GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-813)

Componentes certificados en el ENS

FEBRERO 2012

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

NIPO: 076-11-053-3

Tirada: 1000 ejemplares
Fecha de Edición: febrero de 2012
Raúl Siles ha participado en la elaboración y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

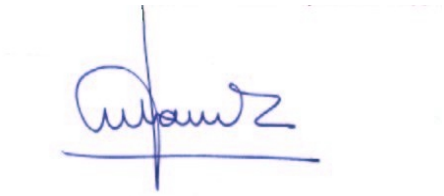
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Febrero de 2012



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. OBJETO

1. Este documento introduce los conceptos y define los criterios específicos que deben guiar y ayudar en la aplicación de los requisitos de adquisición y uso de componentes certificados en el Esquema Nacional de Seguridad (ENS).

2. Dentro de los diferentes aspectos certificables de la seguridad de las tecnologías de la información, esta guía desarrolla los criterios de aplicación de la certificación funcional de seguridad. Quedan fuera de esta guía, por no estar valoradas en el ENS, otras certificaciones no funcionales de seguridad, como puedan ser la criptológica o la TEMPEST.

2. FUNDAMENTO LEGISLATIVO

3. **La adquisición** por parte de las Administraciones públicas de productos y sistemas, en el marco del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, viene determinada por los siguientes artículos y cláusulas tipo.

> **Artículo 18. Adquisición de productos de seguridad.**
>
> 1. En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser utilizados por las Administraciones públicas se valorarán positivamente aquellos que tengan certificada **la funcionalidad de seguridad** relacionada con el objeto de su adquisición.
>
> 2. La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, **en el ámbito de la seguridad funcional.**
>
> 3. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados. El proceso indicado, se efectuará teniendo en cuenta los criterios y metodologías de evaluación, determinados por las normas internacionales que recoge la orden ministerial citada.

ANEXO V

Modelo de cláusula administrativa particular

«Cláusula administrativa particular.–En cumplimiento con lo dispuesto en el artículo 99.4 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, y el artículo 18 del Real Decreto ……/……, de …… de …… por el que se regula el Esquema Nacional de Seguridad, el licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, equipos, sistemas, aplicaciones o sus componentes, han sido previamente certificados por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

En el caso de que no exista la certificación indicada en el párrafo anterior, o esté en proceso, se incluirá, igualmente, referencia precisa, documentada y acreditativa de que son los más idóneos.

Cuando estos sean empleados para el tratamiento de datos de carácter personal, el licitador incluirá, también, lo establecido en la Disposición adicional única del Real Decreto 1720/2007, de 21 de diciembre.»

4. **El uso** de componentes certificados en el despliegue de productos y sistemas de las tecnologías de la información es una medida de seguridad que aplica con carácter general al nivel alto, y en algunos casos al nivel medio, tal como se detalla en el Anexo II del mismo ENS:

4.1.5 Componentes certificados [op.pl.5].

dimensiones	*todas*		
categoría	*básica*	*media*	*alta*
	no aplica	*no aplica*	*aplica*

Se utilizarán preferentemente sistemas, productos o equipos **cuyas funcionalidades de seguridad** y su nivel hayan sido evaluados conforme a normas europeas o internacionales y que estén certificados por entidades independientes de reconocida solvencia.

Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.

Tendrán la consideración de entidades independientes de reconocida solvencia las recogidas en los acuerdos o arreglos internacionales de reconocimiento mutuo de los certificados de la seguridad de la tecnología de la información u otras de naturaleza análoga.

5. Este criterio general de uso se aplica con las siguientes matizaciones:

4.2.5 Mecanismo de autenticación [op.acc.5].

Nivel ALTO

a) Los autenticadores se suspenderán tras un periodo definido de no utilización.

b) No se admitirá el uso de claves concertadas.

c) Se exigirá el uso de dispositivos físicos (tokens) personalizados o biometría.

d) En el caso de utilización de dispositivos físicos (tokens) se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

e) Se emplearán, preferentemente, productos certificados [op.pl.5].

4.3.11 Protección de claves criptográficas [op.exp.11].

Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.

Categoría MEDIA

a) Se usarán programas evaluados o dispositivos criptográficos certificados.

b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

5.4.2 Protección de la confidencialidad [mp.com.2].

Nivel ALTO

a) Se emplearán, preferentemente, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

b) Se emplearán, preferentemente, productos certificados [op.pl.5].

5.4.3 Protección de la autenticidad y de la integridad [mp.com.3].

Nivel ALTO

a) Se valorará positivamente en empleo de dispositivos hardware en el establecimiento y utilización de la red privada virtual.

b) Se emplearán, preferentemente, productos certificados [op.pl.5].

5.5.2 Criptografía. [mp.si.2].

Nivel ALTO

a) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

b) Se emplearán, preferentemente, productos certificados [op.pl.5].

