NORMA CUBANA

NC

IEC 61508-1: 2012
(Publicada por la IEC en 1998)

SEGURIDAD FUNCIONAL DE LOS SISTEMAS ELÉCTRICOS/ELECTRÓNICOS/ELECTRÓNICOS PROGRAMABLES RELACIONADOS CON LA SEGURIDAD — PARTE 1: REQUISITOS GENERALES (IEC 61508-1: 1998 + Corr 1999, IDT)

Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements

ICS: 13.110; 25.040; 29.020; 240.50

1. Edición Diciembre 2012

Oficina Nacional de Normalización (NC) Calle E No. 261 El Vedado, La Habana. Cuba. Teléfono: 830-0835 Fax: (537) 836-8048; Correo electrónico: nc@ncnorma.cu; Sitio Web: www.nc.cubaindustria.cu

Cuban National Bureau of Standards

Prefacio

La Oficina Nacional de Normalización (NC) es el Organismo Nacional de Normalización de la República de Cuba y representa al país ante las organizaciones internacionales y regionales de normalización.

La elaboración de las Normas Cubanas y otros documentos normativos relacionados se realiza generalmente a través de los Comités Técnicos de Normalización. Su aprobación es competencia de la Oficina Nacional de Normalización y se basa en las evidencias del consenso.

Esta Norma Cubana:

- Ha sido elaborada por el Comité Técnico de Normalización NC/CTN 116 de Automática, integrado por representantes de las siguientes entidades:

  - Empresa de Automatización Integral perteneciente al Ministerio de la Informática y las Comunicaciones
  - Ministerio de la Industria Básica
  - Universidad de Oriente
  - Universidad Central de Villa Clara, Marta Abreu
  - Instituto Superior Politécnico, José Antonio Echevarría
  - ALIMATIC del Ministerio de la Industria Alimentaria
  - Universidad de Ciencias Informáticas
  - Instituto de Cibernética, Matemática y Física
  - Ministerio de Ciencia, Tecnología y Medio Ambiente
  - Oficina Nacional de Normalización

- Es una adopción idéntica por el método de reimpresión de la versión oficial en español de la Norma Europea EN 61508-1: 2001 *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements* que a su vez adopta de forma idéntica a la Norma Internacional IEC 61508-1: 1998 + Corr 1999)

Oficina Nacional de Normalización (NC)
Calle E No. 261, El Vedado, La Habana, Habana 4, Cuba.

Impreso en Cuba.

NORMA EUROPEA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 61508-1

Diciembre 2001

ICS 13.110;25.040;29.020;35.240.50

Versión en español

Seguridad funcional de los sistemas eléctricos/electrónicos/ electrónicos programables relacionados con la seguridad
Parte 1: Requisitos generales
(CEI 61508-1:1998 + Corrigendum 1999)

Functional safety of electrical/electronic/ programmable electronic safety-related systems.
Part 1: General requirements.
(IEC 61508-1:1998 + Corrigendum 1999).

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.
Partie 1: Prescriptions générales.
(CEI 61508-1:1998 + Corrigendum 1999).

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme.
Teil 1: Allgemeine Anforderungen.
(IEC 61508-1:1998 + Corrigendum 1999).

Esta norma europea ha sido aprobada por CENELEC el 2001-07-03. Los miembros de CENELEC están sometidos al Reglamento Interior de CEN/CENELEC que define las condiciones dentro de las cuales debe adoptarse, sin modificación, la norma europea como norma nacional.

Las correspondientes listas actualizadas y las referencias bibliográficas relativas a estas normas nacionales, pueden obtenerse en la Secretaría Central de CENELEC, o a través de sus miembros.

Esta norma europea existe en tres versiones oficiales (alemán, francés e inglés). Una versión en otra lengua realizada bajo la responsabilidad de un miembro de CENELEC en su idioma nacional, y notificada a la Secretaría Central, tiene el mismo rango que aquéllas.

Los miembros de CENELEC son los comités electrotécnicos nacionales de normalización de los países siguientes: Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Grecia, Irlanda, Islandia, Italia, Luxemburgo, Malta, Noruega, Países Bajos, Portugal, Reino Unido, República Checa, Suecia y Suiza.

CENELEC
COMITÉ EUROPEO DE NORMALIZACIÓN ELECTROTÉCNICA
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung
SECRETARÍA CENTRAL: Rue de Stassart, 35 B-1050 Bruxelles

ANTECEDENTES

El texto de la Norma Internacional CEI 61508-1:1998 y su corrigendum de mayo de 1999, preparado por el Subcomité SC 65A, *Aspectos de sistemas*, del Comité Técnico TC 65, *Medida y control en procesos industriales*, de CEI, fue sometido al Procedimiento de Aceptación Única (UAP) y fue aprobado por CENELEC como Norma Europea EN 61508-1 el 2001-07-03 sin ninguna modificación.

Se fijaron las siguientes fechas:

– Fecha límite en la que la norma europea debe adoptarse a nivel nacional por publicación de una norma nacional idéntica o por ratificación	(dop)	2002-08-01
– Fecha límite en la que deben retirarse las normas nacionales divergentes con esta norma	(dow)	2004-08-01

Los anexos denominados “normativos” forman parte del cuerpo de la norma.

Los anexos denominados “informativos” se dan sólo para información.

En esta norma el anexo ZA es normativo y los anexos A, B y C son informativos.

El anexo ZA ha sido añadido por CENELEC.

La Norma CEI 61508 es una publicación básica de seguridad que se aplica a la seguridad funcional de los sistemas eléctricos, electrónicos y electrónicos programables relacionados con la seguridad. El objeto y campo de aplicación establece:

"Esta norma internacional trata los aspectos a tener en consideración cuando se utilicen sistemas eléctricos/electrónicos/electrónicos programables (E/E/PE), para ejecutar funciones de seguridad. Uno de los principales objetivos de esta norma internacional es permitir la elaboración de normas internacionales específicas a cada sector de aplicación por los comités técnicos responsables de los sectores correspondientes. Esto permitirá tener en cuenta el conjunto de los factores pertinentes para cada aplicación, y de responder a las necesidades especificas de cada uno de estos sectores. Otro de los objetivos perseguidos por esta norma internacional es permitir el desarrollo de sistemas E/E/PE relacionados con la seguridad en ausencia eventual de normas internacionales para este sector de aplicación".

El Informe CENELEC R0BT-004, ratificado por el 103 BT (marzo 2000) acepta que algunas normas CEI, hoy publicadas o en preparación, sean implementaciones sectoriales de la Norma CEI 61508. Por ejemplo:

- CEI 61511 – *Seguridad funcional. Sistemas instrumentados de seguridad para el sector de industrias de transformación.*

- CEI 62061 – *Seguridad de las máquinas. Seguridad funcional de los sistemas de control eléctricos, electrónicos y electrónicos programables.*

- CEI 61513 – *Centrales nucleares. Instrumentación y control para los sistema importantes para la seguridad. Requisitos generales para los sistemas.*

El sector ferroviario ha desarrollado también un conjunto de normas europeas (EN 50126, EN 50128 y prEN 50129).

NOTA – Las Normas EN 50126 y EN 50128 están basadas en los proyectos iniciales de la Norma CEI 61508. El prEN 50129 está basado en principio, en la última versión de la Norma CEI 61508.

Esta lista no prejuzga otras implementaciones sectoriales de la Norma CEI 61508 que podrán estar actualmente en preparación o publicadas por CENELEC o CEI.

DECLARACIÓN

El texto de la Norma Internacional CEI 61508-1:1998 y su corrigendum de mayo de 1999 fue aprobado por CENELEC como norma europea sin ninguna modificación.

En la versión oficial, para la bibliografía, debe añadirse la siguiente nota para la norma indicada*:

CEI 61355:1997 NOTA – Armonizada como Norma EN 61355:1997 (sin ninguna modificación).

* Introducida en la norma indicándose con una línea vertical en el margen izquierdo del texto.

ÍNDICE

Anexos

Tablas

Figuras

INTRODUCCIÓN

Los sistemas eléctricos y electrónicos se han utilizado durante muchos años para realizar funciones de seguridad en la mayoría de los sectores de aplicación. Los sistemas basados en la informática (generalmente referidos a Sistemas Electrónicos Programables (PES)[1)] se utilizan en todos los sectores de aplicación para realizar funciones no relacionadas con la seguridad, pero cada día más se están utilizando para funciones de seguridad. Si se quiere explotar de forma eficaz y segura la tecnología de los sistemas informáticos, es imprescindible que el responsable de tomar decisiones haya sido orientado en los aspectos de seguridad en los cuales va a tomar las decisiones.

Esta norma internacional establece una aproximación genérica para todas las actividades relacionadas con el ciclo de vida de seguridad de los sistemas que incluyan componentes eléctricos y/o electrónicos y/o electrónicos programables (E/E/PES) que se utilizan para realizar las funciones de seguridad. Esta propuesta unificada ha sido adoptada con el fin de desarrollar una política técnica lógica y coherente relativa a todos los aparatos eléctricos relacionados con la seguridad. Uno de los principales objetivos perseguidos es el de facilitar la elaboración de normas de aplicación sectorial.

En la mayoría de los casos, la seguridad se obtiene gracias a un cierto número de sistemas de protección basados en distintas tecnologías (por ejemplo, mecánica, hidráulica, neumática, eléctrica, electrónica, electrónica programable). Por lo tanto, toda estrategia de seguridad debe tener en cuenta no solamente todos los elementos de un sistema de seguridad individual (por ejemplo, sensores, dispositivos de control e interruptores), sino que también debe tener en cuenta todos los sistemas relacionados con la seguridad como elementos individuales de un conjunto complejo. Es por ello que esta norma internacional, tratando esencialmente los sistemas, relacionados con la seguridad, eléctricos/electrónicos/ electrónicos programables E/E/PE, también puede proporcionar un sistema en el cual pueden considerarse los sistemas relacionados con la seguridad basados en otras tecnologías.

Existe gran variedad de aplicaciones de los E/E/PES. Estos cubren un gran número de grados de complejidad, y potenciales de peligros y riesgos en todos los sectores de aplicación. Para cada aplicación, las medidas de seguridad requeridas dependerán de los propios factores de la aplicación. Esta norma internacional, por ser genérica, debe permitir en lo sucesivo trasponer estas medidas en las normas internacionales de aplicación sectorial.

Esta norma internacional:

- concierne a todas las fases del ciclo de vida de la seguridad de los E/E/PES y del software (desde la concepción inicial, pasando por el diseño, la instalación, la explotación y el mantenimiento, hasta la finalización del servicio) donde los E/E/PES realizan funciones de seguridad;

- ha sido elaborada teniendo en cuenta la rápida evolución de la tecnología; el marco que comprende esta norma internacional es suficientemente sólido y extenso como para prever las evoluciones futuras;

- permite la elaboración de normas internacionales por sectores de aplicación concernientes a los E/E/PES relacionados con la seguridad. La elaboración de normas internacionales por sector de aplicación a partir de esta norma internacional debe permitir alcanzar un alto nivel de coherencia (por ejemplo, principios subyacentes, terminología, etc.) tanto en el seno de cada sector de aplicación, como de un sector a otro. Esto proporcionará una mejora en términos de seguridad y de beneficios económicos;

- proporciona un método para el desarrollo de los requisitos de seguridad necesarios para lograr la seguridad funcional requerida para los sistemas E/E/PE relacionados con la seguridad;

- utiliza los niveles de integridad de seguridad para especificar el nivel objetivo de integridad de seguridad para las funciones de seguridad que deben realizar los sistemas E/E/PE relacionados con la seguridad;

- adopta un planteamiento basado en el riesgo para determinar los requisitos de los niveles de integridad de seguridad;

---

1) PES del inglés: Programmable Electronic Systems.

- fija los objetivos cuantitativos para las medidas de fallo de los sistemas E/E/PE relacionados con la seguridad que tienen relación con los niveles de integridad de seguridad;

- fija un límite inferior para las medidas de fallo, en el caso de un modo de fallo peligroso, este límite podrá exigirse para un sistema E/E/PE relacionado con la seguridad único, en el caso de un sistema E/E/PE relacionado con la seguridad funcionando:

  - en un modo de baja demanda, el límite inferior está fijado a una probabilidad media de fallo de 10^{-5} con el fin de que las funciones por las cuales el sistema ha sido diseñado sean realizadas cuando sean requeridas;

  - en un modo de funcionamiento continuo o de alta demanda, el límite inferior está fijado a una probabilidad de fallo peligroso de 10^{-9} por hora;

  NOTA – Un sistema E/E/PE relacionado con la seguridad único no implica necesariamente una arquitectura en un solo canal.

- adopta una amplia gama de principios, técnicas y medidas para la realización de la seguridad funcional de los sistemas E/E/PE relacionados con la seguridad, pero no utiliza el concepto de "libre de fallo" (seguridad intrínseca) que tiene un sentido particular cuando los modos de fallo están bien definidos y el nivel de complejidad es relativamente bajo. Este concepto ha sido considerado como inadecuado debido a la inmensa gama de complejidad de los sistemas E/E/PE relacionados con la seguridad que entran en el objeto y campo de aplicación de esta norma.

Seguridad funcional de los sistemas eléctricos/electrónicos/ electrónicos programables relacionados con la seguridad
Parte 1: Requisitos generales

1 OBJETO Y CAMPO DE APLICACIÓN

1.1 Esta norma internacional trata los aspectos a tener en consideración cuando se utilicen sistemas eléctricos/ electrónicos/electrónicos programables (E/E/PES) para ejecutar funciones de seguridad. Uno de los principales objetivos de esta norma internacional es permitir la elaboración de normas internacionales específicas a cada sector de aplicación por los comités técnicos responsables de los sectores correspondientes. Esto permitirá tener en cuenta el conjunto de los factores pertinentes para cada aplicación, y de responder a las necesidades específicas de cada uno de estos sectores. Otro de los objetivos perseguidos por esta norma internacional es permitir el desarrollo de sistemas E/E/PE relacionados con la seguridad en ausencia eventual de normas internacionales para este sector de aplicación.

1.2 En particular, esta norma:

a) Se aplica a los sistemas relacionados con la seguridad cuando uno o más de estos sistemas incorpora dispositivos eléctricos/electrónicos/electrónicos programables.

NOTA 1 – En lo referente a los sistemas E/E/PE relacionados con la seguridad de baja complejidad, ciertos requisitos descritos en esta norma pueden no ser necesarios, y es posible que estén exentos de la conformidad con dichos requisitos (véase el apartado 4.2, y la definición de un sistema E/E/PE relacionado con la seguridad de baja complejidad en el apartado 3.4.4 de la Norma CEI 61508-4.

NOTA 2 – Aunque una persona puede formar parte de un sistema relacionado con la seguridad (véase el apartado 3.4.1 de la Norma CEI 61508-4), los requisitos sobre el factor humano en el diseño de los sistemas E/E/PE relacionados con la seguridad no se detallan en esta norma.

b) Está genéricamente basada y es aplicable a cualquier sistema E/E/PE relacionado con la seguridad[1)] sin consideración de su objeto y campo de aplicación.

c) Engloba los riesgos potenciales debidos a los fallos de las funciones a desempeñar por los sistemas E/E/PE relacionados con la seguridad, estos últimos siendo bien distintos de los riesgos que se desprenden del equipo E/E/PE (por ejemplo descargas eléctricas, etc.).

d) No engloba los sistemas E/E/PE donde:

- un sistema E/E/PE único es capaz de proporcionar la reducción del riesgo necesaria; y
- la integridad de seguridad, del sistema E/E/PE, exigida es menor que la especificada para el nivel 1 de integridad de seguridad (el nivel de integridad de seguridad más bajo de esta norma).

e) Trata más en particular los sistemas E/E/PE relacionados con la seguridad en los que una fallo podría tener un impacto sobre la seguridad de las personas y/o el entorno; sin embargo, se reconoce que los fallos pueden provocar serias consecuencias económicas, y en tales casos, esta norma también podría utilizarse para especificar cualquier sistema utilizado para la protección de un equipo o producto.

NOTA – Véanse los apartados 3.1.1 y 7.3.1.2 de la Norma CEI 61508-4.

f) Considera los sistemas E/E/PE relacionados con la seguridad, los sistemas relacionados con la seguridad basados en otras tecnologías y los dispositivos externos de reducción de riesgo para que la definición de los requisitos de seguridad para los sistemas E/E/PE relacionados con la seguridad pueda determinarse de forma sistemática basándose en el riesgo.

---

1) Por extensión, los sistemas E/E/PE relacionados con la seguridad se denominarán “sistemas de seguridad E/E/PE” en los capítulos siguientes.

g) Utiliza un modelo del ciclo de vida de la seguridad global para tratar, de forma sistemática, las actividades a realizar para asegurar la seguridad funcional de los sistemas E/E/PE relacionados con la seguridad.

NOTA 3 – Las primeras fases del modelo del ciclo de vida de la seguridad global incluyen, necesariamente, el estudio de otras tecnologías (además de los sistemas E/E/PE relacionados con la seguridad) y los dispositivos externos de reducción de riesgo, de tal forma que las especificaciones de los requisitos de seguridad para los sistemas E/E/PE relacionados con la seguridad puedan determinarse de forma sistemática basándose en el riesgo.

NOTA 4 – Aunque el ciclo de vida de la seguridad global principalmente concierne a todos los sistema E/E/PE relacionados con la seguridad, también puede servir de marco técnico para el estudio de cualquier sistema relacionado con la seguridad, independientemente de la tecnología empleada por ese sistema (por ejemplo mecánica, hidráulica o neumática).

h) No especifica los niveles de integridad de seguridad exigidos para aplicaciones sectoriales (estos niveles se deben basar en informaciones detalladas y en un buen conocimiento del sector de aplicación). Los comités técnicos responsables de los sectores de aplicación específicos deben indicar, cuando sea necesario, el nivel de integridad de seguridad en sus normas sectoriales.

i) Proporciona los requisitos generales para los sistemas E/E/PE relacionados con la seguridad que no se cubren por una norma sectorial.

j) No cubre las precauciones que pueden ser necesarias para evitar que las personas no autorizadas dañen, y/o produzcan una actividad que afecte a la seguridad funcional de los sistemas E/E/PE relacionados con la seguridad.

1.3 Esta parte de la Norma CEI 61508 define los requisitos generales que se aplican a todas las otras partes. Las otras partes de la Norma CEI 61508 tratan temas más específicos:

– las partes 2 y 3 proporcionan los requisitos suplementarios y específicos para los sistemas E/E/PE relacionados con la seguridad [para el hardware (soporte físico) y el software (soporte lógico)][1)];

– la parte 4 proporciona las definiciones y abreviaturas que se utilizan a lo largo de esta norma;

– la parte 5 proporciona las directrices para la puesta en marcha de la determinación de los niveles de integridad de seguridad, definidos en la parte 1, presentando ejemplos de métodos;

– la parte 6 proporciona las directrices para la aplicación de las partes 2 y 3;

– la parte 7 contiene una presentación de técnicas y de medidas.

1.4 Las partes 1, 2, 3 y 4 de esta norma son publicaciones básicas de seguridad, aunque este estado no sea aplicable en el contexto de los sistemas E/E/PE de baja complejidad relacionados con la seguridad (véase el apartado 3.4.4 de la parte 4). Como publicaciones básicas de seguridad, estas publicaciones son previstas para utilizarse por los comités técnicos para la preparación de normas de acuerdo con los principios contenidos en la Guía CEI 104 y la Guía ISO/CEI 51. Las partes 1, 2, 3 y 4 también están destinadas a utilizarse como publicaciones autónomas.

Una de las responsabilidades de un comité técnico es, en la medida lo posible, utilizar las publicaciones básicas de seguridad para la preparación de sus publicaciones. En este contexto, los requisitos, los métodos de ensayo o las condiciones de ensayo de esta publicación básica de seguridad, sólo se aplican si se indica específicamente o se incluyen en las publicaciones preparadas por estos comités técnicos.

NOTA – En los Estados Unidos de América y en Canadá, las normas nacionales existentes de seguridad de procesos, basadas en la Norma CEI 61508 (por ejemplo la Norma ANSI/ISA S84.01:1996), (véase la referencia [8] en el anexo C) se pueden aplicar en el sector de procesos, en lugar de la Norma CEI 61508, y hasta que las normas internacionales relativas a la aplicación de la Norma CEI 61508 en el sector de procesos sean publicadas.

1) hardware = soporte físico;
software = soporte lógico.

1.5 La figura 1 muestra la estructura general de las partes de la 1 a la 7 de la Norma CEI 61508 e indica el papel que la Norma CEI 61508-1 juega en el logro de la seguridad funcional para los sistemas E/E/PE relacionados con la seguridad.

