{BBBB}}” y sus documentos SIS\_{{BBBB}}, SIS\_{{BBBB}}\_def, SIS\_{{BBBB}}\_cfg y SDS\_{{BBBB}} | -- |
| b) | La adecuación de las Especificaciones de Arquitectura para satisfacer la Especificación de Requisitos del Software en lo que se refiere a la coherencia y compleción; | Conforme | La adecuación de las Especificaciones de Arquitectura del Software del componente “{{BBBB}}” satisface la Especificación de Requisitos del Software “SRS\_CTV Documento de Requerimientos de Software” de la sección “{{EEEE}}” en coherencia y compleción. | -- |
| c) | Que la Especificación de la Arquitectura del Software cumple con los requisitos 7.3.4.1 al 7.3.4.14, 5.3.2.7 al 5.3.2.10 y desde el 6.5.4.14 hasta el 6.5.4.16. | | | |
| 7.3.4.1 | Se debe redactar una Especificación de la Arquitectura del Software bajo la responsabilidad del Diseñador, tomando como base la Especificación de Requisitos del Software. | Conforme | La Especificación de la Arquitectura de Software (SAS\_CTV.docx, ArquitecturaSW\_CTV.pptx, SAS\_Global.docx y SAS\_CTV.xlxs) fue escrito bajo la responsabilidad del diseñador {{CCCC}} acorde a la sección “Anexo A: Asignación de roles para el desarrollo del Software” del documento M-S-Rd-001 Software Quality Assurance Plan.  Para la redacción de la Especificación de la Arquitectura de Software se tomó como base  a) la Especificación de Requisitos del Software (“SRS\_CTV Documento de Requerimientos de Software”) | -- |
| 7.3.4.2 | La arquitectura del software propuesta debe establecerse y detallarse en la Especificación de la Arquitectura del Software. | Conforme | La propuesta de la arquitectura de software está plasmada en los documentos SAS\_CTV.docx, ArquitecturaSW\_CTV.pptx, SAS\_Global.docx y SAS\_CTV.xlxs | -- |
| 7.3.4.3 | La Especificación de la Arquitectura del Software debe recoger la viabilidad de realización de la Especificación de Requisitos del Software al nivel requerido de integridad de seguridad del software.  NOTA: La Arquitectura del Software debería minimizar el tamaño y la complejidad de la parte relativa a la seguridad de la aplicación. | Conforme | La arquitectura establece la realización y la viabilidad de los requisitos de software y lo plasma en los documentos SAS\_CTV.docx, ArquitecturaSW\_CTV.pptx, SAS\_Global.docx y SAS\_CTV.xlxs  Así mismo, descompone los requisitos de software de la sección “{{EEEE}}” en el componente “{{BBBB}}” y estos a su vez en interfaces, disminuyendo así su complejidad y tamaño. | -- |
| 7.3.4.4 | La Especificación de la Arquitectura del Software debe identificar, analizar y detallar la importancia de las interacciones hardware/software. | Conforme | Las interacciones hardware/software están identificadas en las secciones “Vista Lógica” y “Factorización en componentes”. | -- |
| 7.3.4.5 | La Especificación de la Arquitectura del Software debe identificar todos los componentes software y debe determinar para estos componentes:   1. si estos componentes son nuevos o ya existían 2. si estos componentes se han validado de forma previa y de ser así, sus condiciones de validación 3. el nivel de integridad de seguridad del software del componente. | Conforme | a) Puede ser encontrado en SAS\_CTV.xlsx en la hoja “SAS -- Componentes” para el componente “{{BBBB}}” en la columna “Preexistente”.  b) Según evidencia del inciso a) al ser los componentes nuevos y por tanto no se han validado.  c) El componente “{{BBBB}}” tiene un nivel de integridad de seguridad “{{OOOO}}” y puede ser encontrado en SAS\_CTV.xlsx en la hoja “SAS -- Componentes” en la columna “SIL”. | -- |
| 7.3.4.6 | Los componentes software deben:  a) cubrir un subconjunto definido de requisitos del software,  b) estar identificados de manera clara y constituir versiones independientes dentro del sistema de gestión de la configuración. | Conforme | a) Dada la matriz de trazabilidad “Pr-QS-008 F1” se determinan los requisitos que competen al componente “{{BBBB}}” a través de la columna “Documento evidencia arquitectura/diseño”  Ver tabla de Suposiciones.  b) En el documento “SAS\_CTV” en la hoja “SAS -- Componentes” en la columna “SHA1” el componente de software “{{BBBB}}” contiene un SHA1 único que representa su versión. | -- |
