REGLAMENTO (CE) Nº 482/2008 DE LA COMISIÓN

de 30 de mayo de 2008

por el que se establece un sistema de garantía de la seguridad del *software* que deberán implantar los proveedores de servicios de navegación aérea y por el que se modifica el anexo II del Reglamento (CE) nº 2096/2005

(Texto pertinente a efectos del EEE)

LA COMISIÓN DE LAS COMUNIDADES EUROPEAS,

Visto el Tratado constitutivo de la Comunidad Europea,

Visto el Reglamento (CE) nº 550/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, relativo a la prestación de servicios de navegación aérea en el cielo único europeo (Reglamento de prestación de servicios) ([1]), y, en particular, su artículo 4,

Considerando lo siguiente:

(1) En virtud del Reglamento (CE) nº 550/2004, la Comisión debe determinar y adoptar las disposiciones pertinentes de los requisitos reglamentarios de seguridad de Eurocontrol (ESARR), teniendo en cuenta la legislación comunitaria existente. ESARR 6, calificado en materia de «*Software* en sistemas ATM», proporciona un conjunto de requisitos reglamentarios de seguridad para la implantación de un sistema de garantía de la seguridad del *software*.

(2) El Reglamento (CE) nº 2096/2005 de la Comisión, de 20 de diciembre de 2005, por el que se establecen requisitos comunes para la prestación de servicios de navegación aérea ([2]), afirma en su la última frase del considerando 12 que «las disposiciones pertinentes de ESARR 1 sobre el control de seguridad en ATM y ESARR 6 sobre programas informáticos en los sistemas ATM deben determinarse y adoptarse mediante diferentes actos comunitarios».

(3) El anexo II del Reglamento (CE) nº 2096/2005 exige que los proveedores de servicios de tráfico aéreo implanten un sistema de gestión de la seguridad así como de requisitos de seguridad para un análisis y mitigación de riesgos en relación con los cambios. En el marco de su sistema de gestión de la seguridad, y dentro de las actividades de análisis y mitigación de riesgos con respecto a las modificaciones, los proveedores de servicios de tráfico aéreo deben definir e implantar un sistema de garantía de la seguridad del *software* dedicado específicamente a los aspectos relacionados con el *software*.

(4) El principal objetivo de seguridad del *software* que deben alcanzar los sistemas funcionales que contienen *software* es garantizar la reducción a un nivel tolerable de los riesgos asociados al uso del *software* en los sistemas de la red europea de gestión del tránsito aéreo («*software* EATMN»).

(5) El presente Reglamento no debe incluir las operaciones y entrenamientos militares a que se refiere el artículo 1, apartado 2, del Reglamento (CE) nº 549/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se fija el marco para la creación del cielo único europeo (el Reglamento marco) ([3]).

(6) El anexo II del Reglamento debe por tanto ser modificado en consecuencia.

(7) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité del cielo único.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Ámbito de aplicación y alcance

1. El presente Reglamento establece los requisitos para la definición e implantación de un sistema de garantía de la seguridad del *software* por los proveedores de servicios de tránsito aéreo (ATS), las entidades encargadas de la gestión del flujo del tránsito aéreo (ATFM), de la gestión del espacio aéreo (ASM) para el tránsito aéreo general y los proveedores de servicios de comunicación, navegación, y vigilancia (CNS).

Determina y adopta las disposiciones obligatorias del requisito reglamentario de seguridad de Eurocontrol sobre el *software* ESARR 6 calificado en materia de «*Software* en sistemas ATM» publicado el 6 de noviembre de 2003.

2. El presente Reglamento se aplicará al *software* nuevo y a cualquier cambio del *software* de los sistemas de ATS, ASM, ATFM y CNS.

No se aplicará al *software* de los componentes transportados a bordo ni a los equipos espaciales.

Artículo 2

Definiciones

A efectos del presente Reglamento serán de aplicación las definiciones establecidas en el artículo 2 del Reglamento (CE) nº 549/2004.