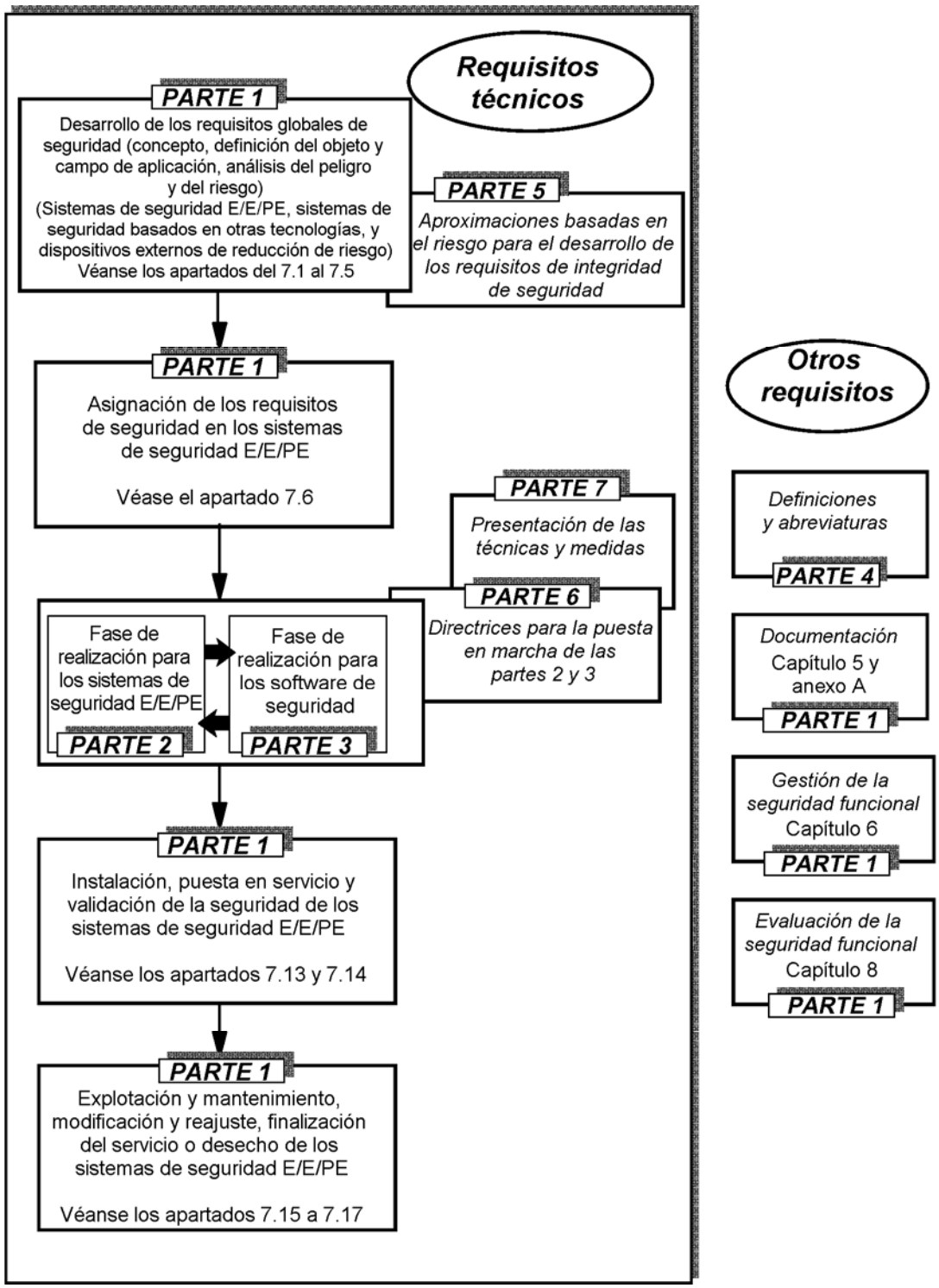


Fig. 1 – Estructura general de esta norma

2 NORMAS PARA CONSULTA

Las normas que a continuación se relacionan contienen disposiciones válidas para esta norma internacional. En el momento de la publicación las ediciones indicadas estaban en vigor. Toda norma está sujeta a revisión por lo que las partes que basen sus acuerdos en esta norma internacional deben estudiar la posibilidad de aplicar la edición más reciente de las normas indicadas a continuación. Los miembros de CEI y de ISO poseen el registro de las normas internacionales en vigor en cada momento.

Guía ISO/CEI 51:1990 – *Directrices para incluir en las normas los aspectos relacionados con la seguridad.*

Guía CEI 104:1997 – *Elaboración de las publicaciones de seguridad y utilización de las publicaciones fundamentales de seguridad y de las publicaciones de grupos de seguridad.*

CEI 61508-2:2000 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 2: Requisitos para los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad.*

CEI 61508-3:1998 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 3: Requisitos del software (soporte lógico).*

CEI 61508-4:1998 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 4: Definiciones y abreviaturas.*

CEI 61508-5:1998 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 5: Ejemplos de métodos de determinación de los niveles de integridad de seguridad.*

CEI 61508-6:2000 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad .Parte 6: Directrices para la aplicación de las Normas CEI 61508-2 y CEI 61508-3.*

CEI 61508-7:2000 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 7: Presentación de técnicas y medidas.*

3 DEFINICIONES Y ABREVIATURAS

Las definiciones y abreviaturas utilizadas en esta parte de la Norma CEI 61508 se encuentran en la Norma CEI 61508-4.

4 CONFORMIDAD CON ESTA NORMA

4.1 Para cumplir con esta norma, se debe demostrar que los requisitos se han cumplido para el criterio requerido especificado (por ejemplo, el nivel de integridad de seguridad), y que todos los objetivos se logran para cada capítulo o apartado.

NOTA – Generalmente no es posible elegir cada factor que determina el nivel al que un requisito debe satisfacerse (grado de rigor). La elección dependerá de un cierto número de factores, que pueden depender del conjunto de las fases y actividades específicas del ciclo de vida de la seguridad del software o de los sistemas E/E/PE. Estos factores incluyen:

- la naturaleza de los peligros;
- la reducción de los riesgos y de las consecuencias;
- el nivel de integridad de seguridad;
- el tipo de tecnología utilizado;
- el tamaño de los sistemas;
- el número de equipos implicados;
- la distribución física;
- la originalidad del diseño.

4.2 Esta norma especifica los requisitos para los sistemas de seguridad E/E/PE y se ha desarrollado para cubrir todos los niveles de complejidad posibles de estos sistemas. Sin embargo, para los sistemas de seguridad E/E/PE de baja complejidad (véase el apartado 3.4.4 de la Norma CEI 61508-4) cuando exista una sólida experiencia en el terreno que aporte la confianza necesaria para asegurar que la integridad de seguridad requerida se puede realizar, son posibles las opciones siguientes:

– en las normas de los sectores de aplicación aplicando los requisitos de la Norma CEI 61508-1 a la CEI 61508-7, ciertos requisitos de esta norma pueden no ser necesarios, y se acepta que esté exenta de la conformidad con estos requisitos;

– si esta norma se utiliza directamente en los casos en los que no existe norma internacional para ese sector de aplicación, ciertos requisitos especificados en esta norma pueden no ser necesarios y la exención de la conformidad con estos requisitos se acepta a condición que sea debidamente justificada.

4.3 Las normas por sector de aplicación para los sistemas de seguridad E/E/PE desarrollados en el marco de esta norma deben tener en cuenta los requisitos de las Guías ISO/CEI 51 y CEI 104.

5 DOCUMENTACIÓN

5.1 Objetivos

5.1.1 El primer objetivo de los requisitos de este capítulo es especificar la información necesaria que debe documentarse para que todas las fases del ciclo de vida global del sistema E/E/PE y del software puedan ejecutarse eficazmente.

5.1.2 El segundo objetivo de los requisitos de este capítulo es especificar la información necesaria que debe documentarse para que las actividades de gestión de la seguridad funcional (véase el capítulo 6), de verificación (véase el apartado 7.18) y de evaluación de la seguridad funcional (véase el capítulo 8) puedan ejecutarse eficazmente.

NOTA 1 – Los requisitos de documentación de esta norma se refieren, esencialmente, a la información más que a los documentos físicos. La información puede que no forme parte de ningún documento, excepto si se indica explícitamente en el apartado.

NOTA 2 – La documentación puede estar disponible bajo diferentes formas (por ejemplo en papel, película o cualquier soporte que pueda presentarse en pantalla).

NOTA 3 – Véase el anexo A para los ejemplos de la estructura de la documentación.

NOTA 4 – Véase también la referencia [4] en el anexo C.

5.2 Requisitos

5.2.1 Para cada fase realizada del ciclo de vida, de la seguridad global del sistema E/E/PE y del software, la documentación debe contener la información necesaria y suficiente para la realización eficaz de las fases siguientes y de las actividades de verificación.

NOTA – Lo que se entiende por “información suficiente” depende de un cierto número de factores, entre ellos, la complejidad y el tamaño del sistema de seguridad E/E/PE y los requisitos relacionados con la aplicación específica.

5.2.2 La documentación debe contener la información necesaria y suficiente para la gestión de la seguridad funcional (capítulo 6).

NOTA – Véanse las notas del apartado 5.1.2.

5.2.3 La documentación debe contener la información necesaria y suficiente para la implementación de la evaluación de la seguridad funcional, así como la información y los resultados de cualquier evaluación de la seguridad funcional.

NOTA – Véanse las notas del apartado 5.1.2.

5.2.4 Excepto justificación en contra dada en la planificación de la seguridad funcional o excepto especificación contraria en la norma de aplicación sectorial, la información a documentar debe ser la mencionada en varios capítulos de esta norma.

5.2.5 La disponibilidad de la documentación debe ser suficiente para realizar las actividades de acuerdo con los capítulos de esta norma.

NOTA – La información necesaria para llevar a cabo una actividad determinada, requerida en esta norma, solamente será necesaria para las partes implicadas.

5.2.6 La documentación debe:

– ser precisa y concisa;

– ser fácil de comprender por las personas que lo deben utilizar;

– corresponder con sus objetivos;

– ser accesible y actualizable.

5.2.7 La documentación o los conjuntos de informaciones deben tener unos títulos o nombres indicando el objeto y el campo de aplicación de sus contenidos, y poseer un sistema de índice que permita un acceso rápido a las informaciones descritas en esta norma.

5.2.8 La estructura de la documentación puede tener en cuenta los procedimientos de la empresa y los hábitos de trabajo de los sectores de aplicación específicos.

5.2.9 Los documentos o conjuntos de informaciones deben tener un índice de revisión (números de versión) que permitan identificar las diferentes versiones de un mismo documento.

5.2.10 Los documentos o conjuntos de informaciones se deben estructurar de forma que permita buscar la información pertinente. Debe ser posible identificar la última revisión (versión) de un documento o de un conjunto de informaciones.

NOTA – La organización práctica de la información será función de un cierto número de factores, como la dimensión del sistema, su complejidad o los requisitos de organización.

5.2.11 Todos los documentos pertinentes deben ser objeto de revisiones, de modificaciones, de repasos y aprobaciones, en el marco de un plan apropiado de control de los documentos.

NOTA – Cuando se utilizan herramientas de producción automática de documentación, pueden ser necesarios unos procedimientos especiales para asegurar que se toman las medidas eficaces para la gestión de las versiones o de otros aspectos del control de los documentos.

6 GESTIÓN DE LA SEGURIDAD FUNCIONAL

6.1 Objetivos

6.1.1 El primer objetivo de los requisitos de este capítulo es especificar las actividades técnicas y de gestión que será necesario realizar a lo largo de las fases del ciclo de vida global del software y sistemas E/E/PE para lograr la seguridad funcional requerida en los sistemas de seguridad E/E/PE.

6.1.2 El segundo objetivo de los requisitos de este capítulo es especificar las responsabilidades de las personas, servicios y organización responsables para cada fase del ciclo de vida global del software y sistemas E/E/PE o para las actividades incluidas en una fase.

NOTA – Las medidas de organización tratadas en este capítulo permiten la implantación eficaz de los requisitos técnicos y tiene por único objetivo la realización y el mantenimiento de la seguridad funcional de los sistemas de seguridad E/E/PE. Los requisitos técnicos necesarios para mantener la seguridad funcional normalmente deben especificarse en una parte de la documentación dada por el suministrador del sistema de seguridad E/E/PE.

6.2 Requisitos

6.2.1 Los organismos o los individuos que tienen una responsabilidad global para una o varias fases del ciclo de vida de la seguridad global del software o sistemas E/E/PE, deben, con respecto a las fases para las que tienen una responsabilidad global, especificar todas las actividades técnicas y de gestión que son necesarias para asegurar que los sistemas de seguridad E/E/PE realicen y mantengan la seguridad funcional requerida. En particular, conviene que se tengan en consideración los elementos siguientes:

a) Política y la estrategia para lograr la seguridad funcional, junto con los medios para evaluar su realización, y los medios de difusión en la organización de esta información y que permitan asegurar una cultura de seguridad del trabajo.

b) Identificación de las personas, servicios y otras organizaciones que son responsables de la ejecución y de la revisión de las fases apropiadas del ciclo de vida global de la seguridad, del software y sistemas E/E/PE (incluyendo, cuando sea útil, los organismos de aprobación o los organismos reguladores de la seguridad).

c) Fases del ciclo de vida de la seguridad global del software o sistemas E/E/PE antes de ser aplicados.

d) Forma en la que la información debe estructurarse y la extensión de la información antes de documentarse (véase el capítulo 5).

e) Medidas elegidas y técnicas utilizadas para cumplir los requisitos de un capítulo o un apartado determinado (véanse las Normas CEI 61508-2, CEI 61508-3 y CEI 61508-6).

f) Actividades de evaluación de la seguridad funcional (véase el capítulo 8).

g) Procedimientos para asegurar rápidamente un seguimiento y una resolución satisfactoria de las recomendaciones relacionadas con los sistemas de seguridad E/E/PE, provenientes de:

   – análisis del peligro y del riesgo (véase al apartado 7.4);

   – evaluación de la seguridad funcional (véase el capítulo 8);

   – actividades de verificación (véase el apartado 7.18);

   – actividades de validación (véanse los apartados 7.8 y 7.14);

   – gestión de la configuración [véanse los apartados 6.2.1 punto o), 7.16 y las Normas CEI 61508-2 y CEI 61508-3].

h) Procedimientos que permiten asegurar que las personas apropiadas, implicadas en cualquiera de las actividades del ciclo de vida de la seguridad global del software o sistemas E/E/PE, son competentes para realizar las actividades de las que son responsables, en particular, conviene especificar lo siguiente:

   – formación del personal para el diagnóstico y la reparación de los fallos y para el ensayo del sistema;

   – formación del personal de explotación;

   – formación continua del personal a intervalos periódicos.

   NOTA 1 – El anexo B proporciona las directrices sobre los requisitos de competencia de las personas implicadas en cualquiera de las actividades del ciclo de vida de la seguridad global del software o sistemas E/E/PE.

i) Procedimientos para que los incidentes peligrosos (o los incidentes que potencialmente pueden crear un peligro) sean analizados, y que se hagan recomendaciones para minimizar la probabilidad de reaparición.

j) Procedimientos de análisis de las prestaciones en explotación y en mantenimiento. En particular los procedimientos para:

   – reconocer los fallos sistemáticos que pueden comprometer la seguridad funcional, incluyendo los procedimientos utilizados durante el mantenimiento sistemático que permite detectar los fallos cíclicos;

– evaluar si las tasas de demanda y las tasas de fallo durante la explotación y el mantenimiento están de acuerdo con las hipótesis hechas durante el diseño del sistema.

k) Requisitos para las auditorías periódicas de la seguridad funcional, de acuerdo con este apartado, que incluyen:

– frecuencia de las auditorías de seguridad funcional;

– consideración del nivel de independencia necesario para los responsables de las auditorías;

– actividades de documentación y de seguimiento.

l) Los procedimientos para iniciar las modificaciones en los sistemas de seguridad (véase el apartado 7.16.2.2).

m) El procedimiento de aprobación y autorización requerido para las modificaciones.

n) Los procedimientos para mantener información precisa sobre los peligros potenciales y los sistemas de seguridad.

o) Los procedimientos para la gestión de configuración de los sistemas de seguridad E/E/PE durante las fases del ciclo de vida de la seguridad global del software y sistemas E/E/PE; en particular, conviene especificar lo siguiente:

– etapa en la que el control formal de la configuración se implemente;

– procedimientos antes de utilizarse para identificar de forma única cada parte constitutiva de un elemento (hardware o software);

– procedimientos para evitar que los elementos no autorizados entren en servicio.

NOTA 2 – Para más detalles sobre la configuración, véanse las referencias [6] y [7] del anexo C.

p) Cuando sea pertinente, las disposiciones de formación y de información para los servicios de emergencia.

6.2.2 Las actividades especificadas como resultado del apartado 6.2.1 deben implementarse y su progreso debe vigilarse.

6.2.3 Los organismos competentes deben revisar formalmente los requisitos desarrollados resultantes del apartado 6.2.1 y debe llegarse a un acuerdo.

6.2.4 Debe informarse de las responsabilidades asignadas a cualquier persona designada como responsable para la gestión de las actividades de seguridad funcional.

6.2.5 Los suministradores, que ofrecen productos o servicios a una organización que tenga una responsabilidad global para uno o varias de las fases del ciclo de vida de la seguridad global del software o sistemas E/E/PE (véase el apartado 6.2.1), deben expedir sus productos o servicios como se prescribe por dicha organización y deben poseer un sistema de gestión de la calidad apropiado.

7 REQUISITOS RELATIVOS AL CICLO DE VIDA DE LA SEGURIDAD GLOBAL

7.1 Generalidades

7.1.1 Introducción

7.1.1.1 Esta norma ha elegido un ciclo de vida de la seguridad global (véase la figura 2) como marco técnico para tratar de forma sistemática todas las actividades necesarias para lograr el nivel de integridad de seguridad requerido por los sistemas E/E/PE relacionados con la seguridad.

NOTA – Para la declaración de conformidad con esta norma, conviene utilizar como base el ciclo de vida de seguridad global, pero puede utilizarse un ciclo de vida de la seguridad global diferente al que se describe en la figura 2, en la medida en que se cumplan los requisitos de cada capítulo de esta norma.

7.1.1.2 El ciclo de vida de la seguridad global engloba las siguientes medidas de reducción de riesgos:

– sistemas de seguridad E/E/PE;

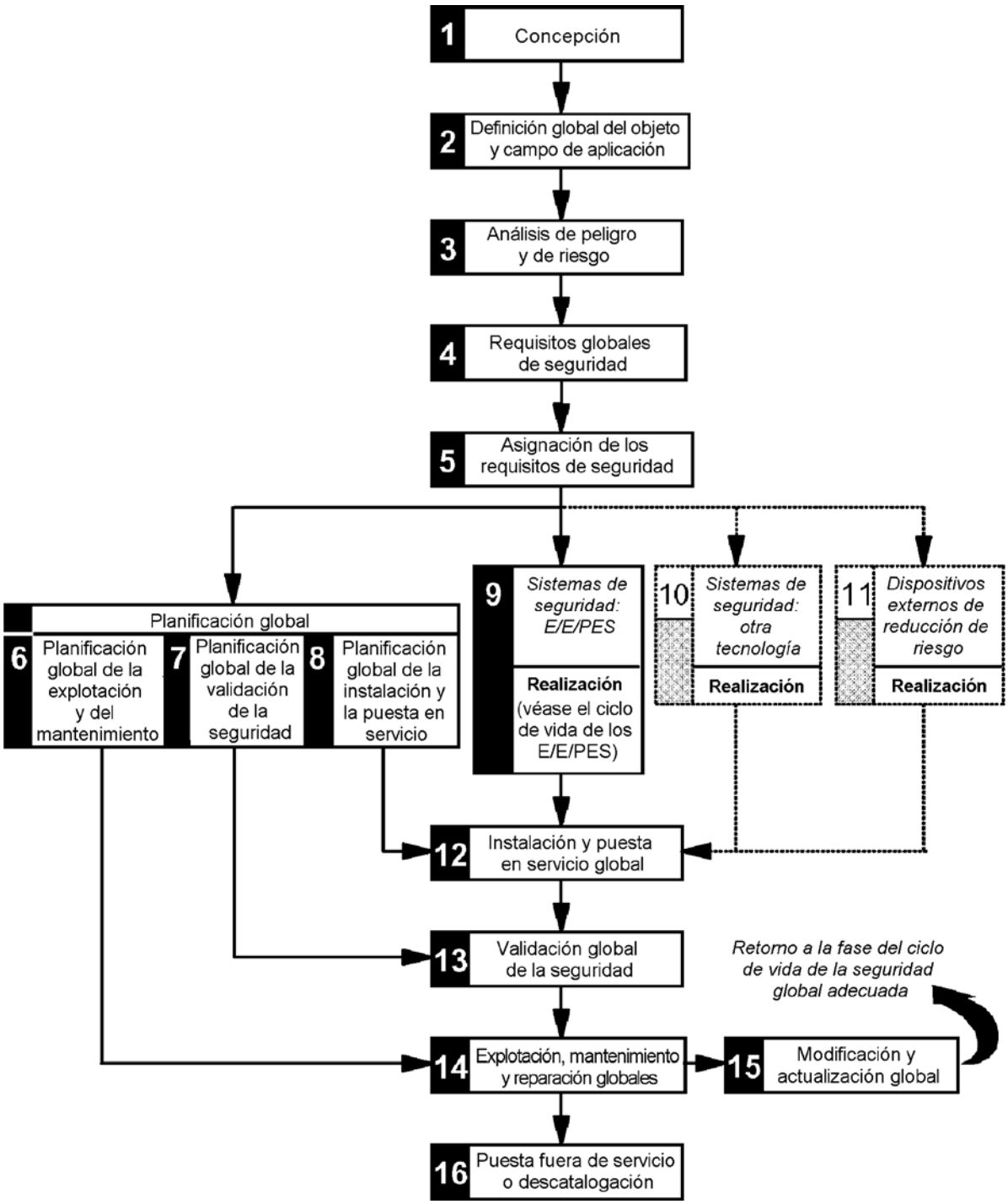
– sistemas de seguridad basados en otras tecnologías;

– dispositivos externos de reducción de riesgo.