5.5.5 Borrado y destrucción [mp.si.5].

NIVEL MEDIO

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su anterior contenido.

b) Se destruirán de forma segura los soportes, en los siguientes casos:

1. Cuando la naturaleza del soporte no permita un borrado seguro.
2. Cuando así lo requiera el procedimiento asociado al tipo de la información contenida.

c) Se emplearán, preferentemente, productos certificados [op.pl.5].

5.7.4 Firma electrónica [mp.info.4].

Nivel ALTO

Se aplicarán las medidas de seguridad referentes a firma electrónica exigibles en el nivel Medio, además de las siguientes:

a) Se usarán certificados reconocidos.

b) Se usarán dispositivos seguros de creación de firma.

c) Se emplearán, preferentemente, productos certificados [op.pl.5].

5.7.5 Sellos de tiempo [mp.info.5].

Los sellos de tiempo prevendrán la posibilidad del repudio posterior:

1. Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
2. Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte.
3. **Se utilizarán productos certificados (según [op.pl.5])** o servicios externos admitidos.

6. Por lo tanto, se valorará positivamente en su contratación la certificación de la funcionalidad de seguridad de todos los productos de nivel alto, y en todo caso, se utilizarán, preferentemente, productos certificados cuando implementen las siguientes funcionalidades y mecanismos de seguridad:

- Mecanismo de autenticación
- Protección de claves criptográficas
- Protección de la confidencialidad
- Protección de la autenticidad y de la integridad
- Criptografía
- Borrado y destrucción
- Firma electrónica
- Sellos de tiempo

3. RELACIÓN CON OTRAS GUÍAS STIC

7. Las normas de certificación funcional a las que se refiere el ENS no especifican los mecanismos criptográficos con los que se pueden o deben implementar los necesarios mecanismos de seguridad, estando su valoración y evaluación fuera del alcance de la certificación funcional.

8. Por ello, es de aplicación la siguiente guía, cuyas recomendaciones deben ser satisfechas por los productos que implementen mecanismos criptográficos, que podrán ser objeto de certificación funcional de seguridad: CCN-STIC-807 “Criptología de empleo en el Esquema Nacional de Seguridad”

4. CONCEPTOS Y PREGUNTAS FRECUENTES

4.1. ¿QUÉ ES LA CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN?

9. La certificación es un mecanism**o de verificación de conformidad. A diferencia de una autodeclaración** de conformidad, o de otros mecanismos de comprobación de la seguridad, la certificación que se otorga por el Organismo de Certificación se basa en la evaluación del producto por una entidad independiente y técnicamente competente, con la supervisión del Organismo de Certificación y bajo criterios de evaluación basados en normas de reconocimiento internacional.

10. La certificación se otorga mediante resolución del CCN, a instancias del solicitante, que suele ser el propio fabricante, y tras la satisfacción del proceso de evaluación. Esta resolución identifica las normas de seguridad utilizadas, la declaración de seguridad, o requisitos de seguridad que cumple el producto, y el nivel de garantía y vigencia de la misma., tal como se puede observar en el siguiente ejemplo:

> *Resolución xxx/xxxxx/aaaa, de <dd> de <mm>, del Centro Criptológico Nacional, por la que se certifica la seguridad del producto <producto>, versión <x>, desarrollado por <fabricante>.*
>
> *Recibida en el Centro Criptológico Nacional la solicitud presentada por <fabricante>, con domicilio social en <dirección>, para la certificación de la seguridad de <producto>, versión <x>, conforme al entorno de uso, garantías y*

limitaciones indicadas en la correspondiente Declaración de Seguridad de fecha <dd/mm/aaaa>.

Visto el correspondiente Informe Técnico de Evaluación de <laboratorio>, de código <código> de <dd/mm/aaaa>, que determina el cumplimiento del producto <producto>, versión <x>, de las propiedades de seguridad indicadas en dicha Declaración de Seguridad, tras el análisis de su seguridad según indican las normas «Common Criteria for Information Technology Security Evaluation» y «Common Methodology for Information Technology Security Evaluation», en su versión 3.1.

Visto el correspondiente Informe de Certificación del Centro Criptológico Nacional, de código INF-<xxxx>, que determina el cumplimiento de <producto>, versión <x>, de los requisitos para la certificación de su seguridad exigidos por el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por la Orden PRE/2740/2007, de 19 de septiembre.

De acuerdo con las facultades que me confiere la Ley 11/2002, reguladora del Centro Nacional de Inteligencia, al amparo de lo dispuesto en el artículo 1 y artículo 2, párrafo 2, letra c, del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, al objeto de resolver la solicitud de certificación mencionada, dispongo:

Primero.

Certificar que la seguridad del <producto>, versión <x>, cumple con lo especificado en la Declaración de Seguridad de <dd/mm/aaaa>, según exigen las garantías definidas en las normas «Common Criteria for Information Technology Security Evaluation» y «Common Methodology for Information Technology Security Evaluation», en su versión 3.1, para el nivel de garantía de evaluación EAL<x>.

Segundo.

Esta certificación, su alcance y vigencia, y el uso de la condición de producto certificado, quedan sujetos a lo establecido en el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

Tercero.