([1]) DO L 96 de 31.3.2004, p. 10.
([2]) DO L 335 de 21.12.2005, p. 13. Reglamento modificado por el Reglamento (CE) nº 1315/2007 (DO L 291 de 9.11.2007, p. 16).
([3]) DO L 96 de 31.3.2004, p. 1.

Además, se entenderá por:

1) «*software*»: los programas informáticos y los correspondientes datos de configuración, incluido el *software* no desarrollado, pero excluidos elementos electrónicos en particular los circuitos integrados de aplicación específica, las matrices de puertas programables o los controladores lógicos de estado sólido;

2) «datos de configuración»: los datos que configuran un sistema *software* genérico para un caso particular de utilización del mismo;

3) «*software* no desarrollado»: un *software* no desarrollado concretamente para el contrato de que se trate;

4) «garantía de seguridad»: todas las acciones planificadas y sistemáticas necesarias para proporcionar la confianza adecuada en que un producto, servicio, organización o sistema funcional alcanzan una seguridad aceptable o tolerable;

5) «organización»: un proveedor de ATS, o un proveedor de CNS o una entidad suministradora de ATFM o ASM;

6) «sistema funcional»: una combinación de sistemas, procedimientos y recursos humanos organizados para llevar a cabo una función en el contexto de la ATM;

7) «riesgo»: la combinación de la probabilidad global, o frecuencia de aparición, de un efecto perjudicial provocado por una situación peligrosa y la severidad de dicho efecto;

8) «situación peligrosa»: cualquier condición, evento o circunstancia que pueda dar lugar a un accidente;

9) «*software* nuevo»: un *software* que ha sido encargado o por el que se han firmado contratos vinculantes tras la entrada en vigor del presente Reglamento;

10) «objetivo de seguridad»: una declaración cualitativa o cuantitativa que define la frecuencia o probabilidad máxima de que se produzca una situación peligrosa;

11) «requisito de seguridad»: un medio para mitigar los riesgos, definido a partir de una estrategia de mitigación de riesgos, que permite alcanzar un objetivo de seguridad determinado, incluidos los requisitos de organización, operación, procedimiento, función, rendimiento, interoperabilidad o características medioambientales;

12) «sustitución en caliente»: el enfoque que permite sustituir los componentes o el *software* del sistema European air traffic management network (EATMN) mientras el sistema sigue funcionando;

13) «requisito de seguridad del *software*»: la descripción de lo que debe producir el *software* dadas unas entradas y unas restricciones, de manera que si se respeta queda garantizado que el *software* EATMN se ejecuta con seguridad y de acuerdo con las necesidades operativas;

14) «*software* EATMN»: el *software* utilizado en los sistemas a que se refiere el artículo 1;

15) «validez de los requisitos»: la confirmación, mediante el examen y la aportación de pruebas objetivas, de que los requisitos particulares para un uso específico responden a lo que se pretende;

16) «conseguido con independencia»: en relación con las actividades del proceso de verificación del *software*, el hecho de que dichas actividades las lleven a cabo una o varias personas distintas del desarrollador del elemento sometido a verificación;

17) «funcionamiento incorrecto del *software*»: la incapacidad de un programa para llevar a cabo correctamente la función requerida;

18) «fallo del *software*»: la incapacidad de un programa para llevar a cabo la función requerida;

19) «producto COTS» (*Commercial Off-The-Shelf*): una aplicación comercialmente disponible vendida a través de catálogos públicos y no está pensada para su personalización o mejora;

20) «componentes de *software*»: los bloques elementales que pueden encajarse o conectarse con otros bloques reutilizables de *software* para, combinados, crear una aplicación de *software* personalizada;

21) «componentes de *software* independientes»: aquellos componentes del *software* a los que no deja inoperativos la misma condición de fallo que causa la situación peligrosa;