7.1.1.3 La porción del ciclo de vida de la seguridad global que concierne a los sistemas de seguridad E/E/PE se muestra de forma detallada en la figura 3. Se llamará "ciclo de vida de la seguridad del sistema E/E/PE" y forma el marco técnico para la Norma CEI 61508-2. El ciclo de vida de la seguridad del software se muestra en la figura 4 y forma el marco técnico para la Norma CEI 61508-3. La relación entre el ciclo de vida de la seguridad global y los ciclos de vida de la seguridad del software y de los sistemas E/E/PE, para los sistemas relacionados con la seguridad, se muestra en la figura 5.

7.1.1.4 Las figuras del ciclo de vida de la seguridad global del software y de los E/E/PES (figuras de la 2 a la 4) son vistas simplificadas de la realidad y no presentan todas las iteraciones correspondientes a las fases particulares o entre ciertas fases. Sin embargo, la iteración es una parte esencial y vital de un desarrollo que utiliza los ciclos de vida de la seguridad globales de los E/E/PES y del software.

7.1.1.5 Las actividades relativas a la gestión de la seguridad funcional (capítulo 6), a la verificación (apartado 7.18) y a la evaluación de la seguridad funcional (capítulo 8) no se representan en los ciclos de vida de la seguridad globales de los E/E/PES o del software. Esta elección se ha hecho para reducir la complejidad de las figuras del ciclo de vida de la seguridad global del software y de los E/E/PES. Estas actividades necesitarán aplicarse a todas las fases apropiadas de los ciclos de vida de la seguridad globales de los E/E/PES y del software.



NOTA 1 – Las actividades relativas a la ***verificación***, a la ***gestión de la seguridad funcional*** y a la ***evaluación de la seguridad funcional*** no se representan por razones de claridad, pero conciernen a todas las fases globales del ciclo de vida de la seguridad de los sistemas E/E/PE y del software.

NOTA 2 – Las fases representadas por las etapas 10 y 11 están fuera del objeto y campo de aplicación de esta norma.

NOTA 3 – Las Normas CEI 61508-2 y CEI 61508-3 tratan de la etapa 9 (realización) pero también tratan, cuando sea oportuno, los aspectos de la electrónica programable (hardware y software) de las etapas 13, 14 y 15.

Fig. 2 – Ciclo de vida de la seguridad global

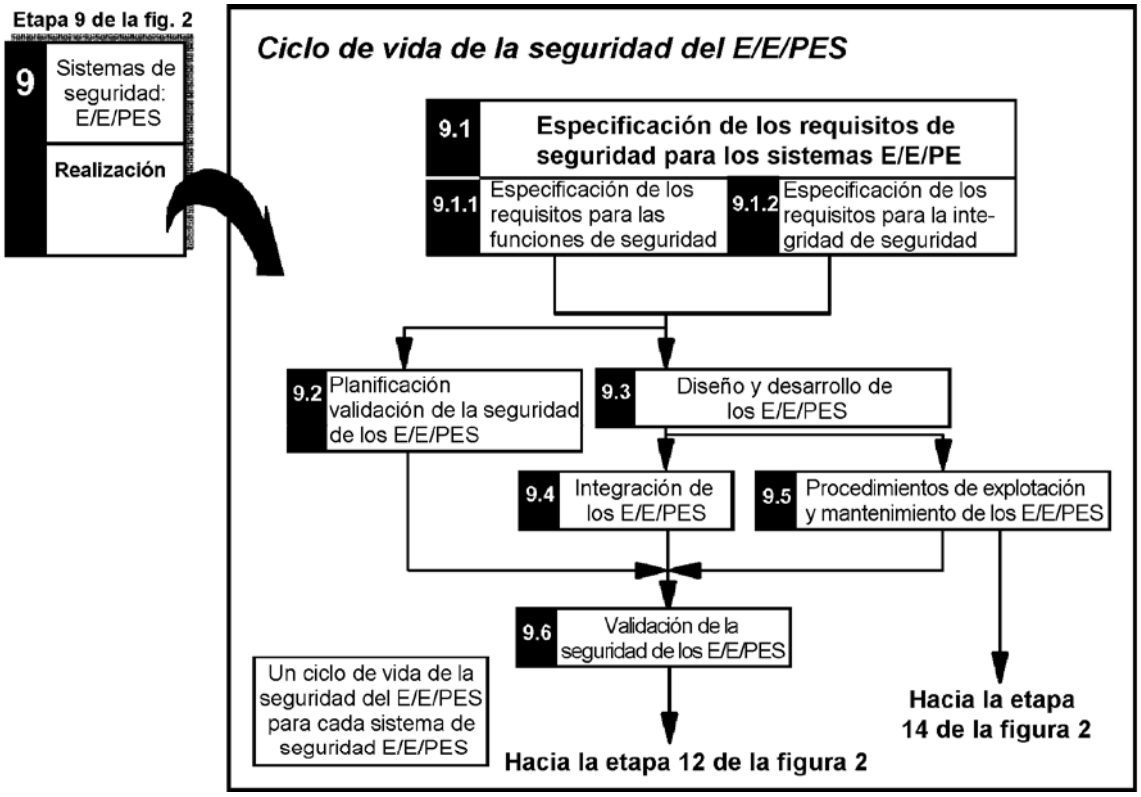


Fig. 3 – Ciclo de vida de la seguridad del sistema E/E/PE (en la fase de realización)

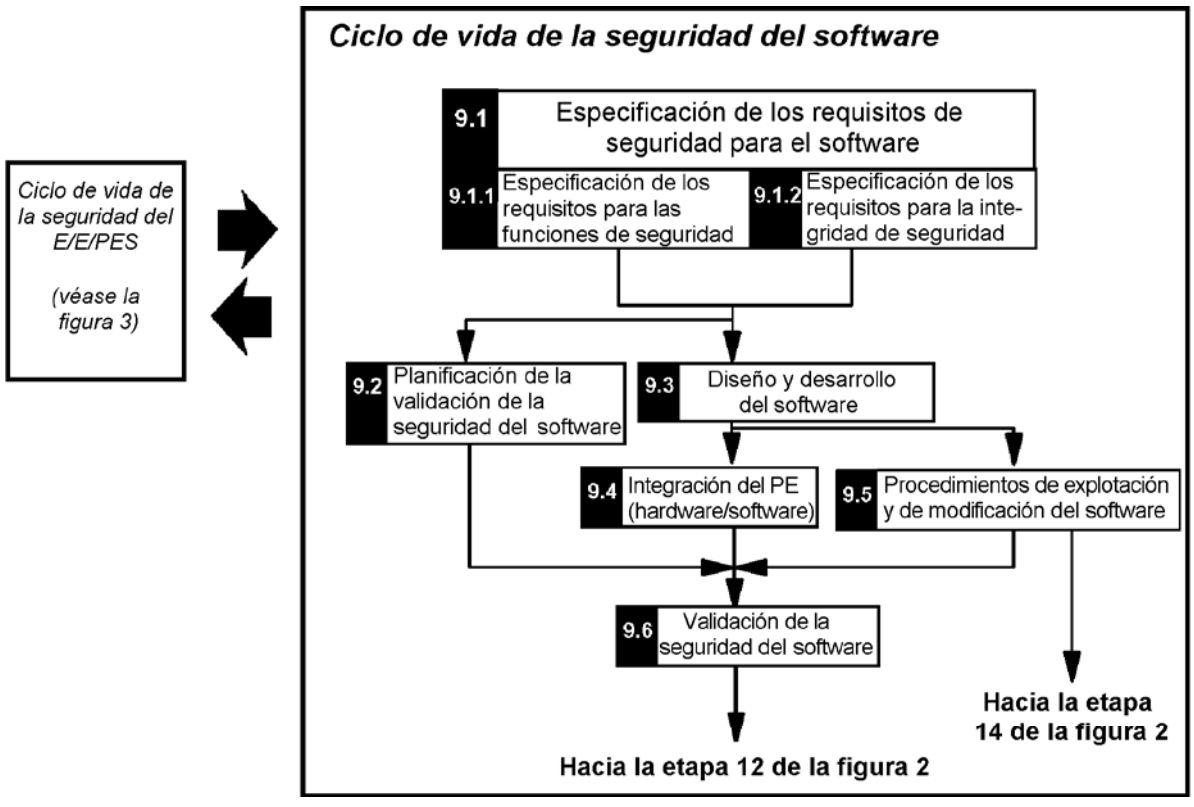


Fig. 4 – Ciclo de vida de la seguridad del software (en la fase de realización)

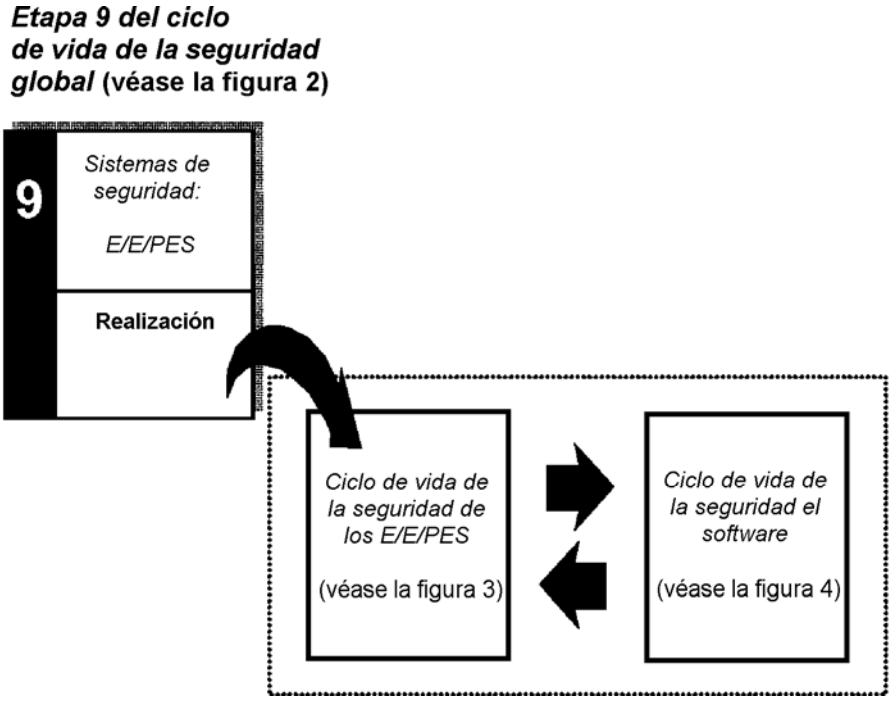


Fig. 5 – Relaciones entre el ciclo de vida de la seguridad global y los ciclos de vida de la seguridad de los E/E/PES y del software

7.1.2 Objetivos y requisitos: generalidades

7.1.2.1 Los objetivos y los requisitos para las fases del ciclo de vida de la seguridad global se describen en los apartados del 7.2 al 7.17. Los objetivos y los requisitos para las fases del ciclo de vida de la seguridad de los E/E/PES y del software se describen respectivamente en las Normas CEI 61508-2 y CEI 61508-3.

NOTA – Los apartados del 7.2 al 7.17 se relacionan con las "etapas" (fases) específicas de la figura 2. La etapa correspondiente se precisa en una nota al comienzo de los apartados.

7.1.2.2 Para todas las fases del ciclo de vida de la seguridad global, la tabla 1 indica:

– los objetivos a alcanzar;

– el objeto y el campo de aplicación de la fase;

– la referencia del apartado que contiene los requisitos;

– los datos de entrada exigidos por la fase;

– los datos de salida exigidos para cumplir con los requisitos.

Tabla 1
Ciclo de vida de la seguridad global: vista de conjunto

Fase del ciclo de vida de la seguridad		Objetivos	Campo de aplicación	Requisitos (apartado)	Entradas	Salidas
Número de etapa de la figura 2	**Título**					
1	**Diseño**	7.2.1: Desarrollar un nivel de comprensión del EUC (equipo bajo control, en adelante EUC) y su entorno (físico, jurídico, etc.) suficiente para permitir a las otras actividades del ciclo de vida de la seguridad desarrollarse de forma satisfactoria	El EUC y su entorno (físico, jurídico, etc.)	7.2.2	Cualquier información apropiada necesaria para cumplir los requisitos de este apartado	La información obtenida por los apartados del 7.2.2.1 al 7.2.2.6
2	**Definición global del objeto y campo de aplicación**	7.3.1: Determinar los límites del EUC y del sistema de control del EUC; Especificar el campo de aplicación del análisis de peligro y de riesgo (por ejemplo los procesos peligrosos, los peligros relacionados con el entorno, etc.)	El EUC y su entorno	7.3.2	La información obtenida en los apartados del 7.2.2.1 al 7.2.2.6	La información obtenida por los apartados del 7.3.2.1 al 7.3.2.5
3	**Análisis de peligro y de riesgo**	7.4.1: Determinar los peligros y los eventos peligrosos del EUC y del sistema de control del EUC (en todos los modos de explotación), para todas las situaciones razonablemente previsibles, incluyendo las de fallo y de mala utilización; Determinar las secuencias de los eventos que provocan eventos peligrosos determinados; Determinar los riesgos del EUC asociados a eventos peligrosos determinados	El campo de aplicación dependerá de la fase alcanzada en los ciclos de vida globales de la seguridad de los sistemas E/E/PE y del software (ya que puede ser necesario realizar más de un análisis de peligro y de riesgo). Para el análisis preliminar de peligro y de riesgo, el campo de aplicación incluye el EUC, el sistema de control del EUC y los factores humanos	7.4.2	La información obtenida en los apartados del 7.3.2.1 al 7.3.2.5	La descripción y la información relativa al análisis de peligro y de riesgo
4	**Requisitos globales de seguridad**	7.5.1: Desarrollar la especificación para requisitos globales de seguridad, en términos de requisitos de funciones de seguridad y de requisitos de integridad de seguridad, para los sistemas de seguridad E/E/PE, los sistemas de seguridad basados en otra tecnología y los dispositivos externos de reducción de riesgo, con el fin de alcanzar la seguridad funcional requerida	El EUC, el sistema de control del EUC y los factores humanos	7.5.2	La descripción y la información relativa al análisis de peligro y de riesgo	Especificación para los requisitos globales de seguridad en términos de requisitos de funciones de seguridad y de requisitos de integridad de seguridad
5	**Asignación de los requisitos de seguridad**	7.6.1: Permitir las funciones de seguridad, que se indican en la especificación para los requisitos globales de seguridad (conjunto de los requisitos de las funciones de seguridad y los requisitos de integridad de seguridad), a los sistemas de seguridad E/E/PE designados, a los sistemas de seguridad basados en otra tecnología y a los dispositivos de reducción de riesgo; Permitir un nivel de integridad de seguridad a cada función de seguridad	El EUC, el sistema de control del EUC y los factores humanos	7.6.2	Especificación para los requisitos globales de seguridad en términos de requisitos de funciones de seguridad y de requisitos de integridad de seguridad	Información y resultados de la asignación de los requisitos de seguridad

(Continúa)

Tabla 1 *(Continuación)*
Ciclo de vida de la seguridad global: vista de conjunto

Fase del ciclo de vida de la seguridad		Objetivos	Campo de aplicación	Requisitos (apartado)	Entradas	Salidas
Número de etapa de la figura 2	**Título**					
6	**Planificación global de la explotación y del mantenimiento**	7.7.1: Desarrollar un plan de explotación y de mantenimiento de los sistemas de seguridad E/E/PE, para lograr que la seguridad funcional requerida se mantiene durante la explotación y el mantenimiento	El EUC, el sistema de control del EUC y los factores humanos; los sistemas de seguridad E/E/PE	7.7.2	Especificación para los requisitos globales de seguridad en términos de requisitos de las funciones de seguridad y los requisitos de integridad de seguridad	Plan de explotación y de mantenimiento de los sistemas de seguridad E/E/PE
7	**Planificación global de la validación de la seguridad**	7.8.1: Desarrollar un plan para facilitar la validación global de la seguridad de los sistemas de seguridad E/E/PE	El EUC, el sistema de control del EUC y los factores humanos; los sistemas de seguridad E/E/PE	7.8.2	Especificación para los requisitos globales de seguridad en términos de requisitos de las funciones de seguridad y los requisitos de integridad de seguridad	Plan para facilitar la validación de los sistemas de seguridad E/E/PE
8	**Planificación global de la instalación y la puesta en marcha**	7.9.1: Desarrollar un plan para que la instalación de los sistemas de seguridad E/E/PE sean controlados, asegurando que la seguridad funcional requerida se alcanza; Desarrollar un plan para que la puesta en marcha de los sistemas de seguridad E/E/PE sean controlados, asegurando que la seguridad funcional requerida se alcanza	El EUC y el sistema de control del EUC los sistemas de seguridad E/E/PE	7.9.2	Especificación para los requisitos globales de seguridad en términos de requisitos de las funciones de seguridad y los requisitos de integridad de seguridad	Plan para la instalación de los sistemas de seguridad E/E/PE; Plan para la puesta en marcha de los sistemas de seguridad E/E/PE
9	**Sistemas de seguridad E/E/PE: realización**	7.10.1 y las partes 2 y 3: Crear unos sistemas de seguridad E/E/PE de acuerdo con la especificación para los requisitos de seguridad de los E/E/PES (incluyendo la especificación para los requisitos de integridad de seguridad de los E/E/PES).	Los sistemas de seguridad E/E/PE	7.10.2, CEI 61508-2 y CEI 61508-3	Especificación para los requisitos de seguridad de los E/E/PES	Confirmación que cada sistema de seguridad E/E/PE alcance la especificación de los requisitos de seguridad de los E/E/PES
10	**Sistemas de seguridad basados en otra tecnología: realización**	7.11.1: Crear unos sistemas de seguridad basado en otra tecnología que cumplan los requisitos de las funciones de seguridad y los requisitos de integridad de seguridad especificados para estos sistemas (fuera del campo de aplicación de esta norma).	Los sistemas de seguridad basados en otra tecnología	7.11.2	Especificación de los requisitos para otra tecnología de la seguridad (fuera del campo de aplicación de esta norma y por lo tanto no examinada en profundidad)	Confirmación que cada sistema de seguridad basado en otra tecnología alcance los requisitos de seguridad de este sistema

(Continúa)

Tabla 1 *(Continuación)*
Ciclo de vida de la seguridad global: vista de conjunto

Fase del ciclo de vida de la seguridad		Objetivos	Campo de aplicación	Requisitos (apartado)	Entradas	Salidas
Número de etapa de la figura 2	**Título**					
11	**Dispositivos externos de reducción de riesgo: realización**	7.12.1: Crear unos dispositivos externos de reducción de riesgo que cumplan los requisitos de las funciones de seguridad y los requisitos de integridad de seguridad especificados para estos dispositivos (fuera del campo de aplicación de esta norma).	Los dispositivos externos de reducción de riesgo	7.12.2	Especificación de los requisitos para los dispositivos externos de reducción de riesgo (fuera del campo de aplicación de esta norma y por lo tanto no examinado en profundidad).	Confirmación que cada dispositivo externo de reducción de riesgo alcance los requisitos de seguridad para este dispositivo
12	**Instalación y puesta en servicio global**	7.13.1: Instalar los sistemas de seguridad E/E/PE; Poner en servicio los sistemas de seguridad E/E/PE	El EUC y el sistema de control del EUC; los sistemas de seguridad E/E/PE	7.13.2	Plan para la instalación de los sistemas de seguridad E/E/PE; Plan para la puesta en marcha de los sistemas de seguridad E/E/PE	Sistemas de seguridad E/E/PE completamente instalados; Sistemas de seguridad E/E/PE completamente puestos en servicio
13	**Validación global de la seguridad**	7.14.1: Validar el hecho que los sistemas de seguridad E/E/PE cumplen la especificación para los requisitos globales de seguridad sobre el plan de requisitos globales de las funciones de seguridad y de los requisitos globales de integridad de seguridad, teniendo en cuenta la asignación de los requisitos de seguridad, para los sistemas de seguridad, realizados de acuerdo con el apartado 7.6	El EUC y el sistema de control del EUC; los sistemas de seguridad E/E/PE	7.14.2	Plan de validación global de la seguridad para los sistemas de seguridad E/E/PE; Especificación para los requisitos globales de seguridad en términos de requisitos de las funciones de seguridad y de los requisitos de integridad de seguridad; Asignación de los requisitos de seguridad	Confirmación que todos los sistemas de seguridad E/E/PE cumplen la especificación para los requisitos globales de seguridad en términos de requisitos de las funciones de seguridad y de los requisitos de integridad de seguridad, teniendo en cuenta la asignación de los requisitos de seguridad para los sistemas de seguridad E/E/PE

(Continúa)

Tabla 1 *(Fin)*
Ciclo de vida de la seguridad global: vista de conjunto

Fase del ciclo de vida de la seguridad		Objetivos	Campo de aplicación	Requisitos (apartado)	Entradas	Salidas
Número de etapa de la figura 2	**Título**					
14	**Explotación, mantenimiento y reparación globales**	7.15.1: Explotar, mantener y reparar los sistemas de seguridad E/E/PE de forma que mantengan la seguridad funcional requerida	El EUC y el sistema de control del EUC; los sistemas de seguridad E/E/PE	7.15.2	Plan global de explotación y mantenimiento de los sistemas de seguridad E/E/PE	Realización permanente de la seguridad funcional requerida por los sistemas de seguridad E/E/PE; Documentación cronológica de la explotación, de la reparación y del mantenimiento de los sistemas de seguridad E/E/PE.
15	**Modificación y actualización globales**	7.16.1: Asegurar que la seguridad funcional para los sistemas de seguridad E/E/PE es apropiada, durante y después de la fase de modificación y actualización	El EUC y el sistema de control del EUC; los sistemas de seguridad E/E/PE	7.16.2	Demanda de modificación o actualización según los procedimientos de gestión de la seguridad funcional	Realización de la seguridad funcional requerida por los sistemas de seguridad E/E/PE, durante y después de la fase de modificación y actualización. Documentación cronológica de la explotación, de la reparación y del mantenimiento de los sistemas de seguridad E/E/PE
16	**Puesta fuera de servicio o descatalogación**	7.17.1: Asegurar que la seguridad funcional para los sistemas de seguridad E/E/PE es apropiada a las circunstancias durante y después de las actividades de puesta fuera de servicio o descatalogación	El EUC y el sistema de control del EUC; los sistemas de seguridad E/E/PE	7.17.2	Demanda de la puesta fuera de servicio o descatalogación según los procedimientos de gestión de la seguridad funcional	Realización de la seguridad funcional requerida por los sistemas de seguridad E/E/PE, durante y después de las actividades de puesta fuera de servicio o descatalogación; Documentación cronológica de las actividades de puesta fuera de servicio o descatalogación

7.1.3 Objetivos

7.1.3.1 El primer objetivo de los requisitos de este apartado es estructurar, de forma sistemática, las fases del ciclo de vida de la seguridad global que deben considerarse con el fin de realizar la seguridad funcional requerida de los sistemas de seguridad E/E/PE.