El Informe de Certificación y la Declaración de Seguridad citados se encuentran disponibles para su consulta en el Centro Criptológico Nacional.

Cuarto.

La presente Resolución entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, <dd de mm de aaaa>.–El Secretario de Estado Director del Centro Criptológico Nacional.

4.2. ¿QUÉ ASPECTOS NO ESTÁN CUBIERTOS POR LA CERTIFICACIÓN?

11. La certificación de la seguridad funcional de componentes no cubre aspectos relativos a:

- La fortaleza de los algoritmos criptográficos, sus modos de operación, o los tamaños de clave, que en este ámbito deben seguir las directrices de la guía **CCN-STIC-807.**
- Los aspectos organizativos, o de personal, que sólo se abordan en la certificación de sistemas operacionales.
- Salvo que se indique lo contrario en el correspondiente informe de certificación, por lo general tampoco se cubren aspectos de la resistencia física de los productos, o de resistencia a ataques pasivos, tipo análisis de emanaciones o de consumos.

4.3. ¿QUÉ NORMAS SE APLICAN EN LA ACTUALIDAD EN LA CERTIFICACIÓN DE LA SEGURIDAD FUNCIONAL?

12. Las normas de evaluación funcional de la seguridad evolucionan con el desarrollo de la tecnología, así como con la consideración de diferentes aspectos o técnicas de análisis de la seguridad.

13. El procedimiento administrativo de certificación de productos y sistemas de tecnologías de la información del Organismo de Certificación es independiente de tales normas técnicas, que dicho Organismo adopta conforme a su vigencia y utilidad. Es requisito general en la aplicación de estas normas, que, además de contemplar el estado del arte en el análisis de la seguridad, garanticen los aspectos de imparcialidad, repetitividad y objetividad que permiten el posterior reconocimiento internacional de los certificados emitidos.

14. A la fecha de la publicación de esta guía, el Organismo de Certificación utiliza las siguientes normas para la certificación:

- Para la certificación de la seguridad funcional de productos y sistemas, la norma fundamental es la llamada “Common Criteria for Information Technology Security Evaluation” (CC), o criterios comunes para la evaluación de la seguridad de las tecnologías de la información. Esta guía utiliza conceptos y términos de esta norma, que son, en esencia, extrapolables a las otras normas utilizadas por el Organismo de Certificación. La norma CC se publica igualmente como ISO/IEC 15408, siendo equivalentes en su contenido.

  Algunos sistemas se certifican utilizando los criterios de evaluación europeos “Information Technology Security Evaluation Criteria” (ITSEC), o criterios para la evaluación de la seguridad de las tecnologías de la información. Estos criterios no gozan del amplio reconocimiento internacional de los anteriores, y su uso tiende a desaparecer.

- Finalmente, para la determinación de la corrección de las implementaciones criptográficas, y de su ajuste a determinados requisitos de funcionalidad y diseño seguro, se utilizan las normas internacionales “ISO/IEC 19790:2008, Security Requirements for Cryptographic Modules” e “ISO/IEC 24759:2008, Test Requirements for Cryptographic Modules”. Estas normas son específicas para un tipo de producto muy determinado, como son los módulos criptográficos, y complementan a las anteriores.

4.4. ¿DE QUÉ MANERA INFLUYE ESTA CERTIFICACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN?

15. De un producto certificado se conoce su utilidad, en qué entorno y condiciones se puede utilizar de manera segura, y qué mecanismos utiliza para la protección de la información, además de tener establecida su fortaleza frente a ataques, y el nivel de garantía que podemos esperar de él.

16. De un producto no certificado no se tiene ninguna información certera relativa a ninguno de los aspectos anteriores. Todos los productos certificados han sufrido mejoras para adecuar su diseño o funcionalidad a los requisitos aplicables, lo cual indica que el proceso de certificación no sólo es efectivo, sino fundamental para poder basar el despliegue de tecnología sobre una base fundamentada.

17. El proceso de evaluación determina con precisión qué utilidad tiene un producto a la hora de proteger la información. La utilización de productos sin seguridad certificada impide desplegar los servicios electrónicos sobre una base cierta, cuestionando la eficacia real de las contramedidas técnicas aplicadas, y poniendo en riesgo real lo que pudiera parecer conforme al ENS.

4.5. ¿QUÉ ES UNA DECLARACIÓN DE SEGURIDAD?

18. La seguridad no es un atributo universal o absoluto, y tampoco en su aplicación a las tecnologías de la información.

19. Las normas de evaluación de seguridad no son normas de cumplimiento directo, esto es, no especifican requisitos de seguridad particulares que los productos deban cumplir, sino que son normas instrumentales que permiten analizar y expresar los requisitos de seguridad aplicables a cada caso, y establecen el proceso de análisis y evaluación correspondiente. De esta manera, para cada evaluación se necesita una “Declaración de Seguridad”, que refleja este análisis y concreta los requisitos de seguridad exigibles. Nótese cómo, en el ejemplo de resolución de certificación expuesto anteriormente, las garantías se acotan al cumplimiento de una Declaración de Seguridad, y al nivel de evaluación aplicable.

