

Guía de Seguridad 10.9

**Garantía de Calidad de las aplicaciones
informáticas relacionadas con la seguridad
de las instalaciones nucleares**

Madrid, 8 de octubre de 1998

© Copyright Consejo de Seguridad Nuclear, 1998

Publicado y distribuido por:
Consejo de Seguridad Nuclear
Justo Dorado, II. 28040-Madrid
<http://www.csn.es>
Peticones@csn.es

Imprime: ARTEGRAF, S.A.
Sebastián Gómez, 5. 28026 Madrid

ISBN: 84-87275-92-3
Depósito legal: M. 48.408-1998



Impreso en papel reciclado

Índice

1 Introducción	7
1.1. Objeto	7
1.2. Ámbito de aplicación	7
2 Antecedentes	7
3 Clasificación de las aplicaciones informáticas	8
4 Sistema de Garantía de Calidad de las aplicaciones informáticas	9
4.1. Criterios generales	10
4.2. Documentación general o básica de calidad	10
4.3. Documentación asociada al ciclo de vida	11
5 Implantación del Sistema de- Garantía de Calidad	12
6 Registros de Garantía de Calidad	13
7 Aplicaciones informáticas existentes	13
Definiciones	15
Bibliografía	16

Prólogo

Las aplicaciones informáticas están desempeñando actualmente un papel muy importante y progresivamente creciente en los procesos de diseño, fabricación, construcción, puesta en servicio, explotación y clausura relacionados con las instalaciones nucleares (I.I.NN).

El Consejo de Seguridad Nuclear (CSN), consciente de esta situación y de la necesidad de que los procesos señalados no sean causa de error, presenta en esta Guía recomendaciones sobre los requisitos de Garantía de Calidad a tener en cuenta en las aplicaciones informáticas relacionadas con la seguridad de las instalaciones nucleares.

El concepto establecido en la presente Guía, de aplicación informática relacionada con la seguridad, es coherente con la definición reflejada en la Guía de Seguridad del CSN GS-10.1 «Guía básica de garantía de calidad para instalaciones nucleares».

Para la realización de esta Guía se ha consultado la normativa nacional existente, UNE-73-404, así como otra normativa internacional encaminada al mismo fin. Como aspectos fundamentales se plantean: la clasificación de las aplicaciones informáticas, tanto las nuevas como las ya en uso, los criterios generales del Sistema de Garantía de Calidad que les aplica y su implantación.

Con estas recomendaciones, el CSN considera que las aplicaciones informáticas satisfarán unos requisitos de calidad equivalentes a los exigidos a los sistemas, equipos y componentes relacionados con la seguridad de las instalaciones nucleares.

1. Introducción

Objeto

Esta Guía establece recomendaciones sobre los requisitos de Garantía de Calidad que deben cumplir las aplicaciones informáticas (AI) relacionadas con la seguridad de las instalaciones nucleares.

Ámbito de aplicación

Dentro del alcance de la presente Guía se incluyen las AI utilizadas en las actividades de diseño, fabricación, construcción, puesta en marcha, explotación y clausura de las instalaciones nucleares, que estén relacionadas con la seguridad.

2. Antecedentes

Las AI utilizadas para las instalaciones nucleares (I.I.N.N.) pueden afectar al comportamiento de las estructuras, sistemas y componentes relacionados con la seguridad, así como al desarrollo de actividades de vigilancia, operativas, de mantenimiento, etc., efectuadas sobre los mismos, en cuyo caso las AI tendrían un impacto directo sobre las funciones de seguridad y salvaguardia destinadas a prevenir o mitigar las consecuencias de los accidentes postulados.

La normativa básica de Garantía de Calidad se refleja, como práctica recomendada, en la Guía de Seguridad del CSN 10.1, «Guía básica de Garantía de Calidad para instalaciones nucleares», así como en los requisitos y buenas prácticas contempladas en otras normas y publicaciones específicas.

Cumpliendo los objetivos de esta normativa, los procesos de definición, desarrollo, operación mantenimiento y cancelación, en definitiva el ciclo de vida, de determinadas AI han de someterse a los mismos controles de ingeniería, incluyendo la aplicación de requisitos de garantía de calidad, que otras actividades relacionadas con el diseño, construcción y explotación de las I.I.N.N.