7.1.3.2 El segundo objetivo de los requisitos de este apartado es documentar las informaciones clave, relacionadas con la seguridad funcional de los sistemas de seguridad E/E/PE, a lo largo del ciclo de vida de la seguridad global.

NOTA – Véase el capítulo 5 del anexo A para la estructura de la documentación. La estructura de la documentación puede tener en cuenta los procedimientos de la empresa y los hábitos de trabajo de los sectores de aplicación específicos.

7.1.4 Requisitos

7.1.4.1 El ciclo de vida de la seguridad global que debe utilizarse como base para la declaración de conformidad de acuerdo con esta norma se especifica en la figura 2. Si se utiliza otro ciclo de vida de la seguridad global, debe especificarse durante la planificación de la seguridad funcional, y todos los objetivos y requisitos de cada capítulo o apartado de esta norma deben respetarse.

NOTA – El ciclo de vida de la seguridad del sistema E/E/PE y el ciclo de vida de la seguridad del software (que forman la fase de realización del ciclo de vida de la seguridad global) que deben utilizarse para la declaración de conformidad se especifican respectivamente en las Normas CEI 61508-2 y CEI 61508-3.

7.1.4.2 Los requisitos para la gestión de la seguridad funcional (véase el capítulo 6) deben llevarse en paralelo con las fases del ciclo de vida de la seguridad global.

7.1.4.3 Cada fase del ciclo de vida de la seguridad global debe aplicarse y deben respetarse los requisitos, en caso contrario debe justificarse.

7.1.4.4 Cada fase del ciclo de vida de la seguridad global debe dividirse en actividades elementales con la especificación del objeto y campo de aplicación, de las entradas y de las salidas para cada fase.

7.1.4.5 El campo de aplicación y las entradas de cada fase del ciclo de vida de la seguridad global deben ser como las especificadas en la tabla 1.

7.1.4.6 Excepto justificación en contra dada en la planificación de la seguridad funcional o excepto especificación en contra en la norma de aplicación sectorial, las salidas de cada fase del ciclo de vida de la seguridad global deben ser como las especificadas en la tabla 1.

7.1.4.7 Las salidas de cada fase del ciclo de vida de la seguridad global deben cumplir los objetivos y los requisitos específicos para cada fase (véanse los apartados del 7.2 al 7.17).

7.1.4.8 Los requisitos de verificación que deben respetarse para cada fase del ciclo de vida de la seguridad global se especifican en el apartado 7.18.

7.2 Concepción

NOTA – Esta fase corresponde a la etapa 1 de la figura 2.

7.2.1 Objetivo. El objetivo de los requisitos de este apartado es desarrollar un nivel de comprensión suficiente del EUC y de su entorno (físico, legal, etc.) para permitir conducir de forma satisfactoria las otras actividades del ciclo de vida de la seguridad.

7.2.2 Requisitos

7.2.2.1 Debe adquirirse un conocimiento profundo del EUC, de sus funciones de control requeridas y de su entorno físico.

7.2.2.2 Deben determinarse las fuentes potenciales de peligros.

7.2.2.3 Debe obtenerse información sobre los peligros determinados (toxicidad, condiciones explosivas, corrosión, reactividad, inflamabilidad, etc.)

7.2.2.4 Debe obtenerse la información sobre la legislación aplicable en materia de seguridad (nacional e internacional).

7.2.2.5 Deben considerarse los peligros debidos a las interacciones con otros EUC (instalados o antes de ser instalados) próximos al EUC.

7.2.2.6 La información y los resultados obtenidos por los apartados del 7.2.2.1 al 7.2.2.5 deben documentarse.

7.3 Definición global del objeto y campo de aplicación

NOTA – Esta fase corresponde a la etapa 2 de la figura 2.

7.3.1 Objetivos

7.3.1.1 El primer objetivo de los requisitos de este apartado es determinar los límites del EUC y del sistema de control del EUC.

7.3.1.2 El segundo objetivo de los requisitos de este apartado es especificar el campo de aplicación del análisis de peligro y de riesgo (por ejemplo los procesos peligrosos, los peligros relacionados con el entorno, etc.).

7.3.2 Requisitos

7.3.2.1 Deben especificarse el equipo físico, incluyendo el EUC y el sistema de control del EUC, que deben formar parte del campo de aplicación del análisis de peligro y de riesgo.

NOTA – Véanse las referencias [1] y [2] en el anexo C.

7.3.2.2 Deben especificarse los eventos exteriores que deben tenerse en cuenta en el análisis de peligro y de riesgo.

7.3.2.3 Deben especificarse los subsistemas que se asocian a los peligros.

7.3.2.4 El tipo de eventos inicializadores de accidentes que es necesario tener en consideración (por ejemplo los fallos de los componentes, los fallos del procedimiento, el error humano, los mecanismos de fallo dependiente que pueden originar secuencias de accidente) deben especificarse.

7.3.2.5 La información y los resultados obtenidos por los apartados del 7.3.2.1 al 7.3.2.4 deben documentarse.

7.4 Análisis de peligro y de riesgo

NOTA – Este apartado corresponde a la etapa 3 de la figura 2.

7.4.1 Objetivos

7.4.1.1 El primer objetivo de los requisitos de este apartado es determinar los peligros y los eventos peligrosos del EUC y del sistema de control del EUC (en cualquier modo de explotación), para todas las situaciones razonablemente previsibles, incluyendo las de fallo y las de mala utilización.

7.4.1.2 El segundo objetivo de los requisitos de este apartado es determinar las secuencias de eventos que conducen a eventos peligrosos determinados en el apartado 7.4.1.1.

7.4.1.3 El tercer objetivo de los requisitos de este apartado es determinar los riesgos del EUC asociados a los eventos peligrosos determinados en el apartado 7.4.1.1.

NOTA 1 – Este apartado es necesario para que los requisitos de seguridad de los sistemas de seguridad E/E/PE se basen sistemáticamente en una aproximación basada en el riesgo. Esto sólo puede hacerse considerando el EUC y el sistema de control del EUC.

NOTA 2 – En el caso de aplicaciones en donde se pueden hacer hipótesis válidas sobre los riesgos, los peligros potenciales, los eventos peligrosos y sus consecuencias, el análisis requerido en este apartado (y el apartado 7.5) se puede realizar por los redactores de las versiones de aplicación sectorial de esta norma, y puede incluirse en los requisitos gráficos simplificados. Unos ejemplos de estos métodos se proporcionan en los anexos D y E de la Norma CEI 61508-5.

7.4.2 Requisitos

7.4.2.1 Debe realizarse un análisis de peligro y de riesgo, que debe tener en cuenta la información que viene de la fase de definición global del objeto y campo de aplicación (véase el apartado 7.3). Si las decisiones, tomadas en etapas ulteriores de las fases del ciclo de vida de la seguridad global del E/E/PES o del software, pueden cambiar las bases sobre las que se tomaron las primeras decisiones, entonces debe llevarse a cabo un nuevo análisis de peligro y de riesgo.

NOTA 1 – Para más guías, véanse la referencia [1] y [2] en el anexo C.

NOTA 2 – Puede ser necesario realizar más de un análisis de peligro y de riesgo.

NOTA 3 – Como ejemplo ilustrando la necesidad de proseguir el análisis de peligro y de riesgo durante todo el ciclo de vida de la seguridad global, consideremos el análisis de un EUC que incorpora una válvula de seguridad. Un análisis de peligro y de riesgo puede determinar dos secuencias de eventos que incluyen respectivamente un fallo con la válvula cerrada y un fallo con la válvula abierta, provocando una situación peligrosa. Sin embargo, cuando el diseño detallado del sistema de control del EUC que controla la válvula se analiza, se puede descubrir un nuevo modo de fallo, válvula oscilante, que introduce una nueva secuencia de eventos que conducen a una situación peligrosa.

7.4.2.2 Debe tenerse en consideración la eliminación de los peligros.

NOTA – Aunque no está en el objeto y campo de aplicación de esta norma, es primordial que los peligros identificados sean eliminados en su raíz, por ejemplo por aplicación de los principios de seguridad intrínseca y la aplicación de las prácticas de buena ingeniería.

7.4.2.3 Los peligros y los eventos peligrosos del EUC y del sistema de control del EUC deben determinarse según todas las circunstancias razonablemente previsibles (incluyendo las condiciones de fallo y de mala utilización razonablemente previsible). Esto incluye cualquier problema relacionado con el factor humano, y debe prestarse una atención particular a los modos de explotación anormales o poco frecuentes del EUC.

NOTA – Para la mala utilización razonablemente previsible, véase el apartado 3.1.11 de la Norma CEI 61508-4.

7.4.2.4 Deben determinarse las secuencias de eventos que conducen a eventos peligrosos determinados en el apartado 7.4.2.3.

NOTA – En general, es beneficioso estudiar si alguna de las secuencias de eventos se puede eliminar por modificación en el diseño del proceso o del equipo utilizado.

7.4.2.5 Deben evaluarse las probabilidades de los eventos peligrosos en lo que concierne a las condiciones especificadas en el apartado 7.4.2.3.

NOTA – La probabilidad de un evento específico puede expresarse cuantitativamente o cualitativamente (véase la Norma CEI 61508-5).

7.4.2.6 Deben determinarse las consecuencias potenciales asociadas a los eventos peligrosos determinados en el apartado 7.4.2.3.

7.4.2.7 Debe evaluarse o estimarse el riesgo del EUC para cada evento peligroso determinado.

7.4.2.8 Pueden cumplirse los requisitos de los apartados del 7.4.2.1 al 7.4.2.7 por aplicación de las técnicas bien cualitativas, o bien cuantitativas para el análisis de peligro y de riesgo (véase la Norma CEI 61508-5).

7.4.2.9 El carácter apropiado de las técnicas y el grado de aplicación de estas técnicas dependerán de un cierto número de factores, tales como:

– peligros específicos y sus consecuencias;

– sector de aplicación y sus buenas prácticas;

– requisitos legales y los que regulan la seguridad;

– riesgo del EUC;

– disponibilidad de los datos precisos que sirven de base para el análisis de peligro y de riesgo.

7.4.2.10 Deben considerarse en el análisis de peligro y de riesgo los puntos siguientes:

– cada evento peligroso determinado y los componentes que contribuyen;

– las consecuencias y la probabilidad de las secuencias de eventos a los que se asocia cada evento peligroso;

– la reducción de riesgo necesaria para cada evento peligroso;

– las medidas tomadas para reducir o suprimir los riesgos y peligros;

– las hipótesis hechas durante el análisis de riesgos, incluyendo las tasas de demanda probables y las tasas de fallo del equipo; cualquier limitación de explotación o de intervención humana debe detallarse;

– las referencias a las informaciones clave (véase el capítulo 5 y el anexo A) relacionadas con los sistemas de seguridad en cada fase del ciclo de vida de la seguridad del sistema E/E/PE (por ejemplo las actividades de verificación y de validación).

7.4.2.11 Debe documentarse la información y los resultados que constituyen el análisis de peligro y de riesgo.

7.4.2.12 La información y los resultados que constituyen el análisis de peligro y de riesgo deben acutalizarse para el EUC y el sistema de control del EUC durante todo el ciclo de vida de la seguridad global, desde la fase de análisis de peligro y de riesgo hasta la fase de puesta fuera de servicio o descatalogación.

NOTA – La actualización de la información y de los resultados desde la fase de análisis de peligro y de riesgo es el principal medio para progresar en la resolución de los problemas relacionados con el análisis de peligro y de riesgo.

7.5 Requisitos globales de seguridad

NOTA – Esta fase corresponde a la etapa 4 de la figura 2.

7.5.1 Objetivo. El objetivo de los requisitos de este apartado es desarrollar la especificación para los requisitos globales de seguridad, en términos de requisitos de funciones de seguridad y de requisitos de integridad de seguridad, para los sistemas de seguridad E/E/PE, los sistemas de seguridad basados en otra tecnología y los dispositivos externos de reducción de riesgo, para alcanzar la seguridad funcional requerida.

NOTA – En el caso de aplicaciones en donde pueden hacerse hipótesis válidas sobre los riesgos, los peligros potenciales, los eventos peligrosos y sus consecuencias, el análisis requerido en este apartado (y el apartado 7.4) puede realizarse por los redactores de las versiones de aplicación sectorial de esta norma, y puede incluirse en los requisitos gráficos simplificados. Unos ejemplos de estos métodos se proporcionan en los anexos D y E de la Norma CEI 61508-5.

7.5.2 Requisitos

7.5.2.1 Deben especificarse las funciones de seguridad necesarias para asegurar la seguridad funcional requerida para cada peligro determinado. Esto debe constituir la especificación para los requisitos globales de funciones de seguridad.

NOTA – Las funciones de seguridad a ejecutar no serán, a este nivel, especificadas en términos puramente técnicos ya que el método y la tecnología de la implementación de las funciones de seguridad no se conocerán hasta más tarde. Durante la asignación de los requisitos de seguridad (véase el apartado 7.6), la descripción de las funciones de seguridad puede necesitar una modificación para mejorar la correspondencia con el método específico de implantación.

7.5.2.2 Debe determinarse la reducción de riesgo necesario para cada evento peligroso determinado. Esta determinación de la reducción de riesgo necesario puede hacerse cuantitativamente y/o cualitativamente.

NOTA – La reducción de riesgo necesaria se requiere para determinar los requisitos de integridad de seguridad para los sistemas de seguridad E/E/PE, los sistemas de seguridad basados en otra tecnología y los dispositivos externos de reducción de riesgo. El anexo C de la Norma CEI 61508-5 proporciona una de las formas de determinar la reducción de riesgo necesario cuando se adopta una aproximación cuantitativa. Los anexos D y E de la Norma CEI 61508-5 proporcionan unos métodos cualitativos, aunque en los ejemplos citados, la reducción de riesgo necesaria se incorpora implícitamente antes que se formule explícitamente.

7.5.2.3 En las situaciones en donde una norma del sector de aplicación existe, que incluyen unos métodos apropiados para determinar directamente la reducción de riesgo necesario, entonces dichas normas pueden utilizarse para satisfacer los requisitos de este apartado.

7.5.2.4 Cuando los fallos del sistema de control del EUC demande uno o varios E/E/PE o sistemas de seguridad basados en otra tecnología y/o dispositivos externos de reducción de riesgo, y cuando no está previsto diseñar el sistema de control del EUC como un “sistema relacionado con la seguridad”, deben aplicarse los requisitos siguientes:

a) la tasa de fallo peligrosa solicitada por el sistema de control del EUC debe apoyarse en los datos adquiridos por alguno de los siguientes medios:

   – experiencia en explotación real del sistema de control del EUC en una aplicación similar;

   – análisis de fiabilidad realizado conforme a un procedimiento reconocido;

   – base de datos industrial sobre la fiabilidad de los equipos genéricos;

b) la tasa de fallo peligrosa que se puede exigir por el sistema de control del EUC no debe ser inferior a 10^{-5} fallos peligrosos por hora;

   NOTA 1 – El fundamento de este requisito es que si el sistema de control del EUC no se diseña como un sistema de seguridad, entonces la tasa de fallo que puede exigirse para el sistema de control del EUC no debe ser inferior a la medida objetivo de fallo más alta para el nivel 1 de integridad de seguridad (que es de 10^{-5} fallos peligrosos por hora; véase la tabla 3).

c) deben determinarse todos los modos de fallo peligroso razonablemente previsibles del sistema de control del EUC y tenerse en cuenta en el desarrollo de la especificación para los requisitos globales de seguridad;

d) el sistema de control del EUC debe estar separado e independiente de los sistemas de seguridad E/E/PE, de los sistemas de seguridad basados en otra tecnología y de los dispositivos externos de reducción de riesgo.

NOTA 2 – Partiendo del principio que los sistemas relacionados con la seguridad se han diseñado para proporcionar una integridad de seguridad adecuada teniendo en cuenta las tasa normal de demanda del sistema de control del EUC, no será necesario diseñar el sistema de control del EUC como un sistema relacionado con la seguridad (y, en consecuencia, sus funciones no serán diseñadas como funciones de seguridad en el contexto de esta norma). En ciertas aplicaciones, particularmente en las que se requiere una muy alta integridad de seguridad, puede ser apropiado reducir la tasa de demanda diseñando el sistema de control del EUC de tal modo que tenga una tasa de fallo más baja de lo normal. En este caso, si la tasa de fallo es más pequeña que el límite objetivo de integridad de seguridad más alto para el nivel 1 de la integridad de seguridad (véase la tabla 3), entonces el sistema de control se convierte en un sistema relacionado con la seguridad y se aplican los requisitos de esta norma.

7.5.2.5 Si los requisitos del apartado 7.5.2.4 del a) al d) incluidos no se pueden cumplir, entonces el sistema de control del EUC debe diseñarse como un sistema relacionado con la seguridad. El nivel de integridad de seguridad permitido al sistema de control del EUC debe basarse en la tasa de fallo exigida por el sistema de control del EUC, de acuerdo con las medidas objetivo de esta norma, en relación al nivel de integridad de seguridad permitido, que deben aplicarse al sistema de control del EUC.

NOTA 1 – Por ejemplo, si se exige una tasa de fallo comprendida entre 10^{-6} y 10^{-5} fallos por hora para el sistema de control del EUC, entonces sería necesario que se cumplieran los requisitos apropiados al nivel 1 de integridad de seguridad.

NOTA 2 – Véase también el apartado 7.6.2.10.

7.5.2.6 Los requisitos de integridad de seguridad, sobre el plan de reducción de riesgo necesario, deben especificarse para cada función de seguridad. Esto debe constituir la especificación para los requisitos globales de integridad de seguridad.

NOTA – La especificación de los requisitos de integridad de seguridad es una etapa intermedia hacia la determinación de los niveles de integridad de seguridad para las funciones de seguridad antes de implantarse por los sistemas de seguridad E/E/PE. Ciertos métodos cualitativos utilizados para determinar los niveles de integridad de seguridad (véanse los anexos D y E de la Norma CEI 61508-5) progresan directamente desde los parámetros de riesgo a los niveles de integridad de seguridad. En estos casos, la reducción de riesgo necesaria se indica implícitamente antes que explícitamente ya que esta reducción se incluye en el propio método.

7.5.2.7 La especificación para las funciones de seguridad (véase el apartado 7.5.2.1) y la especificación para los requisitos de integridad de seguridad (véase el apartado 7.5.2.6) deben constituir juntas la especificación para los requisitos globales de seguridad.

7.6 Asignación de los requisitos de seguridad

NOTA – Esta fase corresponde a la etapa 5 de la figura 2.

7.6.1 Objetivos

7.6.1.1 El primer objetivo de los requisitos de este apartado es asignar las funciones de seguridad, que se indican en la especificación para los requisitos globales de seguridad (conjunto de requisitos de funciones de seguridad y de los requisitos de integridad de seguridad), a los sistemas de seguridad E/E/PE diseñados, a los sistemas de seguridad basados en otra tecnología y a los dispositivos externos de reducción de riesgo.

NOTA – Se consideran necesarios los sistemas de seguridad basados en otra tecnología y los dispositivos externos de reducción de riesgo ya que la asignación de los sistemas de seguridad E/E/PE no pueden realizarse a menos que las estas otras medidas de reducción de riesgo hayan sido tenidas en cuenta.

7.6.1.2 El segundo objetivo de los requisitos de este apartado es asignar un nivel de integridad de seguridad a cada función de seguridad.

NOTA – Los requisitos de integridad de seguridad, especificados en el apartado 7.5, se especifican en términos de reducción de riesgo.

7.6.2 Requisitos

7.6.2.1 Deben especificarse los sistemas de seguridad diseñados que se utilizarán para alcanzar la seguridad funcional requerida. La reducción de riesgo necesaria puede lograrse por medio de:

– dispositivos externos de reducción de riesgo;

– sistemas de seguridad E/E/PE;

– sistemas de seguridad basados en otra tecnología.

NOTA – Este apartado sólo se aplica si uno de los sistemas de seguridad es un E/E/PES.

7.6.2.2 Deben considerarse la asignación de las funciones de seguridad a los sistemas de seguridad E/E/PE diseñados, a los sistemas de seguridad basados en otra tecnología y a los dispositivos externos de reducción de riesgo, las competencias y los recursos disponibles durante todas las fases del ciclo de vida de la seguridad global.