20. De esta manera, cada certificado debe hacer referencia a un documento técnico que detalle las propiedades de seguridad del producto, documento que se conoce como “Declaración de Seguridad”, en términos de ITSEC o CC, o “Política de Seguridad” en la norma ISO/IEC 19790:2008 de seguridad de módulos criptográficos.

21. La Declaración de Seguridad documenta, en primer lugar, el problema de seguridad que debe resolver el producto, y en segundo término, los requisitos funcionales, mecanismos de seguridad y requisitos de garantía que se implementan para resolverlo.

22. La descripción del problema de seguridad incluye la identificación de los activos de información a proteger por el producto, los ataques esperados, la descripción del entorno de uso, las hipótesis que se aplican a este uso y las políticas organizativas que se deben respetar o aplicar. Todas las propiedades de seguridad del producto deben justificar su necesidad y eficacia en tanto que útiles y suficientes para resolver este problema de seguridad, esto es, garantizar la seguridad de los activos en el entorno de uso declarado.

23. Nótese que sobre un mismo producto se pueden realizar diferentes análisis para distintos problemas de seguridad. De esta manera, se podrían tener varias certificaciones para cubrir otros tantos problemas sobre la base del mismo producto.

24. También se pueden encontrar certificados emitidos bajo la misma norma, de distintos productos que parecen realizar la misma función. Sin embargo, el problema de seguridad planteado en cada una de estas evaluaciones puede ser distinto, lo que hace que no sean igualmente aplicables los certificados.

25. De esta manera, la semántica del certificado viene definida por la Declaración de Seguridad a la que se refiere, y el certificado o la condición de producto certificado no debe valorarse sin acudir a la correspondiente Declaración de Seguridad.

4.6. ¿QUÉ ES EL NIVEL DE GARANTÍA O NIVEL DE EVALUACIÓN?

26. Dado un problema de seguridad, el análisis de la solución aportada por un producto, a través de la evaluación del laboratorio, puede realizarse con distintos niveles de rigor (según la aplicación más o menos metódica y formal de las actividades de evaluación), profundidad (según el grado de detalle con que se analiza el diseño y la implementación del producto) o extensión (según cuánto se analiza del producto). De esta manera, las normas de evaluación regulan el esfuerzo a aplicar en cada nivel de evaluación, lo que resulta en un distinto nivel de confianza sobre los resultados de la evaluación, y por tanto, de garantía de seguridad.

27. La certificación no es, en ningún caso, sinónimo de ausencia de vulnerabilidades, sino un índice de confianza en la seguridad del producto. Dicho esto, un mínimo nivel de confianza es bastante más garantía que la ausencia de evidencia de la seguridad de los productos.

28. En la norma CC, se distinguen siete niveles discretos de garantía de seguridad, de EAL1, el más bajo, a EAL7, en términos CC. El primer nivel se corresponde con una verificación funcional del producto, al que se somete a un somero análisis de vulnerabilidades, y conforme se sube el nivel se profundiza en el análisis hasta llegar a un proceso de evaluación donde se examinan todos los detalles de la implementación y se aplican técnicas de penetración de alto potencial de ataque.

29. Parejo al nivel de evaluación va el potencial de ataque con el que un producto resiste los intentos de compromiso de sus activos. En el primer nivel de evaluación, la resistencia es únicamente frente a ataques casi triviales, mientras que en los niveles de evaluación superiores no debe haber posibilidad práctica de efectuar ningún ataque con éxito. Nótese que si un producto no está certificado, no se puede afirmar nada sobre su nivel de resistencia frente a cualquier tipo de ataque.

4.7. ¿QUÉ SON LOS REQUISITOS FUNCIONALES DE SEGURIDAD?

30. Son la expresión detallada de las capacidades funcionales que debe tener un producto para proteger sus activos en el entorno de uso definido. Este detalle puede ser relevante una vez se determine la adecuación del certificado al uso pretendido del producto, pero no deben utilizarse para comparar distintas certificaciones.

4.8. ¿CÓMO SABER SI UN CERTIFICADO ES APLICABLE AL USO QUE PRETENDEMOS DE UN PRODUCTO?

31. Puesto que la semántica de un certificado se encuentra en la correspondiente Declaración de Seguridad, deberemos acudir al análisis de la misma para valorar si el producto protege los activos relevantes en el despliegue correspondiente.

32. El análisis de riesgos de un sistema permite identificar los activos de información del mismo. La Declaración de Seguridad de un producto deberá ser coherente con este análisis de riesgos, de manera que sus propiedades de seguridad sean útiles para proteger el sistema.

4.9. ¿QUÉ ES UN PERFIL DE PROTECCIÓN?

33. En estas normas de evaluación que no contienen requisitos de cumplimiento directo, sino que permiten expresar los requisitos que se consideren aplicables, el autor de la Declaración de Seguridad tiene libertad para establecer el problema de seguridad que entienda más oportuno.