22) «rendimiento en tiempo del *software*»: el tiempo que se concede al *software* para que responda a entradas dadas o a eventos periódicos, y/o el rendimiento del *software* en términos de transacciones o mensajes gestionados por unidad de tiempo;

23) «capacidad del *software*»: la capacidad del *software* para gestionar determinado volumen de flujo de datos;

24) «exactitud»: la precisión requerida de los resultados calculados;

25) «uso de recursos del *software*»: la cantidad de recursos del sistema informático que el *software* de aplicación puede utilizar;

26) «robustez del *software*»: el comportamiento del *software* en caso de entradas inesperadas, averías del *hardware* e interrupciones de la alimentación, sea en el propio sistema informático o en los dispositivos conectados;

27) «tolerancia a la sobrecarga»: el comportamiento del sistema en caso de que las entradas se produzcan a una tasa superior a la esperada durante el funcionamiento normal del sistema y, en particular, su tolerancia a ello;

28) «verificación correcta y completa del *software* EATMN»: el hecho de que todos los requisitos de seguridad del *software* declaren correctamente lo que exige del componente de *software* el proceso de análisis y mitigación de riesgos y de que su implementación esté demostrada al nivel que exige el nivel de seguridad del *software*;

29) «datos del ciclo de vida del *software*»: los datos que se producen durante el ciclo de vida del *software* para planificar, dirigir, explicar, definir, registrar o demostrar las actividades; estos datos permiten la aprobación de los procesos del ciclo de vida del *software*, el sistema o los equipos y la modificación del producto de *software* tras su aprobación;

30) «ciclo de vida del *software*»:

a) una serie ordenada de procesos que una organización considera suficientes y adecuados para producir un producto de *software*;

b) el período de tiempo que se inicia con la decisión de producir o modificar un producto de *software* y concluye cuando se retira del servicio ese producto;

31) «requisitos de seguridad del sistema»: un requisito de seguridad aplicable a un sistema funcional.

Artículo 3

Requisitos generales de seguridad

1. Cuando una organización deba implantar un proceso de análisis y mitigación de riesgos de conformidad con la legislación comunitaria o nacional aplicable, deberá definir e implantar un sistema de garantía de la seguridad del *software* para abordar específicamente los aspectos relacionados con el *software* EATMN, incluidas todas las modificaciones operativas del *software* en línea, y en particular la sustitución en caliente.

2. La organización velará por que, como mínimo, su sistema de garantía de la seguridad del *software* genera pruebas y argumentos que demuestren que:

a) los requisitos de seguridad del *software* manifiestan correctamente lo que el *software* exige a fin de cumplir los objetivos y requisitos de seguridad identificados por el proceso de análisis y mitigación de riesgos;

b) se tiene en cuenta la trazabilidad en relación con todos los requisitos de seguridad del *software*;

c) la implementación del *software* no contiene ninguna función que afecte negativamente a la seguridad,

d) el *software* EATMN satisface sus requisitos con un nivel de confianza en consonancia con la criticidad del *software*,

e) se han aportado las garantías que confirman que se satisfacen los requisitos generales de seguridad establecidos en las letras a) a d) y los argumentos que demuestran cada garantía requerida se deducen en todo momento de:

i) una versión ejecutable conocida del *software*,

ii) un rango conocido de datos de la configuración, y

iii) un conjunto conocido de descripciones y productos de *software*, incluidas las especificaciones, que se han utilizado en la producción de dicha versión.

3. La organización pondrá a disposición de la autoridad nacional de supervisión las garantías requeridas que demuestren que se han satisfecho los requisitos del apartado 2.