NOTA 1 – A menudo se subestima la amplitud de las implicaciones de la utilización de los sistemas relacionados con la seguridad que emplean una tecnología compleja. Por ejemplo, la implementación de las tecnologías complejas necesitan un nivel superior de competencia en cada etapa, desde la especificación hasta la explotación y el mantenimiento. La utilización de otras soluciones tecnológicas, más simples, pueden tener la misma eficacia y varias ventajas por la reducción de la complejidad.

NOTA 2 – La disponibilidad de las competencias y de los recursos para la explotación y el mantenimiento, así como para el entorno de explotación, puede adquirir una importancia crítica ya que trata de asegurar la seguridad funcional requerida durante la explotación.

7.6.2.3 Debe asignarse cada función de seguridad, con su requisito de integridad de seguridad asociado, definido de acuerdo con el apartado 7.5, a los sistemas de seguridad E/E/PE diseñados teniendo en cuenta la reducción de riesgo realizada por los sistemas de seguridad basados en otra tecnología y los dispositivos externos de reducción de riesgo, de forma que la reducción de riesgo necesaria para esta función de seguridad se logre. Esta asignación es iterativa, y si se encuentra que la reducción de riesgo necesaria no se puede conseguir, entonces la arquitectura se debe modificar y repetir la asignación.

NOTA 1 – Cada función de seguridad, asociada a los requisitos de integridad de seguridad, especificada en el plan de reducción de riesgo necesario (véase el apartado 7.5), será asignada a uno o varios sistemas de seguridad E/E/PE, a los sistemas de seguridad basados en otra tecnología y a los sistemas externos de reducción de riesgo. La decisión de asignar una función de seguridad especifica a uno o varios sistemas relacionados con la seguridad dependerá de un conjunto de factores, pero más concretamente de la reducción de riesgo antes de realizarse por esta función de seguridad. Cuanto más grande sea la reducción de riesgo, es más probable que la función sea repartida entre varios sistemas relacionados con la seguridad.

NOTA 2 – La figura 6 presenta la aproximación adoptada en este apartado para la asignación de los requisitos de seguridad.

7.6.2.4 La asignación indicada en el apartado 7.6.2.3 debe realizarse de tal forma que todas las funciones de seguridad sean asignadas y que los requisitos de integridad de seguridad se cumplan para cada función de seguridad (bajo reserva de la preponderancia de los requisitos especificados en el apartado 7.6.2.10).

7.6.2.5 Los requisitos de integridad de seguridad para cada función de seguridad deben cualificarse con el fin de indicar, para cada parámetro de integridad de seguridad objetivo, si corresponde a:

– la probabilidad media de fallo a ejecutar, bajo demanda, las funciones para las que se ha diseñado (para un modo de funcionamiento en baja demanda); o

– la probabilidad de un fallo peligroso por hora (para un modo de funcionamiento continuo o en fuerte demanda).

7.6.2.6 La asignación de los requisitos de integridad de seguridad debe realizarse utilizando las técnicas apropiadas para la combinación de las probabilidades.

NOTA – La asignación de los requisitos de seguridad puede realizarse de forma cualitativa y/o cuantitativa.

7.6.2.7 La asignación debe hacerse teniendo en cuenta la posibilidad de fallos de origen común. Si se prevé tratar independientemente en la asignación los sistemas de seguridad E/E/PE, los sistemas de seguridad basados en otra tecnología y los dispositivos externos de reducción de riesgo, entonces deben:

– estar funcionalmente diversificados (es decir, utilizar aproximaciones totalmente diferentes para lograr los mismos resultados);

– estar basados sobre otras tecnologías (es decir, utilizar diferentes tipos de equipos para lograr los mismos resultados);

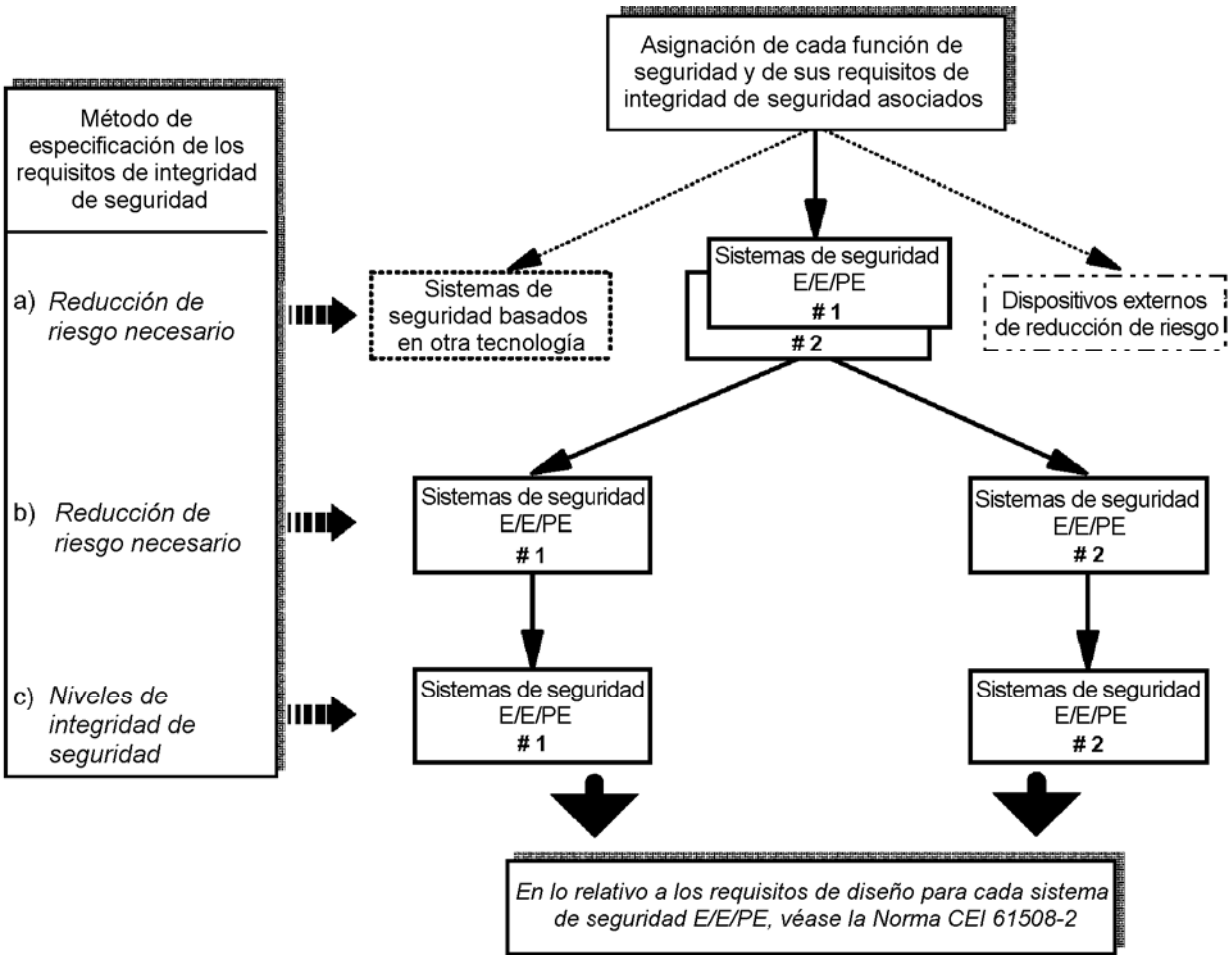
NOTA 1 – Es necesario reconocer que, aunque la tecnología sea muy diversa, en el caso de los sistemas de alto nivel de integridad de seguridad con consecuencias particularmente graves en caso de fallo, se tomarán precauciones especiales para los eventos que tengan un origen común de baja probabilidad, por ejemplo el accidente de un avión y los terremotos.

– no compartir en común las partes, servicios o sistemas anexos (por ejemplo el suministro de energía) en los que un fallo podría conducir a un modo de fallo peligroso de todos los sistemas;

– no compartir procedimientos comunes de explotación, de mantenimiento o de ensayo;

– estar físicamente separados de forma que los fallos previsibles no afecten a los sistemas de seguridad circundantes ni a los dispositivos externos de reducción de riesgos.

NOTA 2 – Esta norma trata específicamente la asignación de requisitos de integridad de seguridad a los sistemas de seguridad E/E/PE, y los requisitos se especifican indicando como debe realizarse. La asignación de los requisitos de integridad de seguridad a los sistemas de seguridad basados en otra tecnología y a los dispositivos externos de reducción de riesgo no se trata en profundidad en esta norma.



NOTA 1 – Los requisitos de integridad de seguridad se asocian a cada función de seguridad antes de la asignación (véase el apartado 7.5.2.6).

NOTA 2 – Una función de seguridad se puede asignar a varios sistemas de seguridad.

Fig. 6 – Asignación de los requisitos de seguridad a los sistemas de seguridad E/E/PE, sistemas de seguridad basados en otra tecnología y dispositivos externos de reducción de riesgo

7.6.2.8 Si no se pueden satisfacer todos los requisitos del apartado 7.6.2.7, entonces los sistemas de seguridad E/E/PE, los sistemas de seguridad basados en otra tecnología y los dispositivos externos de reducción de riesgo no deben considerarse como independientes, en el marco de los objetivos de asignación de la integridad de seguridad, excepto si la realización de un análisis muestra que son suficientemente independientes (desde el punto de vista de la integridad de seguridad).

NOTA 1 – Para más información sobre el análisis de los fallos dependientes, véanse las referencias [9] y [10] en el anexo C.

NOTA 2 – El concepto de independencia suficiente se establece demostrando que la probabilidad de un fallo dependiente es suficientemente baja en relación a los requisitos globales de integridad de seguridad para los sistemas de seguridad E/E/PE.

7.6.2.9 Cuando la asignación ha progresado suficiente, los requisitos de integridad de seguridad, para cada función de seguridad asignada al (los) sistema(s) de seguridad E/E/PE, deben especificarse en el plan de los niveles de integridad de seguridad de acuerdo con las tablas 2 y 3, y ser cualificadas de forma que indique si el parámetro de integridad de seguridad objetivo es o bien:

– la probabilidad media de fallo a ejecutar, bajo demanda, las funciones para las que se ha diseñado (para un modo de funcionamiento en baja demanda), o bien

– la probabilidad de un fallo peligroso por hora (para un modo de funcionamiento continuo o en fuerte demanda).

NOTA 1 – Previamente a esta etapa, los requisitos de integridad de seguridad se han especificado en términos de reducción de riesgo (véase el apartado 7.5).

NOTA 2 – Las tablas 2 y 3 contienen las medidas objetivo de fallo para los niveles de integridad de seguridad. Se acepta que no es posible predecir cuantitativamente la integridad de seguridad de todos los aspectos de los sistemas de seguridad E/E/PE. Las técnicas, medidas y juicios cualitativos se realizarán con las precauciones necesarias para lograr las medidas objetivo de fallo. Esto es particularmente verdad en el caso de una integridad de seguridad sistemática (véase el apartado 3.5.4 de la Norma CEI 61508-4).

Tabla 2
Niveles de integridad de seguridad: medidas objetivo de fallo para una función de seguridad funcionando en modo de baja demanda

Nivel de integridad de seguridad	**Modo de funcionamiento a baja demanda** (Probabilidad media de fallo a ejecutar, bajo demanda, la función para la que ha sido diseñado)
4	$\geq 10^{-5}$ a $< 10^{-4}$
3	$\geq 10^{-4}$ a $< 10^{-3}$
2	$\geq 10^{-3}$ a $< 10^{-2}$
1	$\geq 10^{-2}$ a $< 10^{-1}$
NOTA – Véanse las notas de la 3 a la 9 que hay a continuación para la interpretación detallada de esta tabla.	

Tabla 3
Niveles de integridad de seguridad: medidas objetivo de fallo para una función de seguridad funcionando en modo continuo o de fuerte demanda

Nivel de integridad de seguridad	Modo de funcionamiento continuo o a fuerte demanda (Probabilidad de fallo peligroso por hora)
4	$\geq 10^{-9}$ a $< 10^{-8}$
3	$\geq 10^{-8}$ a $< 10^{-7}$
2	$\geq 10^{-7}$ a $< 10^{-6}$
1	$\geq 10^{-6}$ a $< 10^{-5}$
NOTA – Véanse las notas de la 3 a la 9 que hay a continuación para la interpretación detallada de esta tabla.	

NOTA 3 – Véase el apartado 3.5.12 de la Norma CEI 61508-4 para la definición de los términos “modo de funcionamiento en baja demanda” y “continuo o en fuerte demanda”.

NOTA 4 – El parámetro de la tabla 3 para un modo de funcionamiento continuo o en fuerte demanda, “la probabilidad de un fallo peligroso por hora”, también se llama “frecuencia de fallos peligrosos”, o “tasa de fallo peligroso”, en unidades de fallos peligrosos por hora.

NOTA 5 – Cuando un sistema de seguridad E/E/PE debe explotarse en un modo de funcionamiento continuo o en fuerte demanda, para un tiempo y una misión determinada durante la cual no ha tenido lugar ninguna reparación, el nivel de integridad de seguridad necesario para una función de seguridad dada, se puede deducir como se explica a continuación. Determinar la probabilidad de fallo de la función de seguridad durante el tiempo de la misión y dividir esta probabilidad entre la duración de la misión para obtener la probabilidad de fallo por hora; utilizar entonces la tabla 3 para deducir el nivel requerido de integridad de seguridad.

NOTA 6 – Esta norma define un límite inferior para las medidas objetivo de fallo, en un modo de fallo peligroso, que se puede exigir. Estos se especifican como los límites inferiores para el nivel 4 de integridad de seguridad (es decir, una probabilidad media de fallo de 10^{-5} a ejecutar, bajo demanda, la función para la cual ha sido diseñado, o una probabilidad de fallo peligroso de 10^{-9} por hora). Se pueden diseñar unos sistemas de seguridad que tengan valores más bajos para las medidas objetivo de fallo en el caso de sistemas no complejos, pero se estima que las cifras de estas tablas representan el límite en el que se puede realizar en el momento actual para unos sistemas relativamente complejos (por ejemplo unos sistemas electrónicos programables relacionados con la seguridad).

NOTA 7 – Las medidas objetivo de fallo que se pueden exigir cuando dos o varios sistemas de seguridad E/E/PE se utilizan pueden ser mejores que los indicados en las tablas 2 y 3, a partir del momento en el que los niveles adecuados de integridad se logran.

NOTA 8 – Es importante resaltar que las medidas de fallo para los sistemas de integridad de seguridad 1, 2, 3 y 4 son medidas objetivo de fallo. Se acepta que será posible cuantificar y aplicar las técnicas de predicción de fiabilidad permitiendo evaluar si las medidas objetivo de fallo se han alcanzado, solamente para la integridad de seguridad del hardware (véase el apartado 3.5.5 de la Norma CEI 61508-4). Las técnicas y juicios cualitativos se realizan con los requisitos necesarios para alcanzar las medidas objetivo de fallo en lo que concierne a la integridad de seguridad sistemática (véase el apartado 3.5.4 de la Norma CEI 61508-4).

NOTA 9 – Los requisitos de integridad de seguridad para cada función de seguridad deben estar cualificados de forma que indique si el parámetro de integridad de seguridad objetivo es o bien:

- la probabilidad media de fallo a ejecutar, bajo demanda, las funciones para las que se ha diseñado (para un modo de funcionamiento en baja demanda), o bien
- la probabilidad de un fallo peligroso por hora (para un modo de funcionamiento continuo o en fuerte demanda).

7.6.2.10 Para un sistema de seguridad E/E/PE que pone en funcionamiento las funciones de seguridad que tienen unos niveles de integridad de seguridad diferentes, y excepto si se puede demostrar que existe una independencia suficiente en la implementación de sus funciones de seguridad, las partes del hardware y del software relacionadas con la seguridad en donde no hay una independencia suficiente en su implementación deben tratarse como si formasen parte de la función de seguridad que tiene el más alto nivel de integridad de seguridad . En consecuencia, los requisitos aplicables al más alto nivel de integridad de seguridad correspondiente deben aplicarse a todas estas partes.

NOTA – Véase también el apartado 7.4.2.4 de la parte 2 y el apartado 7.4.2.8 de la parte 3.

7.6.2.11 Una arquitectura (de sistema) que sólo incluye un sistema de seguridad E/E/PE de nivel 4 de integridad de seguridad sólo debe permitirse si los criterios del punto a) o de los puntos b) y c) (en conjunto) siguientes se cumplen:

a) la medida objetivo de fallo de la integridad de seguridad ha sido demostrada de forma explícita, por una combinación de métodos analíticos y de ensayos apropiados;

b) se posee una importante experiencia en explotación de los componentes utilizados como parte del sistema de seguridad E/E/PE; esta experiencia se debe haber adquirido en un entorno similar y, al menos, haber sido utilizada en un sistema de nivel de complejidad comparable;

c) se posee suficientes datos de fallo del hardware, obtenidos de los componentes utilizados como parte del sistema de seguridad E/E/PE, para permitir una confianza suficiente sobre la medida objetivo de fallo de integridad de seguridad del hardware que será exigida. Conviene utilizar unos datos apropiados al entorno propuesto, la aplicación y el nivel de complejidad.

7.6.2.12 A ningún sistema de seguridad E/E/PE único se le debe asignar una medida objetivo de fallo de integridad de seguridad inferior a la especificada en las tablas 2 y 3. Es decir, que para los sistemas de seguridad funcionando en:

– modo de funcionamiento en baja demanda, el límite inferior se fija para una probabilidad media de fallo de 10^{-5} a ejecutar, bajo demanda, la función para la cual ha sido diseñado;

– modo de funcionamiento continuo o en fuerte demanda, el límite inferior se fija para una probabilidad de fallo peligroso de 10^{-9} por hora.

7.6.2.13 Debe documentarse la información y los resultados de asignación de los requisitos de seguridad adquiridos en los apartados del 7.6.2.1 al 7.6.2.12, junto a cualquier hipótesis y justificación hecha.

NOTA – Para cada sistema de seguridad E/E/PE, se recomienda tener suficiente información sobre las funciones de seguridad y sus niveles de integridad de seguridad asociados. Esta información formará la base de los requisitos de seguridad para los sistemas de seguridad E/E/PE desarrollados en la Norma CEI 61508-2.

7.7 Planificación global de la explotación y del mantenimiento

NOTA 1 – Esta fase corresponde a la etapa 6 de la figura 2.

NOTA 2 – Un ejemplo de modelo de actividades en explotación y mantenimiento se presenta en la figura 7.

NOTA 3 – Un ejemplo de modelo de gestión de explotación y del mantenimiento se presenta en la figura 8.

7.7.1 Objetivo. El objetivo de los requisitos de este apartado es desarrollar un plan de explotación y de mantenimiento de los sistemas de seguridad E/E/PE, para asegurar que la seguridad funcional requerida se mantiene durante la explotación y el mantenimiento.

7.7.2 Requisitos

7.7.2.1 Debe prepararse un plan que debe especificar los aspectos siguientes:

a) actividades sistemáticas que deben realizarse para mantener la seguridad funcional requerida de los sistemas de seguridad E/E/PE;

b) actividades y limitaciones que son necesarias (por ejemplo durante el arranque, la explotación normal, los ensayos sistemáticas, las perturbaciones previsibles, los defectos y la parada) para evitar un estado de no seguridad, para reducir las demandas del sistema de seguridad E/E/PE o para reducir las consecuencias de los eventos peligrosos;

NOTA 1 – Las limitaciones, condiciones y acciones siguientes se adecuarán a los sistemas de seguridad E/E/PE:

- limitaciones sobre la explotación del EUC durante un fallo o un defecto de los sistemas de seguridad E/E/PE;
- limitaciones sobre la explotación del EUC durante el mantenimiento de los sistemas de seguridad E/E/PE;
- cuando las limitaciones sobre la explotación se pueden suprimir;
- procedimientos para el retorno de la explotación normal;
- procedimientos para confirmar que la explotación normal se ha restablecido;
- circunstancias durante las cuales las funciones del sistema de seguridad E/E/PE se pueden puentear (by-pass) para el arranque o para una explotación especial o para ensayos;
- procedimientos a seguir antes, durante y después del "by-pass" de los sistemas de seguridad E/E/PE, incluyendo los procedimientos de compromiso de los trabajos y de los niveles de autorización.

c) es necesario conservar los documentos que muestran los resultados de las auditorías y de los ensayos de seguridad funcional;

d) es necesario conservar los documentos sobre los incidentes peligrosos y cualquier incidente que pueda crear potencialmente un evento peligroso;

e) el campo de aplicación de las actividades de mantenimiento (que se distingue de las actividades de modificación);

f) las acciones a tomar cuando ocurre un peligro;

g) el contenido de la documentación cronológica de las actividades de explotación y mantenimiento (véase el apartado 7.15).

NOTA 2 – La mayoría de los sistemas de seguridad E/E/PE tienen unos modos de fallo que sólo pueden ser descubiertos por los ensayos durante el mantenimiento sistemático. En estos casos, si los ensayos no se realizan con una frecuencia suficiente, la integridad de seguridad requerida del sistema de seguridad E/E/PE no se logrará. Cuando los ensayos se realicen en línea "on-line", puede ser necesario desactivar temporalmente el sistema de seguridad E/E/PE. Conviene sólo considerar esta posibilidad si la probabilidad de una demanda que se produce durante este tiempo es muy baja. Cuando no pueda asegurarse, puede ser necesario instalar sensores y accionadores suplementarios para mantener la seguridad funcional requerida durante el ensayo.