34. Esto permite que se puedan certificar propiedades de seguridad distintas de las que un usuario final esperaría de un producto, o cualquier subconjunto de las mismas. En tanto que conforme a las normas de aplicación, el Organismo de Certificación tramita las solicitudes de certificación sin valorar la utilidad de la Declaración de Seguridad. Esta valoración de productos está fuera del ámbito del Organismo de Certificación, aunque en dicha valoración se utilizan los resultados de las certificaciones.

35. En los casos en los que se certifican varios productos semejantes, o cuando se quiere precisar el problema y los requisitos de seguridad a exigir para resolverlo, se puede utilizar el concepto de “Perfil de Protección”, que viene a ser una Declaración de Seguridad, pero independiente de cualquier producto en particular y aplicable a una categoría de los mismos.

36. Diferentes administraciones, grandes consumidores, y asociaciones industriales, han venido publicando Perfiles de Protección, que suponen un acuerdo general sobre un problema de seguridad y una posible solución.

37. Una vez que se dispone de un Perfil de Protección, el fabricante puede certificar la seguridad de su producto identificando este Perfil de Protección, lo que ya establece un marco de referencia de cumplimiento directo.

38. Puesto que estos Perfiles de Protección pueden ser publicados por cualquiera, su existencia no garantiza la adecuación al uso que esperamos de nuestros productos, lo que nos obliga igualmente a valorar la adecuación del problema de seguridad que plantean a nuestro caso particular.

4.10. ¿QUÉ VIGENCIA TIENEN LOS CERTIFICADOS EMITIDOS POR EL CCN?

39. Los certificados emitidos por el Organismo de Certificación son válidos hasta que se revocan. La revocación se publica, al igual que el certificado, en el Boletín Oficial del Estado.

40. Cada dos años desde su emisión, el Organismo de Certificación realiza una revisión de la vigencia de cada certificado. El objetivo de dicha revisión es la comprobación de que el entorno de uso del producto certificado no ha sufrido variaciones, tales como cambios tecnológicos, aparición de vulnerabilidades o cualquier otro aspecto que pueda invalidar las hipótesis, análisis de riesgos y políticas de seguridad reflejadas en dicho entorno de uso.

41. La revisión de la vigencia de los certificados podrá dar lugar a la anulación del certificado, mediante resolución expresa del Director del Organismo de Certificación.

42. El Organismo de Certificación realiza igualmente un seguimiento continuo del uso de los certificados emitidos, mediante el análisis y registro de toda información comercial o técnica de la que tenga conocimiento y que haga referencia a la certificación emitida.

43. El incumplimiento de las condiciones de uso de los certificados, reguladas en el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (Orden PRE 2740/2007, de 19 de septiembre), también podrá dar lugar a la anulación del certificado.

44. Si bien el certificado se refiere únicamente a la versión evaluada del producto, lo habitual es que el fabricante, durante la fase de mantenimiento del producto, lo haga evolucionar, y realice cambios con respecto a la versión certificada. Para estos casos, se dispone de un procedimiento de mantenimiento de la certificación, que permite ampliar el alcance del certificado original a las sucesivas versiones corregidas del producto.

45. La ampliación del alcance del certificado se realiza a instancias del fabricante, que debe aportar la identificación de los cambios realizados y un análisis del impacto de los mismos en el cumplimiento de la Declaración de Seguridad. Conforme a la naturaleza, volumen e impacto de los cambios, el Organismo de Certificación podrá extender el certificado a la nueva versión sin más consideraciones, o requerir de un informe de evaluación que permita determinar si se mantiene el cumplimiento de los requisitos de seguridad. En todo caso, el mecanismo de mantenimiento del certificado pone a disposición de los fabricantes un procedimiento de esfuerzo y coste de evaluación proporcional al impacto de los cambios realizados al producto certificado.

4.11. ¿QUÉ VIGENCIA Y APLICACIÓN TIENEN LOS CERTIFICADOS EMITIDOS POR OTROS PAÍSES?

46. Los certificados emitidos por el Organismo de Certificación tienen diferente reconocimiento internacional, según sean de aplicación los distintos acuerdos que, en esta materia, tiene suscrita la Administración General del Estado, o el propio CCN.

47. A los efectos del ENS, los certificados CC emitidos por terceros países se reconocen hasta un nivel EAL4. La relación de países reconocidos va aumentando con el tiempo, y se puede consultar en la página web del “Arreglo de Reconocimiento Mutuo de Common Criteria”, en www.commoncriteriaportal.org.

48. Sin embargo, la vigencia de cada certificado se ajusta a las normas de cada esquema de certificación, y puede variar desde el modelo español, en el que es válido hasta que se revoca, pasando por un plazo de validez (seis meses, o dos años, por ejemplo), hasta ser válido únicamente en su fecha de expedición, de tal manera que se hace preciso consultar su vigencia a la hora de su valoración.