En coherencia con lo anteriormente expuesto, la actuación de las I.I.N.N. ha de orientarse a planificar, implantar, controlar y optimizar un sistema de Garantía de Calidad

de las AI que aplique, tanto a las desarrolladas directamente por las propias instalaciones, como, a través de las oportunas verificaciones y controles, a las utilizadas en o para las mismas pero desarrolladas por otras organizaciones (ingenierías en procesos de diseño, suministradores en procesos de fabricación, reparación y mantenimiento, empresas de servicios de adiestramiento de operadores o de desarrollo de procesos informáticos, etc.).

3. Clasificación de las aplicaciones informáticas

Las organizaciones que utilicen AI, clasificarán dichas AI en relacionadas y no relacionadas con la seguridad.

Se considerarán AI relacionadas con la seguridad aquellas en las que incidencias en su funcionamiento pudieran provocar acciones, decisiones o inhibiciones que afecten negativamente a la seguridad nuclear. Asimismo, también entrarán dentro de esta clasificación, las AI utilizadas como herramientas para el desarrollo, prueba y mantenimiento de AI relacionadas con la seguridad, así como las bases de datos, librerías, etc. utilizadas por estas AI.

Las organizaciones mantendrán un listado, actualizado, donde figure la clasificación de seguridad de todas las AI utilizadas por las mismas.

Sin pretender establecer ningún criterio de exclusión ni de importancia, entre las AI que deben clasificarse como relacionadas con la seguridad y por lo tanto les sería aplicable lo descrito en la presente Guía, se encuentran aquellas que realicen, o contribuyan a realizar, las siguientes funciones o procesos:

- Diseño de estructuras, sistemas y componentes relacionados con la seguridad de las II.NN.
- Fabricación de estructuras, sistemas y componentes relacionados con la seguridad de las II.NN.
- Simulación del comportamiento de los parámetros dinámicos del emplazamiento.
- Simulación de comportamientos de estructuras, sistemas y componentes relacionados con la seguridad ante sucesos a los que deben hacer frente las II.NN.

- Diseño y fabricación de combustibles nucleares, diseño de recargas, cálculos nucleares y termohidráulicos, códigos de análisis de accidentes.
- Simuladores de entrenamiento para la operación normal y en emergencias.
- Determinación de términos fuente, cálculos dosimétricos, cálculo de blindajes.
- Vigilancia, control y protección de la instalación.
- Control o apoyo al control del cumplimiento de condiciones limitativas de operación, acciones y requisitos de vigilancia de las Especificaciones Técnicas de Funcionamiento y requisitos de otros documentos preceptivos de operación.
- Ayuda a los operadores en la toma de acciones en situaciones anormales de operación y de accidente.
- Planificación de indisponibilidades para garantizar la máxima seguridad de la instalación en recargas y paradas.
- Planificación y control del mantenimiento de estructuras, sistemas y componentes relacionados con la seguridad.
- Realización de análisis probabilísticos de seguridad.

4. Sistema de Garantía de Calidad de las aplicaciones informáticas

La finalidad del establecimiento e implantación de modo sistemático de requisitos de Garantía de Calidad aplicados a las AI es contribuir a conformar su calidad durante el desarrollo de su ciclo de vida, con el fin de garantizar, dentro de lo posible, lo siguiente:

- La detección y corrección de errores potenciales o latentes en las AI.
- La necesaria correspondencia que ha de existir entre las tareas realmente desarrolladas por las AI y las previamente requeridas.
- El mantenimiento eficaz de la configuración de las AI cuando se produzcan las convenientes adaptaciones o modificaciones.

- La optimización de las diferentes características o atributos de las AI (mantenibilidad, corrección, fiabilidad, integridad, estabilidad, portabilidad, facilidad de prueba, etc.) en función de los requisitos que se determinen.
- Para aquellas AI existentes en el mercado ampliamente contrastadas y aceptadas por todas las industrias, se justificará el cumplimiento o, en su caso, la no aplicabilidad de los requisitos de esta Guía.