Artículo 4

Requisitos aplicables al sistema de garantía de la seguridad del *software*

La organización velará por que, como mínimo, el sistema de garantía de la seguridad del *software*:

1) esté documentado, específicamente como parte de la documentación global sobre análisis y mitigación de riesgos;

2) asigne niveles de garantía del *software* a todo el *software* operativo EATMN cumpliendo los requisitos establecidos en el anexo I;

3) incluya garantías de:

a) la validez de los requisitos de seguridad del *software* en cumplimiento de los requisitos establecidos en el anexo II, parte A;

b) la verificación del *software* en cumplimiento de los requisitos establecidos en el anexo II, parte B;

c) la gestión de la configuración del *software* en cumplimiento de los requisitos establecidos en el anexo II, parte C, y

d) la trazabilidad de los requisitos de seguridad del *software* en cumplimiento de los requisitos establecidos en el anexo II, parte D;

4) determine el rigor con el que se establecen las garantías. El rigor se definirá para cada nivel de garantía del *software* y deberá aumentar a medida que se incremente la criticidad del *software*. A tal efecto:

a) la variación del rigor de las garantías, por cada nivel de garantía del *software*, incluirá los criterios:

i) necesarios para conseguirse con independencia,

ii) necesarios para conseguirse,

iii) no necesarios;

b) las garantías correspondientes a cada nivel de garantía del *software* proporcionarán confianza suficiente en que el *software* EATMN puede explotarse de una manera tolerablemente segura;

5) utilice la información obtenida de la experiencia con el *software* EATMN para confirmar la adecuación del sistema de garantía de la seguridad del *software* y de la asignación de los niveles de garantía. A tal fin, deberán evaluarse los efectos de un funcionamiento incorrecto o un fallo del *software* notificados con arreglo a los requisitos pertinentes sobre notificación y evaluación de las incidencias de seguridad comparándolos con los efectos identificados para el sistema de que se trate con arreglo al sistema de clasificación de la severidad establecido en la sección 3.2.4 del anexo II del Reglamento (CE) nº 2096/2005.

Artículo 5

Requisitos aplicables a las modificaciones del *software* y a determinados tipos de *software*

1. Para cualquier cambio del *software* o para tipos de *software* específicos tales como los productos COTS, el *software* no desarrollado o el *software* reutilizado para los que no pueden aplicarse algunos de los requisitos del artículo 3, apartado 2, letras d) o e), o del artículo 4, apartados 2, 3, 4 o 5, la organización velará por que el sistema de garantía de la seguridad del *software* proporcione, por otros medios elegidos y acordados con la autoridad nacional de supervisión, el mismo nivel de confianza que el nivel de garantía del *software* pertinente cuando esté definido.

Los mencionados medios proporcionarán confianza suficiente en que el *software* satisface los objetivos y requisitos de seguridad identificados en el proceso de análisis y mitigación de riesgos.

2. En la evaluación de los medios contemplados en el apartado 1, la autoridad nacional de supervisión podrá ordenar el uso a una organización reconocida o a un organismo notificado.

Artículo 6

Modificación del Reglamento (CE) nº 2096/2005

En el anexo II del Reglamento (CE) nº 2096/2005, se añade la sección siguiente:

«3.2.5. Sección 5

Sistema de garantía de la seguridad del *software*

Dentro de la aplicación del sistema de gestión de la seguridad, los proveedores de servicios de tránsito aéreo implantarán un sistema de garantía de la seguridad del *software* de conformidad con el Reglamento (CE) nº 482/2008 de 30 de mayo de 2008, por el que se establece un sistema de garantía de la seguridad del *software* que deberán implantar los proveedores de servicios de navegación aérea y por el que se modifica el Reglamento (CE) nº 2096/2005 (*)

(*) DO L 141 de 31.5.2008, p. 5».

Artículo 7

Entrada en vigor

El presente Reglamento entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

Se aplicará a partir del 1 de enero de 2009 al nuevo *software* de los sistemas EATMN a que se refiere el artículo 1, apartado 2, párrafo primero.

Se aplicará a partir del 1 de julio de 2010 a cualquier cambio del *software* de los sistemas EATMN a que se refiere el artículo 1, apartado 2, párrafo primero, en funcionamiento en dicha fecha.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 30 de mayo de 2008.