49. A la hora de reconocer un certificado emitido por la administración de otro país reconocido, no se requiere de una resolución de homologación explícita, sino que el propio “Arreglo de Reconocimiento Mutuo de Common Criteria” sienta las bases para el reconocimiento del certificado por parte de la Administración. Por lo tanto, no cabe la solicitud de homologación del certificado, sino la consulta de su vigencia.

4.12. LOS NIVELES DE GARANTÍA Y EL ESFUERZO DEL FABRICANTE

50. A cada nivel de evaluación creciente, o de garantía de seguridad, se necesita de un conocimiento del producto cada vez más detallado por parte del laboratorio. Este nivel de conocimiento se ha de basar en evidencias documentales, que permitan garantizar tanto el nivel técnico del análisis como los aspectos de objetividad y repetitividad.

51. El conocimiento del producto por parte del laboratorio se basa en información de desarrollo común en escenarios de cierta madurez de desarrollo, tales como especificaciones funcionales, documentación de diseño, planes, procedimientos y resultados de pruebas funcionales o unitarias, documentación de instalación y uso, o los manuales de usuario, por citar los tipos más relevantes.

52. Desde este punto de vista, y en la medida en que el desarrollo del producto no se haya ajustado a un proceso que garantice que existan especificaciones funcionales, un modelo del diseño correspondiente, o pruebas documentadas del producto, la primera dificultad del fabricante frente al proceso de evaluación va a ser la preparación de estas evidencias.

53. Los niveles más bajos de evaluación exigen poco más que el fabricante especifique la funcionalidad del producto y desarrolle una Declaración de Seguridad al caso pero a partir del nivel EAL4 se examina hasta el diseño detallado y el código fuente, exigiendo pruebas que demuestren la corrección del diseño. Esta gradación de los requisitos al fabricante tiene una traslación inmediata en la calidad del producto que desarrolla, incluso con carácter previo a la evaluación.

4.13. PRODUCTOS QUE INTEGRAN COMPONENTES DE TERCEROS

54. Los requisitos de información sobre el producto que se exigen conforme al nivel de evaluación requerido son ajenos a las cuestiones de propiedad intelectual o disponibilidad de información que se planteen en la evaluación de un producto o integración particular.

55. Así, si un fabricante o un integrador, utiliza en su producto componentes de terceros, tales como un sistema operativo, una base de datos, o un servidor de aplicaciones, estará obligado a suministrar en todo caso la información sobre su diseño, su código fuente, o a realizar pruebas unitarias sobre el mismo, conforme a los requisitos de la evaluación. El atender estos requisitos será tanto más complicado como disminuya el control y conocimiento del fabricante de los distintos componentes del producto. Igualmente, esta ausencia de control llevará pareja una ausencia de garantía de seguridad, limitando el nivel de evaluación alcanzable.

56. Los distintos niveles de garantía de seguridad exigen diferentes niveles de información y documentación relativa a los productos. Así, en los niveles más bajos, basta con una especificación funcional, mientras que en los niveles superiores se requiere disponer del código fuente y del diseño interno detallado. El nivel de exigencia del conocimiento del producto determinará, por tanto, si se puede evaluar y certificar un producto que integra componentes de terceros.

57. Como norma general, cabe establecer que cuando el componente a evaluar incorpora productos de terceros sobre los que el solicitante de la certificación no tiene disponible conocimiento detallado, únicamente se podrán obtener certificaciones de seguridad de niveles bajos.

58. Otro escenario habitual suele ser que tales componentes de terceros ya estén certificados. Este hecho resulta irrelevante, a no ser que su integración con el producto final sea objeto de una certificación de seguridad que garantice la seguridad del producto resultante. En la certificación de la seguridad funcional de las tecnologías de la información no se pueden aplicar aritméticas sencillas, y de la suma de dos certificados no se conocerá el resultado salvo que sea objeto de una evaluación y certificación explícita.

4.14.COMPLEJIDAD, COSTE Y GARANTÍA DE SEGURIDAD

59. El coste de desarrollo de un producto no tiene porqué estar ligado al coste de su evaluación. Los requisitos de la evaluación exigen analizar la seguridad del producto con diferente nivel de detalle, de manera que el coste de la evaluación se regirá por la funcionalidad del producto, su complejidad o tamaño, y la tecnología con la que está implementado.

60. Raro es el producto de las tecnologías de la información que no incorpora componentes o módulos de terceros, y esta capacidad de integración en el límite permite desplegar soluciones funcionales en corto plazo y a un coste muy controlado. Valga por ejemplo, un portal de información municipal, que se puede desplegar con un sistema operativo, un servidor http y un gestor de contenidos. El esfuerzo para su puesta en marcha se limitará a su integración y generación de contenidos. La complejidad del sistema resultante no es función del coste de integración, pero sí será un factor muy condicionante para la determinación de su seguridad.

4.15.LOS NIVELES DE GARANTÍA Y LAS CATEGORÍAS DEL ENS

61. Esta guía pretende facilitar un criterio para la aplicación y valoración de componentes certificados en la aplicación del ENS.