4.1. Criterios generales

El Sistema de Garantía de Calidad de las AI ha de basarse fundamentalmente en dos tipos de documentos bien diferenciados, a saber:

- a) Documentación general o básica de calidad, que recoja la filosofía y requisitos generales del Sistema de Garantía de Calidad y que será de aplicación a todas las AI relacionadas con la seguridad de una determinada organización.
- b) Documentación asociada al ciclo de vida de las AI que plasme y planifique, con suficiente grado de detalle, los requisitos específicos para el diseño, desarrollo, implantación, utilización y control de cada una de las aplicaciones.

En el caso de coexistir varias versiones de una misma AI, se tratará cada una como independiente a los efectos de esta Guía.

4.2. Documentación general o básica de calidad

Los requisitos básicos del Sistema de Garantía de Calidad de las AI han de establecerse en un documento de carácter programático que podrá estar contenido en el Manual de Garantía de Calidad General de la organización, como un capítulo específico, o constituir un documento único independiente.

En el caso de optar por un documento independiente, éste ha de referenciarse en el Manual de Garantía de Calidad General de la organización.

Los aspectos que básicamente ha de contener la documentación programática, son los siguientes:

- Aplicabilidad.
- Organizaciones responsables de establecer, implantar y verificar el Sistema de Garantía de Calidad aplicable a las AI, así como sus funciones.
- Descripción de las fases del ciclo de vida de la AI.
- Requisitos de formación del personal involucrado en los distintos procesos.
- Documentación mínima requerida para las AI.
- Normativa aplicable, convenios, técnicas o metodologías a utilizar como guía para el desarrollo, implantación y control de las aplicaciones.
- Requisitos generales en cuanto a:
 - Establecimiento de requisitos/especificaciones.
 - Proceso de desarrollo.
 - Revisiones de requisitos, diseño, etc.
 - Procesos de verificación y validación.
 - Gestión de la configuración.
 - Detección de errores y acciones correctoras.
 - Control de acceso.
 - Mantenimiento de registros y documentos.
 - Control e identificación de herramientas, técnicas y metodologías.
 - Control de adquisiciones.
- Planificación, ejecución y seguimiento de auditorías.

Estos requisitos podrán desarrollarse en instrucciones o 'procedimientos de aplicabilidad general al conjunto de las AI.



Documentación asociada al ciclo de vida

Por cada nuevo proyecto de AI, se ha de elaborar, al comienzo de su ciclo de vida, un Plan de Garantía de Calidad que contemple con una mayor especificidad los requisitos establecidos en el documento general o básico indicado en el apartado 4.2. En la con-

fección de este plan, se recomienda utilizar como orientación la norma IEEE 730 «Software Quality Assurance Plans».

Si alguno de los aspectos de la documentación general básica de calidad no son aplicables a un proyecto específico de AI, se indicará que no es aplicable y las razones de su exclusión, permitiéndose de este modo establecer una gradación en los requisitos de Garantía de Calidad.

Como mínimo, durante el desarrollo del ciclo de vida, se ha de documentar lo siguiente:

- Planificación del proyecto -general y del desarrollo de la AI.
- Especificación de requisitos.
- Especificación de diseño.
- Plan e informes de verificación y validación.
- Manual de instalación y explotación.
- Plan de gestión de la configuración.
- Procedimientos específicos.
- Manual de usuario.

5. Implantación del Sistema de Garantía de Calidad

Como práctica recomendada, se considera que los criterios adoptados en la Norma UNE 73-404 «Garantía de Calidad en los Sistemas Informáticos Aplicados a Instalaciones Nucleares» y en la Norma ASME NQA-la «Quality Assurance Requirements for Nuclear Facility Applications» en su parte II, subparte 2.7 «Quality Assurance Requirements for Computer Software for Nuclear Facility Applications», son aceptables como base para implantar los requisitos del Sistema de Garantía de Calidad que han de establecerse en los documentos referenciados en los subapartados 4.2 y 4.3 de la presente Guía.

No obstante, ha de tenerse en cuenta que los criterios adoptados en la Norma UNE 73-404 relativos al equipo físico (conjunto de componentes físicos de un sistema informático, incluyendo los periféricos de adquisición y tratamiento de información), no serán aplicables dentro del contexto establecido para la presente Guía.

6. Registros de Garantía de Calidad

La organización responsable mantendrá registros que proporcionen evidencias objetivas de la idoneidad y funcionamiento adecuado del Sistema de Garantía de Calidad de las AI.