| 7.3.4.7 | El uso de software preexistente debe quedar sujeto a las siguientes restricciones.  NOTA: Se pueden utilizar pruebas estadísticas en la estrategia de validación del software preexistente. | | | |
| a) | Para todos los niveles de integridad de seguridad del software se debe identificar y documentar claramente la siguiente información:  – los requisitos que el software preexistente está destinado a satisfacer;  – las hipótesis relativas al entorno del software preexistente;  – las interfaces con otras partes del software. | Conforme | En el documento SAS\_CTV.xlsx en la hoja “SAS -- Componentes” en la columna “Preexistencia” se indica que el componente de software “{{BBBB}}” es no preexistente, por lo que el requisito no aplica. | -- |
| b) | Para todos los niveles de integridad de seguridad del software se debe incluir el software preexistente en el proceso de validación del software completo. | Conforme | En el documento SAS\_CTV.xlsx en la hoja “SAS -- Componentes” en la columna “Preexistencia” se indica que el componente de software “{{BBBB}}” es no preexistente, por lo que el requisito no aplica. | -- |
| c) | Para los niveles de integridad de seguridad del software SIL 3 o SIL 4, se deben tomar las siguientes precauciones:  – se debe realizar un análisis de los posibles fallos del software preexistente y sus consecuencias en el software completo  – se debe definir una estrategia para detectar fallos del software preexistente y para proteger al sistema de estos fallos  – los procesos de verificación y validación deben garantizar   1. que el software preexistente cumple los requisitos asignados 2. que se detectan los fallos del software preexistente y que el sistema en el que el software preexistente está integrado está protegido de esos fallos. 3. que se cumplen las hipótesis relativas al entorno del software preexistente. | Conforme | En el documento SAS\_CTV.xlsx en la hoja “SAS -- Componentes” en la columna “Preexistencia” se indica que el componente de software “{{BBBB}}” es no preexistente, por lo que el requisito no aplica. | -- |
| d) | El software preexistente debe ir acompañado de una descripción (es decir, las funciones, las restricciones y las pruebas) lo suficientemente precisa (por ejemplo, que se limite a las funciones utilizadas) y completa. La descripción debe incluir las restricciones de hardware y/o software que el integrador debe conocer y tener en cuenta durante la aplicación. Es el medio en particular utilizado para informar al integrador de para qué se diseñó el software, de sus propiedades, de su comportamiento y de sus características. | Conforme | En el documento SAS\_CTV.xlsx en la hoja “SAS -- Componentes” en la columna “Preexistencia” se indica que el componente de software “{{BBBB}}” es no preexistente, por lo que el requisito no aplica. | -- |
| 7.3.4.8 | En la medida de lo posible, se prefiere el uso de componentes software verificados existentes, desarrollados conforme a esta norma europea en lo que se refiere al diseño. | Conforme | Los componentes de software existentes (SCIOPTA) que son usados, han sido desarrollados bajo la norma europea EN50128 y estos cuentan con una precertificación en la norma.  Ver tabla de suposiciones. | -- |
| 7.3.4.9 | Cuando el software está constituido por componentes con diferentes niveles de integridad de seguridad del software, entonces, se debe tratar a todos los componentes software como si tuvieran el más alto de estos niveles a menos que se disponga de pruebas de independencia entre los componentes con un nivel de integridad de seguridad del software más alto y los componentes con un nivel de integridad de seguridad del software más bajo. Dichas pruebas deben quedar registradas en la Especificación de la Arquitectura del Software. | Conforme | El componente “{{BBBB}}” tienen el nivel de integridad de seguridad “{{OOOO}}”, según la hoja “SAS – Componentes” del documento SAS\_CTV.xlxs,  {{CSIL}} | -- |