NOTA 3 – Este apartado se aplica al suministrador del software que tiene que proporcionar la información y los procedimientos con el software que permitirá asegurar la seguridad funcional requerida durante la explotación y el mantenimiento de un sistema de seguridad. Esto incluye los procedimientos preparatorios para cualquier modificación del software que se puede realizar como consecuencia de un requisito de explotación o de mantenimiento (véase también el apartado 7.6 de la Norma CEI 61508-3). La implementación de estos procedimientos se trata en los apartados 7.15 y 7.8 de la Norma CEI 61508-3. Los procedimientos preparatorios para los futuros cambios del software que pueden realizarse como consecuencia de un requisito de modificación para un sistema de seguridad se tratan en los apartados 7.16 y 7.6 de la Norma CEI 61508-3. La implementación de los procedimientos se trata en los apartados 7.16 y 7.8 de la Norma CEI 61508-2.

NOTA 4 – Conviene tener en cuenta los procedimientos de explotación y de mantenimiento desarrollados para cumplir los requisitos de las Normas CEI 61508-2 y CEI 61508-3.

7.7.2.2 Conviene determinar, por un análisis sistemático, las actividades de mantenimiento sistemático que se realizan para determinar los fallos no descubiertos.

NOTA – Si los fallos no descubiertos no se detectan, esto puede:

- conducir a un fallo de funcionamiento durante una demanda, en el caso de los sistemas de seguridad E/E/PE, de los sistemas de seguridad basados en otra tecnología o de los dispositivos externos de reducción de riesgo;
- generar unas demandas de los sistemas de seguridad E/E/PE, de los sistemas de seguridad basados en otra tecnología o de los dispositivos externos de reducción de riesgo, en el caso de sistemas no relacionados con la seguridad.

7.7.2.3 El plan para el mantenimiento de los sistemas de seguridad E/E/PE debe decidirse por las personas responsables de la futura explotación y mantenimiento de los sistemas de seguridad E/E/PE, de los sistemas de seguridad basados en otra tecnología, de los dispositivos externos de reducción de riesgo y de los sistemas no relacionados con la seguridad que pueden potencialmente solicitar los sistemas de seguridad.

7.8 Planificación global de la validación de la seguridad

NOTA – Esta fase corresponde a la etapa 7 de la figura 2.

7.8.1 Objetivo

El objetivo de los requisitos de este apartado es desarrollar un plan para facilitar la validación global de la seguridad de los sistemas de seguridad E/E/PE.

7.8.2 Requisitos

7.8.2.1 Debe desarrollarse un plan que contenga los aspectos siguientes:

a) detalles que conciernen a los datos de la validación;

b) detalles que conciernen a las personas encargadas de la validación;

c) especificación de los modos pertinentes de explotación del EUC, con sus relaciones con el sistema de seguridad E/E/PE, incluyendo, cuando sea apropiado:

- preparativos de utilización, incluyendo la configuración y los reglajes;
- arranque;
- aprendizaje;
- modo automático;
- modo manual;
- modo semiautomático;
- régimen establecido;
- puesta a cero;
- parada;
- mantenimiento;
- condiciones anormales razonablemente previsibles;

d) especificación de los sistemas de seguridad E/E/PE que necesitan validarse para cada modo de explotación del EUC antes de empezar la puesta en servicio;

e) estrategia técnica para la validación (por ejemplo los métodos analíticos, los ensayos estáticos, etc.);

f) medidas, técnicas y procedimientos que deben utilizarse para confirmar que la asignación de las funciones de seguridad se ha realizado correctamente; esto incluye la confirmación de que cada función de seguridad está conforme:

- con la especificación para los requisitos globales de funciones de seguridad, y
- con la especificación para los requisitos globales de integridad de seguridad;

g) referencia específica a cada elemento contenido en los datos de salida de los apartados 7.5 y 7.6;

h) entorno requerido en el que las actividades de validación deben tener lugar (por ejemplo, para los ensayos, esto incluye las herramientas calibradas y los equipos de ensayo);

i) criterios de aceptación y de rechazo;

j) políticas y los procedimientos de evaluación de los resultados de la validación, particularmente de los fallos.

NOTA – Durante la planificación de la validación global, conviene tener en cuenta los trabajos planificados para la validación de la seguridad de los sistemas E/E/PE y para la validación del software, como los requeridos en las Normas CEI 61508-2 y CEI 61508-3. Es importante asegurar que las interacciones entre todas las medidas de reducción de riesgo se han considerado y que todas las funciones de seguridad (tales como las especificadas en las salidas del apartado 7.5), se han realizado.

7.8.2.2 La información que proviene del apartado 7.8.2.1 debe documentarse y constituir el plan para la validación global de la seguridad de los sistemas de seguridad E/E/PE.

7.9 Planificación global de la instalación y puesta en servicio

NOTA – Esta fase corresponde a la etapa 8 de la figura 2.

7.9.1 Objetivos

7.9.1.1 El primer objetivo de los requisitos de este apartado es desarrollar un plan para controlar la instalación de los sistemas de seguridad E/E/PE, asegurando que se alcanza la seguridad funcional requerida.

7.9.1.2 El segundo objetivo de los requisitos de este apartado es desarrollar un plan para controlar la puesta en servicio de los sistemas de seguridad E/E/PE, asegurando que se alcanza la seguridad funcional requerida.

7.9.2 Requisitos

7.9.2.1 Debe desarrollarse un plan para la instalación de los sistemas de seguridad E/E/PE, especificando:

- programa de instalación;
- persona responsable de las diferentes partes de la instalación;
- procedimientos para la instalación;
- secuencia de integración de los distintos elementos;
- criterios que permiten afirmar que todo o parte de los sistemas de seguridad E/E/PE están listos para la instalación y permiten afirmar que las actividades de la instalación están terminadas;
- procedimientos para la resolución de los fallos e incompatibilidades.

7.9.2.2 Debe desarrollarse un plan para la puesta en servicio de los sistemas de seguridad E/E/PE, especificando:

- programa de la puesta en servicio;
- persona responsable de las diferentes partes de la puesta en servicio;
- procedimientos para la puesta en servicio;
- relaciones entre las diferentes etapas de la instalación;
- relaciones con la validación.

7.9.2.3 Debe documentarse la planificación global de la instalación y de la puesta en servicio.

7.10 Realización: E/E/PES

NOTA – Esta fase correspondiente a la etapa 9 de la figura 2 y a las etapas de la 9.1 a la 9.6 de las figuras 3 y 4.

7.10.1 Objetivo. El objetivo de los requisitos de este apartado es crear unos sistemas de seguridad E/E/PE conformes a la especificación para los requisitos de seguridad de los E/E/PES (incluyendo la especificación para los requisitos de las funciones de seguridad de los E/E/PES y la especificación para los requisitos de integridad de seguridad de los E/E/PES). Véanse las Normas CEI 61508-2 y la CEI 61508-3.

7.10.2 Requisitos. Los requisitos deben cumplirse de acuerdo con la Norma CEI 61508-2 y CEI 61508-3.

7.11 Realización: otra tecnología

NOTA – Esta fase corresponde a la etapa 10 de la figura 2.

7.11.1 Objetivo. El objetivo de los requisitos de este apartado es crear unos sistemas de seguridad basados en otra tecnología que cumplan los requisitos de las funciones de seguridad y los requisitos de integridad de seguridad especificados para tales sistemas.

7.11.2 Requisitos. No se trata en esta norma la especificación que permite cumplir los requisitos de funciones de seguridad y los requisitos de integridad de seguridad para los sistemas de seguridad basados en otra tecnología.

NOTA – Los sistemas de seguridad basados en otra tecnología se basan en otra tecnología diferente a la eléctrica/electrónica/electrónica programable (por ejemplo, hidráulica, neumática, etc.). Los sistemas de seguridad basados en otra tecnología se han incluido en el ciclo de vida de la seguridad global, con los dispositivos externos de reducción de riesgo, por razones de exhaustividad (véase el apartado 7.12).

7.12 Realización: dispositivos externos de reducción de riesgo

NOTA – Esta fase corresponde a la etapa 11 de la figura 2.

7.12.1 Objetivo. El objetivo de los requisitos de este apartado es crear unos dispositivos externos de reducción de riesgo que cumplan los requisitos de las funciones de seguridad y los requisitos de integridad de seguridad especificados por tales dispositivos.

7.12.2 Requisitos. No se trata en esta norma la especificación que permite cumplir los requisitos de las funciones de seguridad y los requisitos de integridad de seguridad para los dispositivos externos de reducción de riesgo.

NOTA – Los dispositivos externos de reducción de riesgo se incluyen en el ciclo de vida de la seguridad global, con los sistemas de seguridad basados en otra tecnología, por razones de exhaustividad (véase el apartado 7.11).

7.13 Instalación y puesta en servicio globales

NOTA – Esta fase corresponde a la etapa 12 de la figura 2.

7.13.1 Objetivos

7.13.1.1 El primer objetivo de los requisitos de este apartado es instalar los sistemas de seguridad E/E/PE.

7.13.1.2 El segundo objetivo de los requisitos de este apartado es asegurar la puesta en servicio de los sistemas de seguridad E/E/PE.

7.13.2 Requisitos

7.13.2.1 Las actividades de instalación deben realizarse de acuerdo con el plan para la instalación de los sistemas de seguridad E/E/PE.

7.13.2.2 La información documentada durante la instalación debe constar de:

– documentación sobre las actividades de instalación;

– resolución de los fallos e incompatibilidades.

7.13.2.3 Las actividades de puesta en servicio se deben realizar de acuerdo con el plan para la puesta en servicio de los sistemas de seguridad E/E/PE.

7.13.2.4 La información documentada durante la puesta en servicio debe constar de:

– documentación sobre las actividades de la puesta en servicio;

– referencias de los informes de fallo;

– resolución de los fallos e incompatibilidades.

7.14 Validación global de la seguridad

NOTA – Esta fase corresponde a la etapa 13 de la figura 2.

7.14.1 Objetivo. El objetivo de los requisitos de este apartado es validar el hecho que los sistemas de seguridad cumplan la especificación para los requisitos globales de seguridad sobre el plan de los requisitos globales de las funciones de seguridad y de los requisitos globales de integridad de seguridad, teniendo en cuenta la asignación de los requisitos de seguridad, para los sistemas de seguridad E/E/PE, realizada de acuerdo con el apartado 7.6.

7.14.2 Requisitos

7.14.2.1 Las actividades de validación deben realizarse de acuerdo con el plan de validación global de la seguridad para los sistemas de seguridad E/E/PE.

7.14.2.2 Todo equipo utilizado para las medidas cuantitativas, en el marco de las actividades de validación, debe calibrarse de acuerdo con una especificación referida a una norma nacional o a la especificación del vendedor.

7.14.2.3 La información documentada durante la validación debe incluir:

– documentación cronológica de las actividades de validación;

– versión de la especificación para los requisitos globales de seguridad que se han utilizado;

– función de seguridad que se ha validado (por ensayo o por análisis);

– herramientas y el equipo utilizado, así como los datos de calibración;

– resultados de las actividades de validación;

– identificación de la configuración de la entidad ensayada, los procedimientos aplicados y el entorno de ensayo;

– diferencias entre los resultados esperados y los resultados reales.

7.14.2.4 Cuando existen diferencias entre los resultados esperados y los resultados reales, el análisis hecho y las decisiones tomadas relativas a la consecución de la validación o bien la emisión de una demanda de modificación y el retorno a una parte anterior de la validación deben documentarse.

7.15 Explotación, mantenimiento y reparación globales

NOTA 1 – Esta fase corresponde a la etapa 14 de la figura 2.

NOTA 2 – Las medidas de organización tratadas en este apartado permiten la implementación eficaz de los requisitos técnicos y tienen por único objetivo la realización y el mantenimiento de la seguridad funcional de los sistemas de seguridad E/E/PE. Los requisitos técnicos necesarios para mantener la seguridad funcional serán normalmente especificados en una parte de la documentación dada por el suministrador del sistema de seguridad E/E/PE.

NOTA 3 – Los requisitos de seguridad funcional durante las actividades de mantenimiento y de reparación pueden ser diferentes a los requeridos durante la explotación.

NOTA 4 – No es necesario suponer que los procedimientos de ensayos desarrollados para la instalación y la puesta en servicio inicial puedan utilizarse sin verificar su validez y su viabilidad en el contexto de una explotación "en línea" del EUC.

7.15.1 Objetivo. El objetivo de los requisitos de este apartado es explotar, mantener y reparar los sistemas de seguridad E/E/PE de forma que mantengan la seguridad funcional requerida.

7.15.2 Requisitos

7.15.2.1 Debe llevarse a la práctica lo siguiente:

– plan para el mantenimiento de los sistemas de seguridad E/E/PE;

– procedimientos de explotación, mantenimiento y reparación para los sistemas de seguridad E/E/PE (véase la Norma CEI 61508-2);

– procedimientos de explotación y de mantenimiento para el software (véase la Norma CEI 61508-3).

7.15.2.2 La implementación de los puntos citados en el apartado 7.15.2.1 debe incluir el lanzamiento de las siguientes acciones:

– puesta en marcha de los procedimientos;

– seguimiento de los programas de mantenimiento;

– mantenimiento de los documentos;

– realización periódica de auditorías de la seguridad funcional (véase el punto k del apartado 6.2.1);

– documentación de las modificaciones que se han realizado sobre los sistemas de seguridad E/E/PE.

NOTA 1 – Un ejemplo de modelo de actividades de explotación y mantenimiento se muestra en la figura 7.

NOTA 2 – Un ejemplo de modelo de gestión de la explotación y del mantenimiento se muestra en la figura 8.

7.15.2.3 La documentación cronológica de la explotación, de las reparaciones y del mantenimiento de los sistemas de seguridad E/E/PE debe mantenerse y contener la siguiente información:

– resultados de los ensayos y auditorías de la seguridad funcional;

– registro de la hora y del origen de las demandas de los sistemas de seguridad E/E/PE (en explotación real), así como la respuesta de los sistemas de seguridad E/E/PE cuando han sido sometidos a estas demandas, y los defectos descubiertos durante el mantenimiento sistemático;

– registro de las modificaciones aportadas al EUC, al sistema de control del EUC y a los sistemas de seguridad E/E/PE.

7.15.2.4 Los requisitos exactos relativos a la documentación cronológica dependerán de la aplicación específica y deben, cuando sea apropiado, detallarse en las normas de aplicación sectorial.

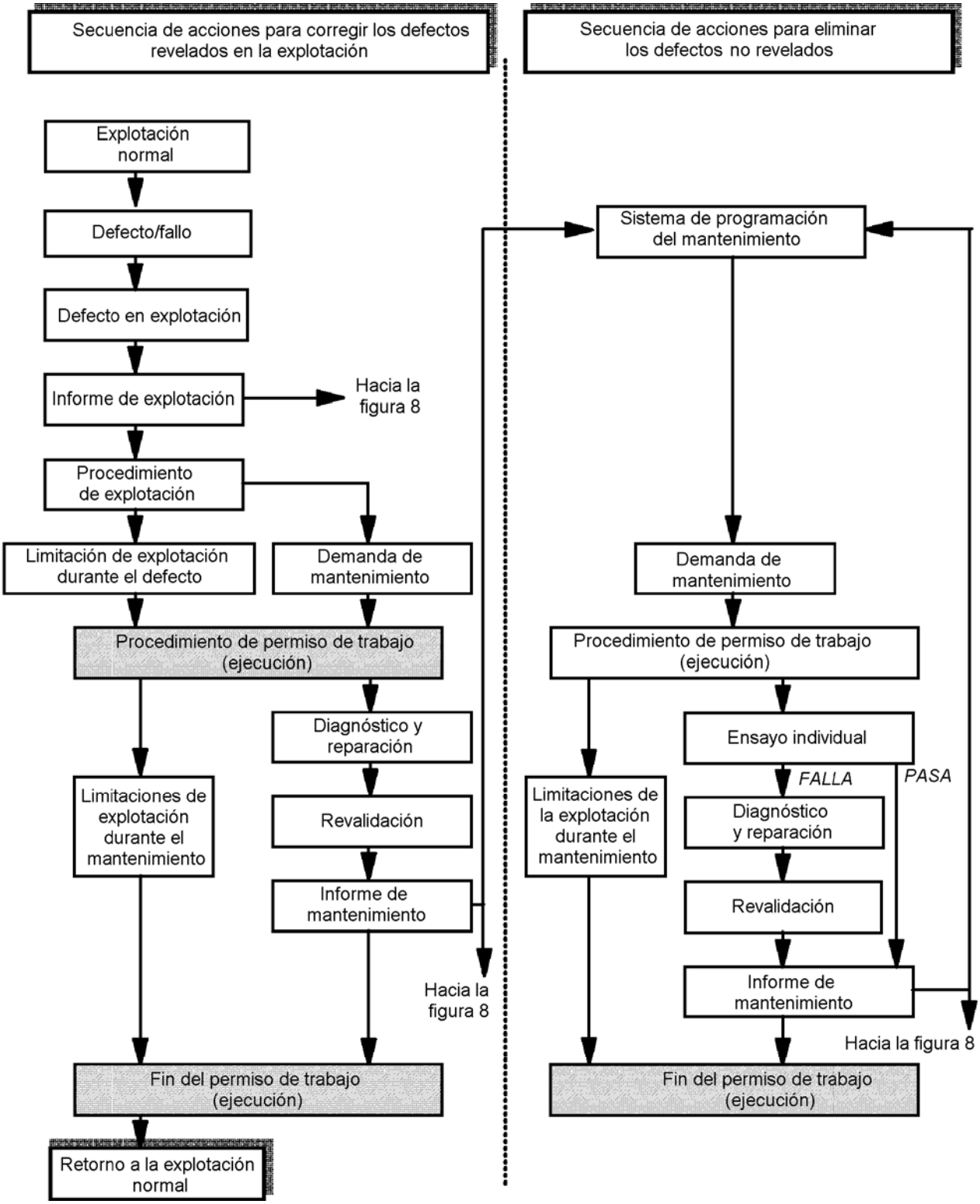


Fig. 7 – Ejemplo de modelo de actividades de explotación y de mantenimiento

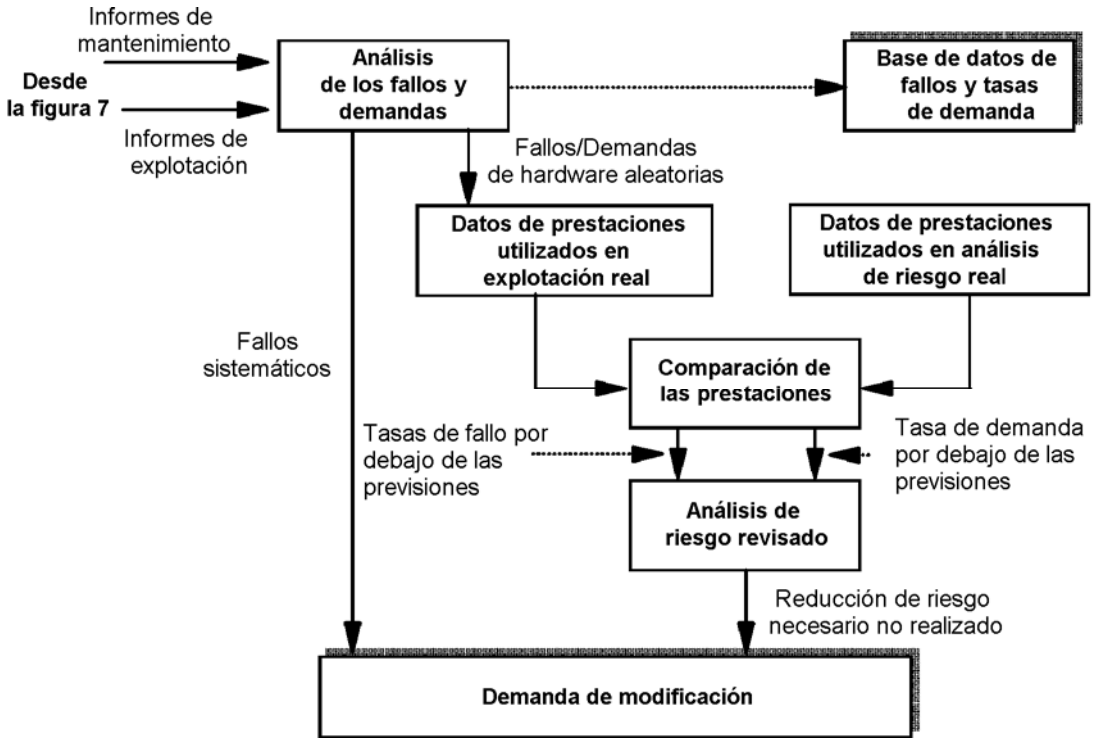


Fig. 8 – Ejemplo de modelo de gestión de la explotación y el mantenimiento

7.16 Modificación y actualización globales

NOTA 1 – Esta fase corresponde a la etapa 15 de la figura 2.

NOTA 2 – Las medidas de organización tratadas en este apartado permiten la implementación eficaz de los requisitos técnicos y tienen por único objetivo la realización y el mantenimiento de la seguridad funcional de los sistemas de seguridad E/E/PE. Los requisitos técnicos necesarios para mantener la seguridad funcional serán normalmente especificados en una parte de la documentación dada por el suministrador del sistema de seguridad E/E/PE.

7.16.1 Objetivo. El objetivo de los requisitos de este apartado es asegurar que la seguridad funcional para los sistemas de seguridad E/E/PE es apropiada, durante y después de que la fase de modificación y de actualización se haya realizado.