Por la Comisión

Antonio TAJANI

Miembro de la Comisión

ANEXO I

Requisitos aplicables al nivel de seguridad del *software* a que se refiere el artículo 4, apartado 2

1. El nivel de garantía del *software* deberá relacionar el rigor de las garantías del *software* EATMN con la criticidad del *software* utilizando el sistema de clasificación de la severidad del punto 3.2.4, sección 2, del anexo II del Reglamento (CE) nº 2096/2005, combinado con la probabilidad de que ocurra determinado efecto adverso. Se definirá un mínimo de cuatro niveles de garantía del *software*, designándose el más crítico con el número 1.

2. El nivel de garantía del *software* asignado deberá guardar proporción con el efecto más adverso que pueda ocasionar el funcionamiento incorrecto o el fallo del *software*, con arreglo al punto 3.2.4, sección 2, del anexo II del Reglamento (CE) nº 2096/2005. En particular, se tendrán en cuenta los riesgos asociados con el funcionamiento incorrecto o el fallo del *software* y las defensas de arquitectura y/o procedimiento identificadas.

3. Los componentes del *software* EATMN cuya independencia mutua no pueda demostrarse se asignarán al nivel de garantía del componente dependiente más crítico.

ANEXO II

Parte A: Requisitos aplicables a la garantía de validez de los requisitos de seguridad del *software* a que se refiere el artículo 4, apartado 3, letra a)

1. Los requisitos de seguridad del *software* especificarán el comportamiento funcional en modos nominal y degradado del *software* EATMN, el rendimiento en tiempo, la capacidad, la exactitud, el uso de recursos del *software* en el *hardware* a que va destinado, la robustez en condiciones operativas anormales y la tolerancia a la sobrecarga, según proceda.

2. Los requisitos de seguridad del *software* serán completos y correctos, y cumplirán también con los requisitos de seguridad del sistema.

Parte B: Requisitos aplicables a la garantía de verificación del *software* a que se refiere el artículo 4, apartado 3, letra b)

1. El comportamiento funcional del *software* EATMN, el rendimiento en tiempo, la capacidad, la exactitud, el uso de recursos del *software* en el *hardware* a que va destinado, la robustez en condiciones operativas anormales y la tolerancia a la sobrecarga cumplirán con los requisitos del *software*.

2. El *software* EATMN será verificado adecuadamente mediante análisis y/o ensayos y/o en medios equivalentes, según se acuerde con la autoridad nacional de supervisión.

3. La verificación del *software* EATMN deberá ser correcta y completa.

Parte C: Requisitos aplicables a las garantías de gestión de la configuración del *software* a que se refiere el artículo 4, apartado 3, letra c)

1. Se considerará que existen la identificación, la trazabilidad y el registro del estado de la configuración cuando se pueda demostrar que los datos del ciclo de vida del *software* se encuentran sometidos al control de la configuración a lo largo de todo el ciclo de vida del *software* EATMN.

2. Se considerará que existen la notificación, el seguimiento y las medidas correctoras de los problemas cuando se pueda demostrar que los problemas relacionados con la seguridad asociados al *software* han sido mitigados.

3. Se considerará que existen procedimientos de recuperación y entrega cuando se pueda demostrar que los datos del ciclo de vida del *software* pueden ser regenerados y restituidos a través del ciclo de vida del *software* EATMN.

Parte D: Requisitos aplicables a las garantías de trazabilidad de los requisitos de seguridad del *software* a que se refiere el artículo 4, apartado 3, letra d)

1. Cada requisito de seguridad de *software* será trazable hasta el mismo nivel de diseño al que se demuestra su satisfacción.

2. Cada requisito de seguridad de *software* será trazable, en cada nivel del diseño al que se demuestra su satisfacción, será trazable hasta un requisito de seguridad del sistema.