| 7.3.4.10 | La Especificación de la Arquitectura del Software debe describir la estrategia para el desarrollo del software dentro del alcance requerido por el nivel de integridad de seguridad del software. La Especificación de la Arquitectura del Software debe expresarse y estructurarse de forma que sea:  a) completa, coherente, clara, precisa, inequívoca, verificable, que se pueda someter a ensayo, que se pueda mantener y que sea realizable;  b) trazable hasta la Especificación de Requisitos del Software. | Conforme | Se describen las estrategias para el desarrollo de software en la sección “Seguridad Operacional (Safety)” del documento SAS\_Global.docx  a) Según juicio experto De acuerdo con la evidencia de revision (MinRev\_SAS CTV) de la Especificación de Arquitectura del Software es completa, coherente, clara, precisa, inequívoca, verificable, se puede someter a ensayos, se puede mantener y que sea realizable.  b) A través del documento Pr-QS-008 F1 se trazan los requisitos al componente “{{BBBB}}” | -- |
| 7.3.4.11 | La Especificación de la Arquitectura del Software debe incluir las medidas para gestionar los errores con el fin de alcanzar el equilibrio entre las estrategias para evitar errores y las estrategias de tolerancia a errores. | Conforme | En la sección “Gestión de Errores” del documento SAS\_CTV.docx se mencionan las medidas para gestionar los errores con el fin de alcanzar el equilibrio entre las estrategias para evitar errores y las estrategias de tolerancia a errores. | -- |
| 7.3.4.12 | La Especificación de la Arquitectura del Software debe justificar que las técnicas, medidas y herramientas elegidas forman un conjunto que satisface la Especificación de Requisitos del Software al nivel requerido de integridad de seguridad del software. | Conforme | En la sección “Seguridad Operacional (Safety)” del documento SAS\_CTV, se menciona el documento M-S-Rd-001 Software Quality Assurance Plan en donde puede ser encontradas las técnicas y medidas usadas en el “Anexo B: Técnicas para el desarrollo de Software”. Así mismo, las herramientas se puede encontrar información en la sección “Herramientas de Desarrollo de Software”. | -- |
| 7.3.4.13 | La Especificación de la Arquitectura del Software debe tener en cuenta los requisitos del apartado 8.4.8 cuando el software esté configurado mediante datos o algoritmos de aplicación. | | | |
| 8.4.8.1 | El desarrollo de software genérico, que soporte la ejecución de los datos/algoritmos de aplicación, debe cumplir con los requisitos descritos desde el apartado 7.1 al 7.7 de esta norma europea. Se deben respetar igualmente los siguientes requisitos adicionales. | Conforme | {{XXXX}} El componente “{{BBBB}}” es desarrollado para soportar la ejecución de los datos/algoritmos de aplicación, la evidencia de los requisitos descritos de la norma EN50128, desde el apartado 7.1 al 7.7, estarán registrados en sus respectivos reportes de verificación. | -- |
| 8.4.8.2 | En los documentos de la Especificación de Requisitos del Software del software genérico se deben identificar los tipos o clases de funciones que pueden configurarse mediante datos/algoritmos de aplicación en cada sistema y subsistema. El nivel de integridad de la seguridad asignado a las funciones determinará las normas a aplicar en el desarrollo posterior de los datos/algoritmos de aplicación para todas las instalaciones del sistema. | Conforme | {{XXXX}} Se identifica en la sección “{{EEEE}}” del documento Especificación de Requisitos del Software (SRS\_CTV Documento de Requerimientos de Software) que el componente “{{BBBB}}” deberá ser configurado mediante datos/algoritmos de aplicación y mediante su nivel de integridad de seguridad se determinarán las normas a aplicar en el desarrollo del software. | -- |