Del mismo modo que es aplicable a los registros de calidad derivados del Sistema General de Garantía de Calidad, se procederá a identificar, conservar y controlar adecuadamente estos registros y a clasificarlos en permanentes y no permanentes.

A continuación se relacionan, sin pretender establecer criterios de exclusión, los tipos de registros que podrían considerarse registros de calidad y que se elaboran en los procesos de establecimiento, implantación y verificación del Sistema de Garantía de Calidad de las AI:

- Listado de AI con su identificación.
- Documentación general o básica de calidad.
- Documentación asociada al ciclo de vida.
- Documentación justificativa de la clasificación de seguridad de las aplicaciones informáticas,
- Órdenes de compra.
- Informes y registros de verificación y validación.
- Programas de inspección/supervisión.
- Informes de seguimiento del proyecto.
- Partes de desviación.
- Informes de auditorías.
- Informes finales.

7. Aplicaciones informáticas existentes

El tratamiento a que han de someterse las AI que, con anterioridad a la fecha de aplicación de la presente Guía, estuvieran operativas, ha de responder a los siguientes hitos:

- Identificación de la AI.
- Determinación de si la AI está o no relacionada con la seguridad y en caso afirmativo, realización de una evaluación documentada del grado de cumplimiento de la misma con los requisitos expuestos en esta Guía definiendo los siguientes aspectos, como mínimo:
 - Capacidades y limitaciones de la AI.
 - Plan de pruebas requeridas para validar las capacidades de la aplicación dentro de las limitaciones.
 - Instrucciones para su utilización dentro de las limitaciones que se establezcan.
- Justificación documentada de las excepciones a los requisitos documentales establecidos en el subapartado 4.3 de la Guía. En todo caso estas AI deberán disponer como mínimo de un Plan de Calidad para las fases de operación, mantenimiento y cancelación, y de un Plan de Gestión de la Configuración para el control de cambios.

Definiciones

Las definiciones de los términos y conceptos contenidos en la presente Guía se corresponden con los contenidos en los siguiente documentos:

- Ley 2511964, de 29 de abril, sobre Energía Nuclear (BOE nº 107, de 4-05-64, artículo segundo) modificada por la Ley 54/1997, de 27 de noviembre, del Sector Eléctrico (BOE nº 285, de 21-11-97).
- Ley 1511980, de 22 de abril, de creación del Consejo de Seguridad Nuclear (BOE nº 100, de 25-04-80).
- Decreto 2869/1972, de 21 de julio, por el que se aprueba el Reglamento sobre Instalaciones Nucleares y Radiactivas (BOE nº 255, de 24-10-72).
- Real Decreto 53/1992, de 24 de enero, por el que se aprueba el Reglamento sobre Protección Sanitaria contra las Radiaciones Ionizantes (BOE nº 37, de 12-02-92).
- Norma UNE 73-404-98 «Garantía de calidad de los sistemas informáticos aplicados a instalaciones nucleares».

Además de lo anterior, dentro del contexto de esta Guía, el término Aplicación Informática se entiende como sigue:

- Aplicación Informática: Soporte lógico perteneciente a un sistema informático utilizado para realizar, o como apoyo a la realización de las actividades propias de una organización, o que forme parte integral de equipos y sistemas necesarios para la operación y control de sus instalaciones.

Bibliografía

La siguiente relación recoge los documentos más representativos a utilizar sobre la materia objeto de esta Guía.

- *UNE 73-4X-98. Garantía de calidad en los sistemas informáticos aplicados a instalaciones nucleares.*
- *Manual on Quality Assurance for Computer Software Related to the Safety of Nuclear Power Plants. Technical Reports Series nº 282. OIEA, Viena (1988).*
- *Verification and Validation of Software Related to Nuclear Power Plant Control and Instrumentation. Draft, chapter 0, Draft H. OIEA, Viena.*
- *Handbook of Software Quality Assurance Techniques Applicable to the Nuclear Industry. NUREG/CR-4640, PNL-5784. U.S. Nuclear Regulatory Commission, 1987.*
- *Quality Assurance Requirements of Computer Software for Nuclear Facility Applications. ASME NQA-1a-1995, Part II Subpart 2.7.*
- *IEEE Standard for Software Quality Assurance Plans. IEEE Std 730-1989.*
- *IEEE Guide for Software Quality Assurance Planning. IEEE Std 730.1-1995.*