7.16.2 Requisitos

7.16.2.1 Antes de realizar cualquier modificación o actualización, deben planificarse los procedimientos (véase el apartado 6.2.1).

NOTA – En la figura 9 se muestra un modelo de procedimiento para las modificaciones.

7.16.2.2 La fase de modificación y actualización sólo debe poder iniciarse por la emisión de una demanda oficial según los procedimientos para la gestión de la seguridad funcional (véase el capítulo 6). Esta demanda debe detallarse en los puntos siguientes:

– peligros determinados que pueden ser afectados;

– modificación propuesta (ambos, hardware y software);

– razones de dicha modificación.

NOTA – Las razones de dicha demanda de modificación pueden venir, por ejemplo

- seguridad funcional inferior a la especificada;
- descubrimiento de un defecto sistemático;
- nueva legislación o corrección en materia de seguridad;
- modificaciones del EUC o de su utilización;
- modificación de los requisitos globales de seguridad;
- análisis de las prestaciones de explotación y de mantenimiento, indicando que la prestación está por debajo de los objetivos;
- auditorías sistemáticas de la seguridad funcional.

7.16.2.3 Debe realizarse un análisis de impacto. Debe incluir una evaluación del impacto sobre la seguridad funcional de cualquier sistema de seguridad E/E/PE, de las actividades de modificación de actualización propuestas. La evaluación debe incluir un análisis de peligro y de riesgo suficiente para determinar la extensión y la profundidad que deben cubrir las fases globales ulteriores del ciclo de vida de la seguridad del E/E/PES o del software. La evaluación también debe tener en cuenta el impacto de otras actividades de modificación o de actualización llevadas en paralelo, y también debe tener en cuenta la seguridad funcional durante y después de que se realicen las actividades de modificación y actualización.

7.16.2.4 Deben documentarse los resultados obtenidos en el apartado 7.16.2.3.

7.16.2.5 La autorización de realizar las actividades de modificación o de actualización requerida debe depender de los resultados del análisis de impacto.

7.16.2.6 Cualquier modificación que tenga un impacto sobre la seguridad funcional de todo sistema de seguridad E/E/PE debe volver a la fase global apropiada del ciclo de vida del software o sistemas de seguridad E/E/PE. Todas las fases siguientes deben ejecutarse respetando los procedimientos especificados para cada fase específica, de acuerdo con los requisitos de esta norma.

NOTA 1 – Podría ser necesario implementar un análisis completo de peligro y de riesgo, que podría generar unas necesidades de niveles de integridad de seguridad que son diferentes a los actualmente especificados para los sistemas de seguridad E/E/PE.

NOTA 2 – No debe presuponerse que los procedimientos de ensayo desarrollados para la instalación y la implementación inicial puedan utilizarse sin verificar su validez y su viabilidad en el contexto de una explotación “en línea” del EUC.

7.16.2.7 Debe establecerse y mantenerse una documentación cronológica. Ésta debe contener los detalles de todas las modificaciones y puestas a punto, y debe incluir referencia a:

- las demandas de modificaciones y puestas a punto;
- el análisis de impacto;
- la reverificación y la revalidación de los datos y resultados;
- todos los documentos afectados por las actividades de modificación y de actualización.

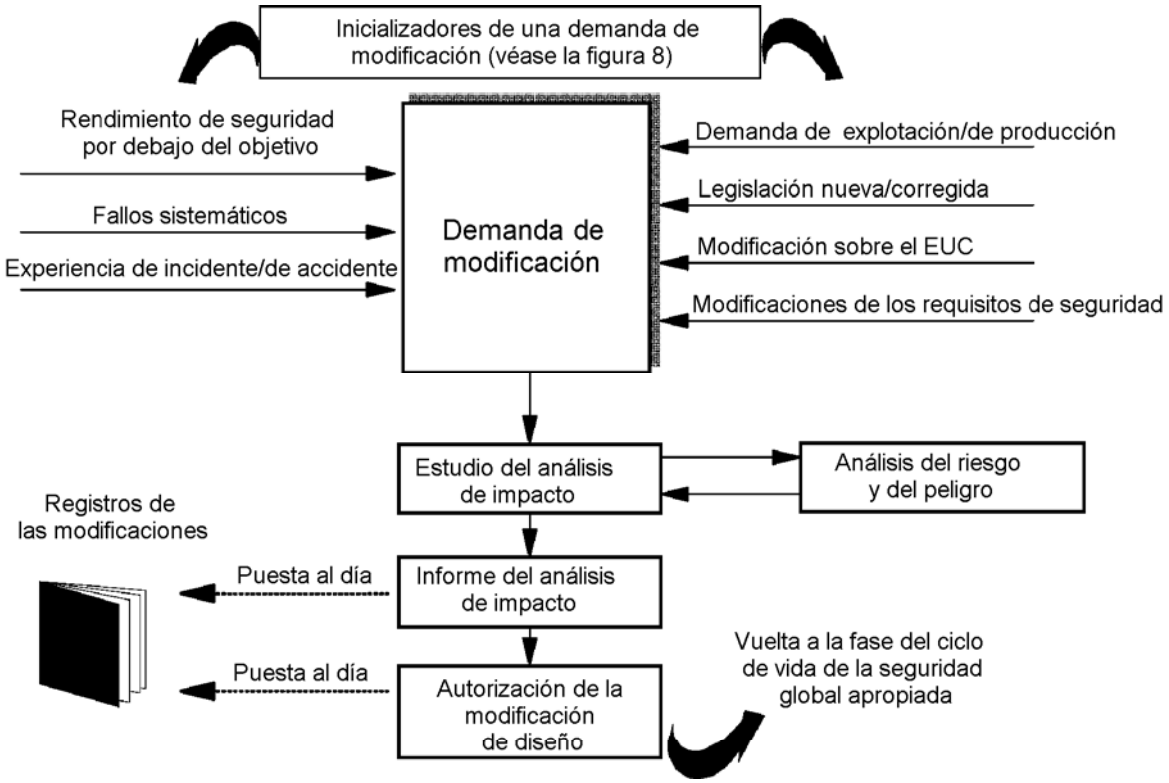


Fig. 9 – Ejemplo de modelo de procedimiento para las modificaciones

7.17 Puesta fuera de servicio o descatalogación

NOTA – Esta fase corresponde a la etapa 16 de la figura 2.

7.17.1 Objetivo. El objetivo de los requisitos de este apartado es asegurar que la seguridad funcional para los sistemas de seguridad E/E/PE es apropiada a las circunstancias durante y después de las actividades de puesta fuera de servicio o descatalogación del EUC.

7.17.2 Requisitos

7.17.2.1 Antes de realizar cualquier actividad de puesta fuera de servicio o descatalogación, se debe realizar un análisis de impacto. Éste debe constar de una evaluación del impacto de la actividad propuesta de puesta fuera de servicio o descatalogación sobre la seguridad funcional de todo sistema de seguridad E/E/PE asociado al EUC. El análisis de impacto también debe tener en cuenta los EUCs adjuntos y el impacto sobre los sistemas de seguridad E/E/PE. La evaluación debe incluir un análisis de peligro y de riesgo suficiente para determinar la extensión y la profundidad que deben cubrir las fases globales ulteriores del ciclo de vida de la seguridad del E/E/PES o del software.

7.17.2.2 Los resultados obtenidos en el apartado 7.17.2.1 deben documentarse.

7.17.2.3 La fase de puesta fuera de servicio o descatalogación sólo debe iniciarse por la emisión de una demanda oficial de acuerdo con los procedimientos para la gestión de la seguridad funcional (véase el capítulo 6).

7.17.2.4 La autorización de realizar la puesta fuera de servicio o descatalogación demandada debe depender de los resultados del análisis de impacto.

7.17.2.5 Antes de realizar la puesta fuera de servicio o descatalogación, debe prepararse un plan. Éste debe constar de los procedimientos para:

– parada definitiva de los sistemas de seguridad E/E/PE;

– desmantelamiento de los sistemas de seguridad E/E/PE.

7.17.2.6 Si una de las actividades de puesta fuera de servicio o descatalogación ejerce un impacto sobre la seguridad funcional de cualquier sistema de seguridad E/E/PE, éste debe llevar un retorno a la fase global apropiada del ciclo de vida del software o sistemas de seguridad E/E/PE. Todas las fases siguientes deben ejecutarse de acuerdo con los procedimientos especificados en esta norma para los niveles de integridad de seguridad especificados para los sistemas de seguridad E/E/PE.

NOTA 1 – Puede ser necesario poner en marcha un análisis completo de peligro y de riesgo, que podrá generar una necesidad de diferente nivel de integridad de seguridad para los sistemas de seguridad E/E/PE.

NOTA 2 – Los requisitos de seguridad funcional durante la fase de puesta fuera de servicio o descatalogación pueden ser diferentes de los requeridos durante la fase de explotación.

7.17.2.7 Se debe establecer y mantener una documentación cronológica. Ésta debe contener los documentos detallando el proceso de puesta fuera de servicio o descatalogación, y debe hacer referencia:

– al plan utilizado para las actividades de puesta fuera de servicio o descatalogación;

– al análisis de impacto.

7.18 Verificación

7.18.1 Objetivo. El objetivo de los requisitos de este apartado es demostrar, para cada fase de los ciclos de vida globales de la seguridad de los E/E/PES y del software (mediante revisiones, análisis y/o ensayos), que los datos de salida cumplen en todos los aspectos los objetivos y los requisitos especificados para esta fase.

7.18.2 Requisitos

7.18.2.1 Para cada fase de los ciclos de vida globales de la seguridad de los E/E/PES y del software, debe establecerse un plan para verificación en paralelo con el desarrollo de esta fase.

7.18.2.2 El plan de verificación debe documentar o hacer referencia a los criterios, técnicas, herramientas antes de utilizarse en actividades de verificación.

7.18.2.3 La verificación debe realizarse de acuerdo con el plan de verificación.

NOTA – La sección de las técnicas y medidas para la verificación, y el grado de independencia para las actividades de verificación, dependerá de un cierto número de factores y se puede especificar en las normas de aplicación sectorial.

Estos factores podrán incluir, por ejemplo:

– tamaño del proyecto;

– grado de complejidad;

– grado de innovación del diseño;

– grado de innovación de la tecnología.

7.18.2.4 La información sobre las actividades de verificación debe reunirse y documentarse como ensayo de que la fase en curso de verificación ha sido, en todos los aspectos, correctamente realizada.

8 EVALUACIÓN DE LA SEGURIDAD FUNCIONAL

8.1 Objetivo

El objetivo de los requisitos de este capítulo es investigar y elaborar un juicio sobre la seguridad funcional realizada por los sistemas de seguridad E/E/PE.

8.2 Requisitos

8.2.1 Una o varias personas deben ser asignadas para realizar una evaluación de la seguridad funcional para elaborar un juicio sobre la seguridad funcional realizada por los sistemas de seguridad E/E/PE.

8.2.2 Los responsables de esta evaluación de la seguridad funcional deben poder contactar con todas las personas implicadas en cualquier actividad del ciclo de vida de la seguridad global del E/E/PES o del software, y tener acceso a toda la información y todos los equipos (hardware y software) pertinentes.

8.2.3 La evaluación de la seguridad funcional debe aplicarse a todas las fases de los ciclos de vida globales de la seguridad de los sistemas E/E/PE y del software. Los responsables de la evaluación de la seguridad funcional deben tener en cuenta las actividades llevadas a cabo, y los datos de las salidas obtenidos durante cada fase de los ciclos de vida globales de la seguridad de los E/E/PES y del software, y juzgar en qué medida se cumplen los objetivos y los requisitos de esta norma.

8.2.4 La evaluación de la seguridad funcional debe realizarse a lo largo de los ciclos de vida globales de los E/E/PES y del software y puede realizarse después de cada fase del ciclo de vida de la seguridad o después de un conjunto de fases del ciclo de vida de la seguridad, sujeto al requisito prioritario que requiere que se realice una evaluación de la seguridad funcional antes de que se presenten los peligros determinados.

8.2.5 Si se utilizan unas herramientas durante el diseño o la evaluación para cualquier actividad del ciclo de vida de la seguridad global del E/E/PES o del software, conviene someterlas a una evaluación de la seguridad funcional.

NOTA 1 – Como ejemplo de herramienta, citamos los sistemas de CAD/CAM, los compiladores y los sistemas objetivo principales.

NOTA 2 – El grado de evaluación de la utilización de estas herramientas dependerá de su impacto sobre la seguridad funcional de los sistemas de seguridad E/E/PE.

8.2.6 La evaluación de la seguridad funcional debe tener en cuenta los puntos siguientes:

– trabajo realizado después de la evaluación de la seguridad funcional precedente (que, normalmente, englobará a las fases precedentes del ciclo de vida de la seguridad);

– planes o estrategia para la implementación de ulteriores evaluaciones de la seguridad funcional de los ciclos de vida de la seguridad global de los E/E/PES y del software;

– recomendaciones de las evaluaciones de la seguridad funcional precedentes, y la extensión de los cambios realizados posteriormente.

8.2.7 Las actividades de evaluación de la seguridad funcional para las distintas fases de los ciclos de vida de la seguridad global de los E/E/PES y del software deben ser coherentes y planificados.

8.2.8 El plan para la evaluación de la seguridad funcional debe especificar:

– responsabilidades de la evaluación de la seguridad funcional;

– resultados de cada evaluación de la seguridad funcional;

– campo de aplicación de evaluación de la seguridad funcional.

NOTA – Durante la definición del campo de aplicación de la evaluación de la seguridad funcional, será necesario especificar los documentos, y sus estados, que se utilizarán como datos de entrada para cada actividad de evaluación.

– organismos de seguridad implicados;

– recursos necesarios;

– grado de independencia de los responsables de la evaluación de la seguridad funcional;

– competencia de las responsabilidades de la evaluación de la seguridad funcional relativa a la aplicación.

8.2.9 Antes de realizar la evaluación de la seguridad funcional, el plan para la evaluación de la seguridad funcional debe ser aprobada por los responsables de la evaluación de la seguridad funcional y por los responsables de la gestión de la seguridad funcional para las fases del ciclo de vida antes de evaluarse.

8.2.10 Como conclusión de la evaluación de la seguridad funcional, deben emitirse unas recomendaciones para la aceptación, la aceptación condicional o el rechazo.

8.2.11 Los responsables de la evaluación de la seguridad funcional deben ser competentes para las actividades llevadas a cabo, y se recomienda prestar atención a los factores para la evaluación de la competencia indicados en el anexo B.

8.2.12 Excepto si una norma de aplicación sectorial internacional indica lo contrario, el grado mínimo de independencia de los responsables de la evaluación de la seguridad funcional debe ser como el especificado en las tablas 4 y 5. Las recomendaciones de las tablas son las siguientes:

– HR: El grado de independencia especificado es altamente recomendado (Hihgly Recommended) como un mínimo para la "consecuencia" especificada (tabla 4) o el nivel de integridad de seguridad (tabla 5). En caso de adopción de un grado de independencia inferior, conviene explicar en detalle por qué no se ha utilizado el grado HR.

– NR: El grado de independencia especificado se considera como insuficiente y es claramente no recomendado (Not Recommended) para la "consecuencia" especificada (tabla 4) o el nivel de integridad de seguridad (tabla 5). En caso de adopción de este grado de independencia, conviene explicar en detalle los motivos de esta elección.

– –: El grado de independencia especificada no tiene recomendación ni a favor ni en contra de su adopción.

NOTA 1 – Antes de la aplicación de la tabla 4, será necesario definir las categorías de "consecuencias", teniendo en cuenta las buenas prácticas habituales del sector de aplicación. Las "consecuencias" son las que podrían producirse en caso de fallo de los sistemas de seguridad E/E/PE cuando su funcionamiento sea requerido.

NOTA 2 – Según la organización de la empresa y de la experiencia en la compañía, el requisito para las personas y servicios independientes puede tener que cumplirse utilizando una organización exterior. Por contra, las empresas que tienen organizaciones internas cualificadas para la evaluación del riesgo y de su aplicación a los sistemas de seguridad, que son independientes y separadas (por medio de la jerarquía y otros medios) de los responsables del desarrollo principal, pueden ser capaces de utilizar sus propios recursos para cumplir los requisitos que se aplican a una organización independiente.

NOTA 3 – Véanse los apartados 3.8.10, 3.8.11 y 3.8.12 de la Norma CEI 61508-4 para las definiciones, respectivamente, de las "personas independientes", del "servicio independiente" y de la "organización independiente".

8.2.13 En el marco de las tablas 4 y 5, se aplica bien HR^1, o bien HR^2 (no ambos), en función de un cierto número de factores propios de la aplicación. Si HR^1 se aplica, conviene considerar HR^2 como que no es un requisito; si se aplica HR^2, conviene considerar HR^1 como NR (no recomendado). Si no existen normas de aplicación sectorial, conviene explicar en detalle las razones de la elección de HR^1 o HR^2. Los factores que tienden a hacer HR^2 más apropiado que HR^1 son:

– falta de experiencia anterior de un diseño del sistema similar;

– mayor nivel de complejidad;

– mayor novedad del diseño;

– mayor novedad de la tecnología;

– falta de normalización de las particularidades del diseño.

8.2.14 En el marco de la tabla 5, los grados mínimos de independencia deben basarse en la función de seguridad, ejecutada por el sistema de seguridad E/E/PE, que posee el mayor nivel de integridad de seguridad.

Tabla 4
Grados mínimos de independencia de los responsables de la evaluación de la seguridad funcional [fases del ciclo de vida de la seguridad global de la 1 a la 8 y de la 12 a la 16 inclusive (véase la figura 2)]

Grado mínimo de independencia	Consecuencia (véase la nota 2)			
	A	B	C	D
Persona independiente	HR	HR[1]	NR	NR
Servicio independiente	–	HR[2]	HR[1]	NR
Organización independiente (véase la nota 2 del apartado 8.2.12)	–	–	HR[2]	HR

NOTA 1 – Véanse los apartados 8.2.12 (notas incluidas) y 8.2.13 para los detalles de interpretación de esta tabla.

NOTA 2 – Las consecuencias típicas pueden ser: consecuencia A – daño leve (por ejemplo pérdida temporal de función); consecuencia B – daño grave y permanente de una o varias personas, muerte de una persona; consecuencia C – muerte de varias personas; consecuencia D: muchas personas muertas.

Tabla 5
Grados mínimos de independencia de los responsables de la evaluación de la seguridad funcional [fase 9 del ciclo de vida de la seguridad, incluyendo todas las fases de los ciclos de vida de la seguridad del E/E/PES y del software (véanse las figuras 2, 3 y 4)]

Grado mínimo de independencia	Nivel de integridad de seguridad			
	1	2	3	4
Persona independiente	HR	HR[1]	NR	NR
Servicio independiente	–	HR[2]	HR[1]	NR
Organización independiente (véase la nota 2 del apartado 8.2.12)	–	–	HR[2]	HR

NOTA – Véanse los apartados 8.2.12 (notas incluidas), 8.2.13 y 8.2.14 para los detalles de interpretación de esta tabla.

ANEXO A (Informativo)

EJEMPLO DE ESTRUCTURA DE LA DOCUMENTACIÓN

A.1 Generalidades

Este anexo propone un ejemplo de estructura de la documentación y un método de especificación de los documentos para estructurar la información con el fin de cumplir los requisitos del capítulo 5. La documentación debe contener la información necesaria y suficiente para la ejecución eficaz de:

– cada fase de los ciclos de vida de la seguridad globales de los E/E/PES y del software;

– gestión de la seguridad funcional (capítulo 6);

– evaluaciones de la seguridad funcional (capítulo 8).

La construcción de la información suficiente dependerá de un cierto número de factores, incluyendo la complejidad y el tamaño de los sistemas de seguridad E/E/PE y los requisitos relativos a las aplicaciones específicas. La documentación necesaria se puede especificar en las normas internacionales de aplicación sectorial.

La cantidad de información en cada documento puede ir desde algunas líneas a algunas páginas, y el conjunto completo de información se puede dividir y presentar en varios documentos físicos o en un solo documento físico. La estructura física de la documentación dependerá de la complejidad y del tamaño de los sistemas de seguridad E/E/PE y tendrá en cuenta los procedimientos de la empresa así como los hábitos de trabajo del sector de aplicación específico.

El ejemplo de estructura de la documentación indicado en este anexo se propone para ilustrar una forma entre otras de estructurar la información y la forma en la que los documentos se podrían titular. Véase la referencia [4]* del anexo C para más detalles.

Un documento es una cantidad estructurada de información destinada a la percepción humana, pudiendo intercambiarse entre los usuarios y/o los sistemas (véase la Norma ISO 8613-1) [5]*. Este término no se aplica sólo a los documentos tradicionales, sino también a los conceptos como los ficheros de datos y las bases de datos de información.

En esta norma, el término “documento” significa generalmente “información” más que documento físico, excepto si se indica específicamente lo contrario o si el contexto del capítulo o del apartado en el que se ha empleado conduce a otro significado. Los documentos pueden estar disponibles bajo distintas formas para presentaciones (por ejemplo en papel, transparencia o cualquier soporte de datos que se pueda presentar en pantalla).

El ejemplo de estructura de la documentación de este anexo especifica los documentos en dos partes:

– **tipo de documento;**

– **actividad u objetivo.**

El tipo de documento se define en la Norma CEI 61355 [3] y caracteriza el contenido del documento, por ejemplo una “descripción de función” o un “diagrama de circuito”. La actividad o el objeto describe el campo de aplicación del contenido, por ejemplo “sistema de control de bomba”.