| 8.4.8.3 | Durante el diseño del software genérico se deben especificar las interfaces detalladas entre el software genérico y los datos/algoritmos de aplicación, a menos que ya se hubiera hecho en una etapa anterior del ciclo de vida, por ejemplo, como resultado del requisito de utilización de un lenguaje específico existente para la aplicación. | Conforme | En la sección “Definición de interfaces entre el Software genérico y los datos de aplicación” del documento M-S-Rd-015 Plan de Configuración de Aplicación se especifican las interfaces entre software genérico y los datos/algoritmos de aplicación. | -- |
| 8.4.8.4 | Se debe poner en práctica una separación rígida entre el software genérico y los datos/algoritmos de aplicación, es decir, se debe poder recompilar y actualizar o bien el software genérico o bien los datos/algoritmos de aplicación, sin necesidad de actualizar el otro, a menos que se haya producido una modificación en la interfaz definida entre el software genérico y los datos/algoritmos de aplicación. Del mismo modo, los datos/algoritmos específicos de aplicaciones deben separarse de los datos/algoritmos genéricos de aplicaciones. | Conforme | El componente “{{BBBB}}” será parte del binario final el cual no será recompilado. Sin embargo, los datos de aplicación serán recompilados/actualizados mediante las técnicas definidas en la sección “Técnicas de recopilación y actualización de los datos de aplicación” del documento M-S-Rd-015 Plan de Configuración de Aplicación | -- |
| 8.4.8.5 | Los procedimientos de control de las modificaciones deben garantizar que toda modificación que se realice en el software genérico solo puede instalarse después de que se haya establecido que o bien el software revisado es compatible con los datos/algoritmos de aplicación originales o que se han revisado los datos/algoritmos de aplicación | Conforme | En la sección “Procedimientos de control para modificaciones para los datos de aplicación” del documento M-S-Rd-015 Plan de Configuración de Aplicación se especifica el procedimiento de control de modificaciones para datos/algoritmos de aplicación. | -- |
| 8.4.8.6 | Se debe prestar atención particular en el proceso de verificación y en la fase de ensayos de validación del software genérico con el fin de garantizar que se tienen en cuenta todas las combinaciones pertinentes de datos y algoritmos.  Si no se han tenido en cuenta todas las combinaciones de datos y algoritmos en los procesos de verificación, ensayos y validación del software genérico, este hecho se debe identificar claramente como un límite en el uso del software genérico. Se debe realizar un complemento de los procesos de verificación, ensayos y validación del software genérico cuando se definan datos o algoritmos más allá de este límite. | Conforme | El software genérico con datos/algoritmos de aplicación será desarrollado bajo los procesos de verificación, ensayos y validación descritos en la sección “Técnicas de verificación, ensayos y validación para datos de aplicación” del documento M-S-Rd-015 Plan de Configuración de Aplicación y será responsabilidad del verificado analizar que en cada etapa del ciclo de vida que se sigan dichos procesos. | -- |
| 8.4.8.7 | El software genérico debe diseñarse para detectar datos/algoritmos de aplicación dañados, cuando sea factible. | Conforme | Se definen métodos para la detección de datos/algoritmos de aplicación dañados en la sección “Técnicas de detección de datos corruptos” del documento M-S-Rd-015 Plan de Configuración de Aplicación | -- |