62. Puesto que uno de los parámetros a determinar, una vez que queda establecida la relevancia de la certificación, es el nivel de evaluación aplicable, toca establecer un criterio para determinar en cada caso el nivel recomendable.

63. Los esquemas de asignación de nivel de evaluación en otros escenarios basan el requisito del nivel de evaluación en función del nivel de seguridad o criticidad de la información a procesar. Este criterio es difícil de cumplir en términos generales, por cuanto las exigencias de los niveles de evaluación pretendidos se pueden escapar a la realidad de la oferta tecnológica o de las capacidades presupuestarias de los proyectos.

64. Los criterios estáticos de asignación del nivel de evaluación permiten ser satisfechos alterando el alcance del objeto a evaluar. Por ejemplo, en un sistema complejo, se puede evaluar con un alto nivel de detalle un componente del fabricante, pero que funciona en un entorno del que se desconocen los detalles, y que se supone seguro. Cabe cuestionarse si las garantías que otorgaría este escenario son mayores que las resultantes de un menor nivel de evaluación, pero que considerara todo el entorno de ejecución.

65. Esta guía sugiere un criterio que incluye los aspectos económicos para la asignación y valoración del nivel de evaluación, de manera que se obtengan las máximas garantías de seguridad posibles en cada caso.

5. CRITERIOS DE APLICACIÓN

5.1. USO Y ADQUISICIÓN

66. Se distingue en el ENS el uso de la adquisición de productos.

67. Se entiende que, en el despliegue de los servicios electrónicos objeto del ENS, se utilizarán preferentemente soluciones y productos ya en poder de la Administración, y son las recomendaciones de uso las que permiten determinar su adecuación. Cuando se identifica la carencia de una contramedida técnica, se podrá acudir a su contratación, aplicando para ello y con carácter general la cláusula administrativa particular de su Anexo V, matizada con lo indicado a continuación.

68. Los criterios expuestos en los siguientes apartados, han de entenderse que son de aplicación a aquellos componentes del expediente de contratación sobre los que descansa responsabilidad de seguridad, y no de manera general a todo el sistema a adquirir. Así, cuando se diseña la seguridad de un sistema, es práctica habitual determinar distintos dominios de seguridad, que se harán corresponder con diferentes perfiles de garantía de seguridad, en atención a la relevancia de los activos a proteger. Únicamente será objeto de valoración especial en su adquisición la certificación de los productos que implementan las medidas de protección de estos activos.

5.2. DOMINIOS TÉCNICOS Y NIVELES DE CERTIFICACIÓN

69. Si bien las normas de certificación son independientes del producto al que se aplica, la necesaria especialización técnica de los laboratorios, y las propias características de seguridad de la tecnología permiten alcanzar diferentes niveles de garantía de seguridad en función del tipo de producto evaluado.

70. El Organismo de Certificación, en consonancia con otros esquemas de certificación de su ámbito, maneja el concepto de dominio técnico, que permite establecer requisitos específicos por tipo de producto o tecnología, determinando el máximo nivel de garantía de seguridad alcanzable en cada dominio.

71. Así, las tarjetas inteligentes, base habitual de los dispositivos seguros de creación de firma electrónica, conforman a día de hoy un dominio técnico a estos efectos, al igual que los módulos criptográficos. En estos dominios, el nivel de garantía de seguridad exigible es generalmente superior al de otros productos más genéricos.

5.3. GARANTÍA DE SEGURIDAD DE COMPONENTES CERTIFICADOS EN CONTRATOS DE ADQUISICIÓN DE COMPONENTES COMERCIALES

72. En componentes comerciales, el criterio de la garantía de seguridad puede ser de correspondencia entre categorías de seguridad y niveles de evaluación, por lo que se puede entender que el coste de la certificación no es imputable completamente a la adjudicación en trámite.

Categoría	*básica*	*media*	*alta*
Nivel de evaluación general	*EAL1*	*EAL2*	*EAL3*
Tarjetas inteligentes y módulos criptográficos	*EAL3*	*EAL4*	*EAL4+ AVA_VAN.5*

73. La garantía de seguridad es un aspecto importante de la certificación, pero no es suficiente para garantizar la aplicabilidad del producto al uso pretendido.

74. Se deberá revisar la correspondiente Declaración de Seguridad para determinar si el problema de seguridad que plantea se ajusta al uso pretendido de los productos a adquirir. En particular, los activos que protege el producto, las amenazas frente a las que los debe proteger, la descripción del entorno, las hipótesis de uso y las políticas organizativas que se identifiquen, debe ser analizado, para determinar su adecuación al uso del producto.

Aspectos de la Declaración de Seguridad	Análisis de aplicabilidad
Activos a proteger	
Amenazas a soportar	
Entorno de uso	
Hipótesis de uso	
Políticas organizativas	

75. Se deberá revisar el Informe de Certificación del producto, buscando información que permita entender con más precisión las recomendaciones y restricciones de uso que puedan ser identificadas en el mismo. Igualmente se podrían encontrar recomendaciones con respecto a la vigencia esperada del certificado que ostenta el producto, que se podrá contrastar con el ciclo de vida del producto objeto del contrato.