Los tipos de documentos de base especificados en este anexo son:

– **especificación** – especifica una función o actividad descrita (por ejemplo una especificación de requisitos);

---

* Las cifras entre corchetes se refieren a la bibliografía dada en el anexo C.

– **descripción** – especifica una función, un proyecto, un funcionamiento o actividad previsto o real (por ejemplo una descripción de función);

– **instrucción** – especifica en detalle las instrucciones explicando cuándo y cómo realizar ciertos trabajos (por ejemplo, una instrucción de operario);

– **plan** – especifica el plan explicando cómo, cuándo y por quién se deben realizar las actividades específicas (por ejemplo, un plan de mantenimiento);

– **diagrama** – especifica la función con la ayuda de un diagrama (símbolos y líneas) representando las señales entre los símbolos;

– **lista** – proporciona información bajo la forma de una lista (por ejemplo, listas de códigos, de señales);

– **registro** –proporciona información de los eventos en forma de registro cronológico;

– **informe** – describe los resultados de las actividades tales como las encuestas, las evaluaciones, los ensayos, etc. (por ejemplo, un informe de ensayo);

– **demanda** – proporciona una descripción de las acciones demandadas y que se deben aprobar y especificar ulteriormente (por ejemplo, demanda de mantenimiento).

Los tipos básicos de documento pueden tener un sufijo, tal como especificación de **requisitos** o especificación de **ensayo**, que caracterizan el contenido.

A.2 Estructura del documento del ciclo de vida de la seguridad

Las tablas A.1, A.2 y A.3 proporcionan un ejemplo de estructura de la documentación para estructurar la información para satisfacer a los requisitos especificados en el capítulo 5. Las tablas indican la fase del ciclo de vida de la seguridad que se asocia principalmente a los documentos (generalmente la fase en la que se elaboran). Los nombres dados a los documentos en las tablas están de acuerdo con el esquema expuesto en el capítulo A.1.

Además de los documentos listados en las tablas A.1, A.2 y A.3, puede haber documentos suplementarios que dan una información detallada suplementaria o una información estructurada en un objetivo específico, por ejemplo una listas de piezas, unas listas de señales, unas listas de cables, unas tablas de cableado, unos diagramas de bucle, unas listas de variables.

NOTA – Como ejemplo de estas variables, se citan los valores para los reguladores, los valores de alarma para las variables, las prioridades en la ejecución de tareas por el ordenador. Ciertos valores de las variables pueden darse antes de la entrada del sistema, otros pueden darse durante la puesta en servicio o el mantenimiento.

Tabla A.1
Ejemplo de estructura de la documentación para la información relacionada con el ciclo de vida de la seguridad global

Fase del ciclo de vida de la seguridad global	Información
Concepto	Descripción (concepto global)
Definición global del objeto y campo de aplicación	Descripción (definición global del objeto y campo de aplicación)
Análisis de peligro y de riesgo	Descripción (análisis de peligro y de riesgo)
Requisitos globales de seguridad	Especificación (requisitos globales de seguridad, incluyendo: funciones de seguridad globales e integridad de seguridad global)
Asignación de los requisitos de seguridad	Descripción (asignación de los requisitos de seguridad)
Planificación global de la explotación y del mantenimiento	Plan (explotación y mantenimiento globales)
Planificación global de la validación de la seguridad	Plan (validación global de la seguridad)
Planificación global de la instalación y de la puesta en servicio	Plan (instalación global); Plan (puesta en servicio global)
Realización	Realización de los sistemas de seguridad E/E/PE (véanse las Normas CEI 61508-2 y CEI 61508-3)
Instalación y puesta en servicio globales	Informe (instalación global); Informe (puesta en servicio global)
Validación global de la seguridad	Informe (validación global de la seguridad)
Explotación y mantenimiento globales	Registro (explotación y mantenimiento globales)
Modificación y actualización globales	Demanda (modificación global); Informe (análisis de impacto de las modificaciones y puestas a punto globales); Registro (modificación y actualización globales)
Puesta fuera de servicio o descatalogación	Informe (análisis de impacto de la puesta fuera de servicio o descatalogación global); Plan (puesta fuera de servicio o descatalogación global); Registro (puesta fuera de servicio o descatalogación global)
Relativo a todas las fases	Plan (seguridad); Plan (verificación); Informe (verificación); Plan (evaluación de la seguridad funcional); Informe (evaluación de la seguridad funcional)

Tabla A.2
Ejemplo de estructura de la documentación para la información relacionada con el ciclo de vida de la seguridad del sistema E/E/PE

Fase del ciclo de vida de la seguridad del sistema E/E/PE	Información
Requisitos de seguridad de los E/E/PES	Especificación (requisitos de seguridad de los E/E/PES, incluyendo: las funciones de seguridad y la integridad de seguridad del E/E/PES)
Planificación de la validación del E/E/PES	Plan (validación de la seguridad del E/E/PES)
Diseño y desarrollo del E/E/PES	
Arquitectura del E/E/PES	Descripción (diseño de la arquitectura del E/E/PES, incluyendo: la arquitectura del hardware y la arquitectura del software); Especificación (ensayos de integración de la electrónica programable); Especificación (ensayos de integración del hardware electrónico programable y no electrónico programable)
Arquitectura del hardware	Descripción (diseño de la arquitectura del hardware); Especificación (ensayo de integración de la arquitectura del hardware)
Diseño del módulo del hardware	Especificación (diseño de los módulos del hardware); Especificaciones (ensayo de los módulos del hardware)
Construcción y/o compra de componentes	Módulos del hardware; Informe (ensayo de los módulos del hardware)
Integración de la electrónica programable	Informe (ensayo de integración de la electrónica programable y del software) (véase la tabla A.3)
Integración del E/E/PES	Informe (ensayo de integración de la electrónica programable y otro hardware)
Procedimientos de explotación y mantenimiento del E/E/PES	Instrucción (usuario) Instrucción (explotación y mantenimiento)
Validación de la seguridad del E/E/PES	Informe (validación de la seguridad del E/E/PES)
Modificación del E/E/PES	Instrucción (procedimientos de modificación del E/E/PES); Demanda (modificación del E/E/PES); Informe (análisis de impacto de una modificación del E/E/PES); Registro (modificación del E/E/PES)
Relativo a todas las fases	Plan (seguridad del E/E/PES); Plan (verificación del E/E/PES); Informe (verificación del E/E/PES); Plan (evaluación de la seguridad funcional del E/E/PES); Informe (evaluación de la seguridad funcional del E/E/PES)

Tabla A.3
Ejemplo de estructura de la documentación para la información relacionada con el ciclo de vida de la seguridad del software

Fase del ciclo de vida de la seguridad del software	Información
Requisitos de seguridad del software	Especificación (requisitos de seguridad del software, incluyendo: las funciones de seguridad del software y la integridad de seguridad del software)
Planificación de la validación de la seguridad del software	Plan (validación de la seguridad del software)
Diseño y desarrollo del software	
Arquitectura del software	Descripción (diseño de la arquitectura del software) (véase la tabla A.2 para la descripción de la arquitectura del hardware);
	Especificación (ensayos de integración de la arquitectura del software);
	Especificación (ensayos de integración de la electrónica programable y del software);
	Instrucción (herramientas de desarrollo y manual de codificación)
Diseño del sistema del software	Descripción (diseño del sistema del software);
	Especificación (ensayo de integración del sistema del software)
Diseño del módulo del software	Especificación (diseño del módulo del software);
	Especificaciones (ensayo del módulo del software)
Codificación	Lista (código fuente);
	Informe (ensayo del módulo del software);
	Informe (revisión de código)
Ensayo del módulo del software	Informe (ensayo de del módulo del software)
Integración del software	Informe (ensayo de integración del módulo del software);
	Informe (ensayo de integración del sistema del software);
	Informe (ensayo de integración de la arquitectura del software)
Integración de la electrónica programable	Informe (ensayo de integración de la electrónica programable y del software)
Procedimientos de explotación y mantenimiento del software	Instrucción (usuario);
	Instrucción (explotación y mantenimiento)
Validación de la seguridad del software	Informe (validación de la seguridad del software)
Modificación del software	Instrucción (procedimientos de modificación del software);
	Demanda (modificación del software);
	Informe (análisis de impacto de una modificación del software);
	Registro (modificación del software)
Relativo a todas las fases	Plan (seguridad del software);
	Plan (verificación del software);
	Informe (verificación del software);
	Plan (evaluación de la seguridad funcional del software);
	Informe (evaluación de la seguridad funcional del software)

A.3 Estructura física del documento

La estructura física de la documentación corresponde a la forma como los diferentes documentos son combinados en documentos, juegos de documentos, clasificadores y grupos de clasificadores. La figura A.1 presenta dos ejemplos de estos conjuntos de clasificadores estructurados según los grupos de usuarios. El mismo documento puede aparecer en diferentes conjuntos.

En un sistema grande y complejo, es muy probable que los numerosos documentos sean divididos en varios clasificadores. En un sistema pequeño de baja complejidad, con un número limitado de documentos físicos, pueden combinarse en un clasificador con diferentes etiquetas intercaladas para los diferentes conjuntos de documentos (véase la figura A.2).

La estructura física suministra un medio de selección de la documentación necesaria para actividades específicas por personas o grupos de personas que realizan estas actividades. En consecuencia, algunos documentos físicos pueden aparecer en varios conjuntos de clasificadores o cualquier otro medio (por ejemplo, los discos de ordenador).

NOTA – La información requerida por los documentos de la tabla A.1 puede contenerse en distintos conjuntos de documentos presentados en las figuras A.1 y A.2. Por ejemplo, en el grupo para la ingeniería, se podrá encontrar unos documentos como la descripción del análisis de peligro y de riesgo y/o la especificación de los requisitos globales de seguridad.

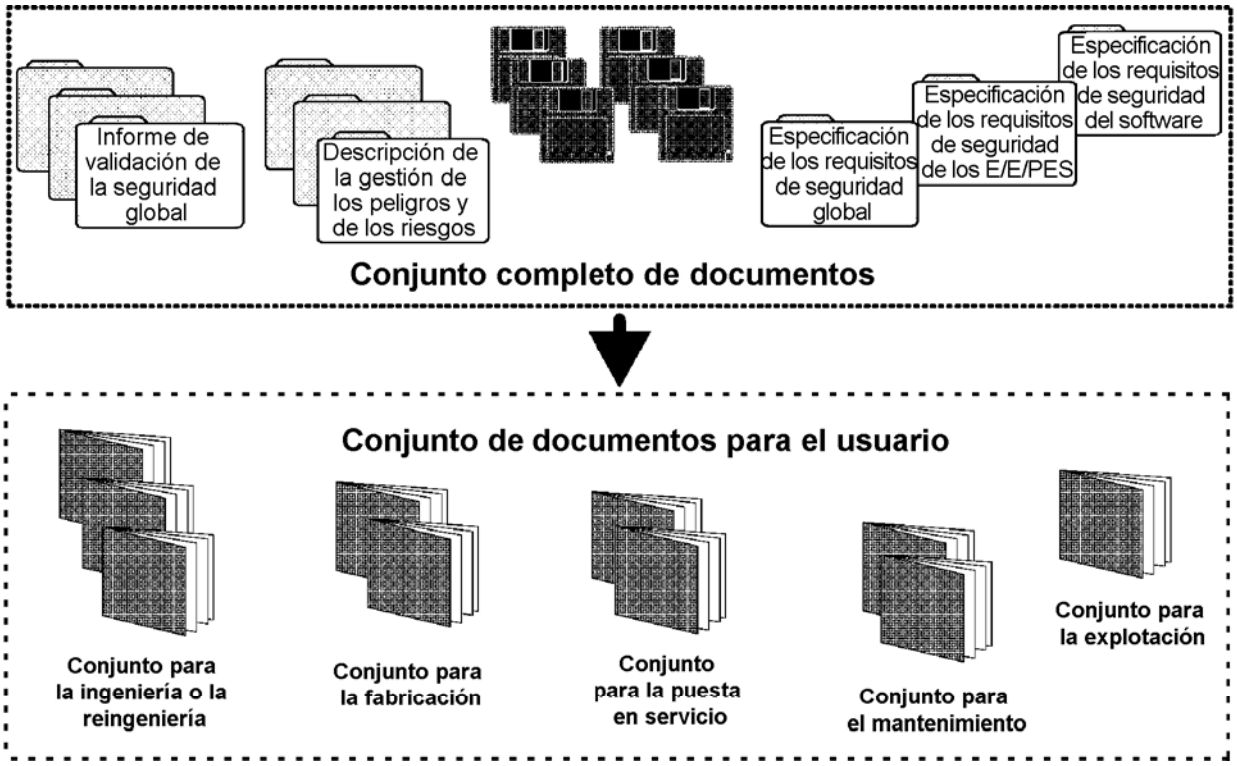


Fig. A.1 – Estructuración de la información en conjuntos de documentos para los grupos de usuarios

Fig. A.2 – Estructuración de la información para los grandes sistemas complejos y los pequeños sistemas de baja complejidad

A.4 Lista de los documentos

La lista de los documentos incluirá normalmente la información siguiente:

- número de gráficos o documentos;
- índice de revisión;
- código de designación del documento;
- título;
- fecha de revisión;
- soporte de datos.

Esta lista puede tener en cuenta diferentes aspectos, por ejemplo, los de una base de datos clasificada de acuerdo con los números del gráfico, del documento o el código de designación del documento. El código de designación del documento puede contener la designación de referencia para la función, la localización o el producto descrito en el documento, haciendo de este código una herramienta de búsqueda de información potente.

ANEXO B (Informativo)

COMPETENCIA DE LAS PERSONAS

B.1 Objetivo

Este anexo resume los puntos a tener en consideración para asegurar que las personas que tienen la responsabilidad para cualquier actividad del ciclo de vida de la seguridad global del E/E/PES o del software son competentes para desempeñar estas responsabilidades.

B.2 Consideraciones generales

Se recomienda que todas las personas implicadas en cualquier actividad del ciclo de vida de la seguridad global del E/E/PES o del software, incluyendo las actividades de gestión, posean la formación apropiada, el conocimiento técnico, la experiencia y las cualificaciones relevantes de los cargos específicos que tendrán que realizar.

Se recomienda evaluar la formación, la experiencia y la cualificaciones de cualquier persona implicada en cualquier actividad del ciclo de vida de la seguridad global del E/E/PES o del software, incluyendo cualquier actividad de gestión de la seguridad funcional, relacionada con la aplicación en particular.

Conviene considerar los siguientes factores, durante la evaluación de la competencia de las personas que van a realizar su trabajo:

a) conocimientos de ingeniería apropiados al objeto y campo de aplicación;

b) conocimientos de ingeniería apropiados a la tecnología (por ejemplo, ingeniería eléctrica, electrónica, electrónica programable, software);

c) conocimientos de ingeniería de la seguridad apropiados a la tecnología;

d) conocimientos del marco legal y reglamentario relacionado con la seguridad;

e) consecuencias en el caso de un fallo de los sistemas de seguridad E/E/PE; conviene tener una especificación y una evaluación de competencia tanto más rigurosa cuanto más importantes sean las consecuencias;

f) niveles de integridad de seguridad de los sistemas de seguridad E/E/PES; conviene tener una especificación y una evaluación de competencia tanto más rigurosa cuanto más elevados sean los niveles de integridad de seguridad;

g) innovación en el diseño, los procedimientos de diseño o aplicación; conviene tener una especificación y una evaluación de competencia tanto más rigurosa cuanto más nuevos o innovadores sea el diseño, los procedimientos de diseño o la aplicación;

h) experiencia acumulada y su relevancia en las tareas específicas antes de realizarse y de la tecnología antes de ser empleada; conviene que las experiencias adquiridas por la experiencia y las exigidas para realizar las tareas específicas sean tanto más próximas cuanto más elevados sean los niveles de competencia exigidos;

i) relevancia de las cualificaciones de las tareas específicas que deben realizarse.

Conviene documentar la formación, la experiencia y la cualificaciones de todas las personas implicadas en cualquier actividad del ciclo de vida de la seguridad global del E/E/PES o del software.

ANEXO C (Informativo)

BIBLIOGRAFÍA

[1] IEC 60300-3-1:1991 – *Dependability management. Part 3: Application guide. Section 1: Analysis techniques for dependability: Guide on methodology.*

[2] IEC 60300-3-9:1995 – *Dependability management. Part 3: Application guide. Section 9: Risk analysis of technological systems.*

[3] IEC 61355:1997 – *Classification and designation of documentations for plants, systems and equipment.*

NOTA – Armonizada como Norma EN 61355:1997* (sin ninguna modificación).

[4] IEC 61506:1997 – *Industrial-process measurement and control. Documentation of application software.*

[5] ISO 8613-1:1994 – *Information technology. Open Document Architecture (ODA) and interchange format: Introduction and general principles.*

[6] ISO 10007:1995 – *Quality management. Guidelines for configuration management.*

[7] ISO/IEC TR 15846 – *Information technology. Software life cycle processes. Configuration management for software.*

[8] ANSI/ISA S84:1996 – *Application of safety Instrumented Systems for the Process Industries.*

[9] *Procedures for treating common cause failures in safety and reliability studies. Procedural framework and examples*, NUREG/CR-4780, Volume 1, January 1988.

[10] *Procedures for treating common cause failures in safety and reliability studies. Analytical background and techniques*, NUREG/CR-4780, Volume 2, January 1989.

* UNE-EN 61355:1998.

ANEXO ZA (Normativo)

OTRAS NORMAS INTERNACIONALES CITADAS EN ESTA NORMA CON LAS REFERENCIAS DE LAS NORMAS EUROPEAS CORRESPONDIENTES

Esta norma europea incorpora disposiciones de otras normas por su referencia, con o sin fecha. Estas referencias normativas se citan en los lugares apropiados del texto de la norma y se relacionan a continuación. Las revisiones o modificaciones posteriores de cualquiera de las normas citadas con fecha, sólo se aplican a esta norma europea cuando se incorporan mediante revisión o modificación. Para las referencias sin fecha se aplica la última edición de esa norma (incluyendo sus modificaciones).

NOTA – Cuando una norma internacional haya sido modificada por modificaciones comunes CENELEC, indicado por (mod), se aplica la EN/HD correspondiente.

Norma Internacional	Fecha	Título	EN/HD	Fecha	Norma UNE correspondiente[1)]
Guía ISO/CEI 51	1990	Directrices para incluir en las normas los aspectos relacionados con la seguridad	–	–	–
Guía CEI 104	1997	Elaboración de las publicaciones de seguridad y utilización de las publicaciones fundamentales de seguridad y de las publicaciones de grupos de seguridad	–	–	–
CEI 61508-2	2000	Seguridad funcional de los sistemas eléctricos /electrónicos/electrónicos programables relacionados con la seguridad. Parte 2: Requisitos para los sistemas eléctricos/electrónicos/ electrónicos programables relacionados con la seguridad	EN 61508-2	2001	PNE-EN 61508-2[2)]
CEI 61508-3 + corr. abril	1998 1999	Seguridad funcional de los sistemas eléctricos/ electrónicos/electrónicos programables relacionados con la seguridad. Parte 3: Requisitos del software (soporte lógico).	EN 61508-3	2001	UNE-EN 61508-3:2003
CEI 61508-4 + corr. abril	1998 1999	Seguridad funcional de los sistemas eléctricos/ electrónicos/electrónicos programables relacionados con la seguridad. Parte 4: Definiciones y abreviaturas	EN 61508-4	2001	PNE-EN 61508-4[2)]
CEI 61508-5 + corr. abril	1998 1999	Seguridad funcional de los sistemas eléctricos/ electrónicos/electrónicos programables relacionados con la seguridad. Parte 5: Ejemplos de métodos de determinación de los niveles de integridad de seguridad	EN 61508-5	2001	UNE-EN 61508-5:2003
CEI 61508-6	2000	Seguridad funcional de los sistemas eléctricos/ electrónicos/electrónicos programables relacionados con la seguridad .Parte 6: Directrices para la aplicación de las Normas CEI 61508-2 y CEI 61508-3	EN 61508-6	2001	PNE-EN 61508-6[2)]
CEI 61508-7	2000	Seguridad funcional de los sistemas eléctricos/ electrónicos/electrónicos programables relacionados con la seguridad. Parte 7: Presentación de técnicas y medidas	EN 61508-7	2001	PNE-EN 61508-7[2)]

1) Esta columna se ha introducido en el anexo original de la norma europea únicamente con carácter informativo a nivel nacional.
2) En preparación.

ANEXO NACIONAL (Informativo)

Las normas que se relacionan a continuación, citadas en esta norma europea, han sido incorporadas al cuerpo normativo UNE con los siguientes códigos:

Norma UNE	Título	Normas europeas e internacionales
UNE 200001-3-1:1998	Gestión de la confiabilidad. Parte 3: Guía de aplicación. Sección 1: Técnicas de análisis de la confiabilidad. Guía de metodología	CEI 60300-3-1:1991
UNE 200001-3-9:1999	Gestión de la confiabilidad. Parte 3: Guía de aplicación. Sección 9: Análisis de riesgo de sistemas tecnológicos	CEI 60300-3-9:1995
UNE-EN 61355:1998	Clasificación y designación de documentos para instalaciones industriales, sistemas y materiales	EN 61355:1997 CEI 61335:1997
UNE-EN ISO 10007:1997	Gestión de la calidad. Directrices para la gestión de la configuración	EN ISO 10007:1996 ISO 10007:1995

AENOR Asociación Española de Normalización y Certificación

Dirección C Génova, 6
28004 MADRID-España

Teléfono 91 432 60 00

Fax 91 310 40 32