| 8.4.8.8 | Los diseñadores deben publicar la Nota de la Versión Publicada del software genérico y de las herramientas de aplicación como muy tarde durante la fase de Ensayos del Software en Conjunto/Fase de Validación Final del software genérico y de las herramientas de aplicación. El contenido de estos documentos debe estar sujeto a actividades de verificación y validación.  En el documento "Condiciones de aplicación del software genérico y de las herramientas de aplicación" se debe recoger la siguiente información:  1) referencias a los manuales de usuario del software genérico y de otras herramientas de aplicación;  2) cualquier restricción en los datos/algoritmos de aplicación, por ejemplo, reglas de arquitectura o de codificación impuestas para cumplir con los niveles de integridad de la seguridad. | Conforme | En la sección "Datos de aplicación " del documento SAS\_CTV.docx se hace mención del documento “Reusabilidad de implementación" donde se hace referencia al documento “M-S-Rd-015 Plan de Configuración de Aplicación” que describe las restricciones que tendrán los datos y algoritmos de aplicación tales como reglas de arquitectura, documentación y reglas de codificación que aseguran su nivel de integridad de software. Así mismo, se hace referencia a los manuales de usuario del software genérico y otras herramientas de aplicación.  Ver tabla de suposiciones. | -- |
| 7.3.4.14 | La Especificación de la Arquitectura del Software debe seleccionar técnicas y medidas de entre las enumeradas en la tabla A.3. La combinación seleccionada debe justificarse como un conjunto que satisfaga los apartados 4.8 y 4.9. | Conforme. | En la sección “Seguridad Operacional (Safety)” se menciona el documento “M-S-Rd-001 (Software Quality Assurance Plan)” en donde puede ser encontradas las técnicas y medidas usadas en el “Anexo B: Técnicas para el desarrollo de Software” y en la tabla “Arquitectura del Software” se describen las técnicas y medidas seleccionadas de la tabla A.3 de la norma EN50128 | - |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reqs.** | **Criterio de aceptación** | **Conforme/**  **No Conforme** | **Descripción de la Evidencia/Deficiencia** | **¿Es critica la desviación?** |
| 5.3.2.7 | Se debe asegurar la trazabilidad de los documentos mediante un número de referencia único y una relación definida y documentada con otros documentos. | Conforme | Se asegura la trazabilidad de los documentos mediante un número de referencia único SAS\_CTV.docx, SAS\_Global.docx, SAS\_CTV.xlxs y ArquitecturaSW\_CTV.pptx  La relación con otros documentos se describe en la sección “Referencias” en el documento SAS\_CTV.docx | -- |
| 5.3.2.8 | Cada término, acrónimo o abreviatura debe tener el mismo significado en los distintos documentos. Si no es posible por razones históricas, se deben enumerar los distintos significados y dar las referencias. | Conforme | Las abreviaturas y definiciones utilizadas en los archivos SAS\_CTV.docx, SAS\_Global.docx, SAS\_CTV.xlxs y ArquitecturaSW\_CTV.pptx concuerdan con las definidas en:  “Referencia a Definiciones de Software.txt” | -- |
| 5.3.2.9 | Todo documento, debe estar redactado siguiendo las siguientes reglas:  – debe contener o implementar todas las condiciones y requisitos aplicables del documento que le precede con el que tenga una relación jerárquica;  – no debe contradecir al documento que le precede  Note: Excepto aquellos relativos a software preexistente (véase 7.3.4.7). | Conforme | Los documentos SAS\_CTV.docx, SAS\_Global.docx, SAS\_CTV.xlxs y ArquitecturaSW\_CTV.pptx implementan todas las condiciones y requisitos especificados para el componente “{{BBBB}}” por los documentos:  a) Especificación de Requisitos del Software (“SRS\_CTV Documento de Requerimientos de Software”)  b) Especificación de Diseño del Software (“SDS\_{{BBBB}}”)  c) Especificaciones de la Interfaz del Software (“SIS\_{{BBBB}}.h”, “SIS\_{{BBBB}}\_def.h” y “SIS\_{{BBBB}}\_cfg.h”)  los cuales especifican el comportamiento del componente y estos no se contradicen por los documentos SAS\_CTV.docx, SAS\_Global.docx, SAS\_CTV.xlxs y ArquitecturaSW\_CTV.pptx | -- |