Aspectos del Informe de Certificación	Análisis de aplicabilidad
Recomendaciones de uso	
Restricciones de uso	
Vigencia del certificado	

5.4. GARANTÍA DE SEGURIDAD DE COMPONENTES CERTIFICADOS EN CONTRATOS DE DESARROLLO DE PRODUCTOS ESPECÍFICOS

76. En proyectos de integración o desarrollo de productos específicos, el criterio de asignación de la garantía de seguridad exigible con la certificación puede establecerse atendiendo al importe económico del contrato.

77. Ya se señaló que el coste de la integración o del desarrollo no es indicativo de la complejidad del producto final, por cuanto el adjudicatario podrá integrar componentes de alta complejidad a coste muy reducido.

78. En todo caso, el coste de obtener una garantía de seguridad determinada no está en función del importe del desarrollo o integración, sino de la complejidad del producto, su tecnología y el problema de seguridad al que debe enfrentarse.

79. Por otro lado, cabe recordar que el impacto en la mejora de la calidad y de las garantías de seguridad es evidente desde los primeros niveles de evaluación.

80. Los costes de certificación de un producto pueden dividirse entre los costes internos de desarrollo de la calidad a exigir al producto, incluyendo la documentación de soporte a la evaluación, más los gastos del laboratorio de evaluación.

81. El sobrecoste de desarrollo puede entenderse asumido por el coste directo de la contratación, al no ser distinto del coste de desarrollo conforme a cualquier metodología establecida y documentada de desarrollo al uso, tipo Métrica.

82. Con todo esto, se puede establecer, de manera orientativa, qué parte del presupuesto de adjudicación se destinará a la inversión en la garantía de la seguridad, y valorar los diferentes niveles de garantía de seguridad que, conforme a tal presupuesto, propongan los ofertantes.

Categoría	*Básica*	*media*	*alta*
Presupuesto para garantía de seguridad	*20%*	*30%*	*40%*

83. En el caso de desarrollos específicos, no habrá una Declaración de Seguridad que cubra el desarrollo, sino que el contrato debería establecer los requisitos de seguridad a cumplir. Para ello, el licitante consultará al Organismo de Certificación los Perfiles de Protección aplicables y recomendados.

84. En ausencia de perfiles de protección, es muy recomendable la inclusión de los requisitos de seguridad en el pliego de prescripciones técnicas con el formato de Declaración de Seguridad.

5.5. VALORACIÓN DE LA CONDICIÓN DE PRODUCTO CERTIFICADO

85. Determinado el nivel de evaluación, o garantía de seguridad deseada, cabe finalmente establecer la valoración adicional de la que podrán beneficiarse las ofertas de los productos certificados.

86. No cabe establecer un marco rígido para esta cuestión, pero sí llamar la atención a la importancia que tienen las garantías de seguridad que la certificación otorga en la aplicación de la contramedida técnica para la que se realiza la adquisición, por cuanto cabe negar la utilidad de los productos, a los efectos de su seguridad, si no están certificados.

87. En este caso, la valoración adicional sí debe ser proporcional a la categoría de seguridad, aunque para la determinación del nivel de seguridad se atiendan a criterios económicos en el caso de adquisiciones de productos específicos.

Categoría	*básica*	*Media*	*alta*
Importancia de la garantía de seguridad	*20%*	*30%*	*40%*

88. En general, la aceptación de la condición de producto certificado únicamente puede satisfacerse mediante el correspondiente certificado, y nunca mediante evidencias de que el proceso de evaluación está en curso, por cuanto esta situación no determina nada con respecto al cumplimiento final de los requisitos de evaluación.

ANEXO A. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Términos

Componente	Término utilizado en el ENS para denotar un producto de las tecnologías de la información, que es objeto de adquisición y cuya seguridad funcional puede certificarse. Se corresponde a los efectos de esta guía con el término "Producto a Evaluar" de la Orden PRE/2740/2007.

Abreviaturas

CC	"Common Criteria for Information Technology Security Evaluation"
CCN	Centro Criptológico Nacional
EAL	Evaluation Assurance Level
ENS	Esquema Nacional de Seguridad

ANEXO B. RELACIÓN DE PERFILES DE PROTECCIÓN RECOMENDADOS.

Para Tarjetas Inteligentes:	CWA 14169, "Dispositivos seguros de creación de firma EAL4+"
Para Aplicaciones de Creación y Verificación de Firma Electrónica:	PPSCVA-T1-EAL3 v2.0, http://www.oc.ccn.cni.es/PPCert_es.html PPSCVA-T2-EAL3 v2.0

ANEXO C. REFERENCIAS

[Ref. 1] CCN-STIC-800 Glosario de términos y abreviaturas del ENS

[Ref. 2] CCN-STIC-807 Criptología de empleo en el ENS