| 5.3.2.10 | Se debe hacer referencia con el mismo nombre o descripción a cada elemento o concepto en todos los documentos. | Conforme | Las abreviaturas y definiciones utilizadas en los archivos SAS\_CTV.docx, SAS\_Global.docx, SAS\_CTV.xlxs y ArquitecturaSW\_CTV.pptx  concuerdan con las definidas en:  “Referencia a Definiciones de Software.txt” | -- |

| **Reqs.** | **Criterio de aceptación** | **Conforme/**  **No Conforme** | **Descripción de la Evidencia/Deficiencia** | **¿Es critica la desviación?** |
| --- | --- | --- | --- | --- |
| 6.5.4.14 | La trazabilidad de los requisitos debe ser una de las consideraciones importantes a tener en cuenta para la validación de un sistema relacionado con la seguridad y se deben proporcionar los medios que permitan demostrarla durante todas las fases del ciclo de vida. | Conforme | Se tienen los requisitos de software para el componente “{{BBBB}}”, descritos en la sección “{{EEEE}}”, y estos están trazados mediante el documento “Pr-QS-008 F1 Requisitos”.  Ver tabla de Suposiciones. | -- |
| 6.5.4.15 | Dentro del contexto de esta norma europea, y dentro de un límite apropiado al nivel de integridad de seguridad del software especificado, la trazabilidad debe hacer referencia principalmente a: a) la trazabilidad de los requisitos con respecto al diseño u otros objetos que los satisfagan.  b) la trazabilidad de los objetos de diseño en relación a los objetos de implementación que los instancian.  c) la trazabilidad de los requisitos y de los objetos de diseño en relación a los ensayos (componente, integración, ensayo de conjunto) y los análisis que los verifiquen. | Conforme | Para la trazabilidad del conjunto de requisitos del componente “{{BBBB}}” descritos en la sección “{{EEEE}}” se usará el documento “Pr-QS-008 F1”.  a) Se cumplirá con la columna “Documento evidencia arquitectura/diseño”.  b) Se cumplirá con la columna “documento evidencia/ implementación”.  c) Se cumplirá con la columna “Documento evidencia verificación/validación”  Ver tabla de Suposiciones. | -- |
| 6.5.4.16 | En determinados casos, por ejemplo, para softwares preexistentes o para prototipos de software, la trazabilidad puede establecerse después de la implementación y/o documentación del código, pero antes de la verificación/validación. En estos casos, se debe demostrar que la verificación/validación es tan efectiva como lo hubiera sido con la trazabilidad en todas las fases. | Conforme | El componente no es preexistente acorde a columna “Preexistente” de la hoja “SAS – Componentes” del documento “SAS\_CTV.xlxs”, por lo que la trazabilidad se está estableciendo en cada fase del desarrollo. | -- |

|  |  |  |  |
| --- | --- | --- | --- |
| **Componentes, datos, estructuras y algoritmos adaptados de manera deficiente en el diseño o implementación.** | | | |
| **Si aplica, liste los componentes, datos, estructuras y algoritmos:** | | | |
| **No** | **Tipo** | **Nombre/Identificador** | **Deficiencias** |
| **1** | - | - | **-** |
| **2** | - | - | - |
| **3** | - | - | - |

|  |  |
| --- | --- |
| **No** | **Suposiciones (si aplican)** |
| **1** | Se supone que el documento “M-S-Rd-015 Plan de Configuración de Aplicación” es el documento “Condiciones de aplicación del software y de las herramientas de aplicación” (documento mencionado en la norma EN50128). Este documento será revisado y verificado. |
| **2** | En caso de cambio en Especificación de Requisitos de Software, el verificador deberá asegurar que las modificaciones en los requisitos mantienen su trazabilidad en esta etapa. |
| **3** | Se cuenta con la documentación completa para asegurar que el software existente es seguro y esta desarrollado con estándares de la norma EN 50128 |

|  |  |
| --- | --- |
| **Resumen de resultados.** | |
| **Documento en revisión:** | SAS\_CTV.docx  SAS\_Global.docx  SAS\_CTV.xlxs  ArquitecturaSW\_CTV.pptx  ( {{BBBB}} ) |
| **Versión:** | {{FFFF}} |
| El reporte tiene como resultado el cumplimentó de todos los puntos de la norma | |
| {{AAAA}}  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Nombre y Firma del verificador** | |