



**Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.**

(BOE 25-09-2007)

- 
- Artículo único. Aprobación del Reglamento.
  - DISPOSICIONES FINALES
  - REGLAMENTO DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS ECOLOGÍAS DE LA INFORMACIÓN.
  - CAPÍTULO I. Disposiciones generales
  - CAPÍTULO II. Estructura y funciones del organismo de certificación
    - SECCIÓN 1ª. Estructura del organismo de certificación
    - SECCIÓN 2ª. Funciones de los cargos del organismo de certificación
    - SECCIÓN 3ª. Consejo de acreditación y certificación
    - SECCIÓN 4ª. Acreditación y certificación
  - CAPÍTULO III. Requisitos de acreditación de laboratorios
    - SECCIÓN 1ª. Requisitos de seguridad para laboratorios que evalúen productos clasificados
    - SECCIÓN 2ª. Requisitos de seguridad para laboratorios que evalúen productos no clasificados
    - SECCIÓN 3ª. Requisitos de los procedimientos de evaluación
  - CAPÍTULO IV. Acreditación de laboratorios
    - SECCIÓN 1ª. Acreditación
    - SECCIÓN 2ª. Alcance de la acreditación
    - SECCIÓN 3ª. Criterios de acreditación
    - SECCIÓN 4ª. Procedimiento de acreditación
    - SECCIÓN 5ª. Seguimiento de la actividad de evaluación
    - SECCIÓN 6ª. Formulación de observaciones, plazos y recursos
  - CAPÍTULO V. Certificación de productos y sistemas
    - SECCIÓN 1ª. Certificación
    - SECCIÓN 2ª. Alcance de la certificación
    - SECCIÓN 3ª. Criterios de certificación
    - SECCIÓN 4ª. Procedimiento de certificación
    - SECCIÓN 5ª. Seguimiento del uso de los certificados
    - SECCIÓN 6ª. Formulación de observaciones, plazos y recursos
  - CAPÍTULO VI. Criterios y metodologías de evaluación
  - CAPÍTULO VII. Uso de la condición de laboratorio acreditado y de producto certificado

---

La utilización de las Tecnologías de la Información (TI) en amplias áreas de la actividad de la Administración, así como la creciente participación de España en proyectos de desarrollo de la sociedad de la información de carácter internacional, imponen la necesidad de garantizar un nivel de seguridad en la utilización de las TI equiparable, como mínimo, al conseguido en el tratamiento tradicional de la información en soporte papel.

Por tanto, la seguridad que las TI deben poseer, ha de abarcar la protección de la confidencialidad, la integridad y la disponibilidad de la información que manejan los sistemas de información, así como la integridad y disponibilidad de los propios sistemas.

La garantía de seguridad de las Tecnologías de la Información debe estar basada en el establecimiento de mecanismos y servicios de seguridad, adecuadamente diseñados, que impidan la realización de funciones no deseadas.

Uno de los métodos, admitido internacionalmente, para garantizar la corrección y efectividad de dichos mecanismos y servicios, consiste en la evaluación de la seguridad de las TI, realizada mediante la utilización de criterios rigurosos, con posterior certificación por el organismo legalmente establecido.

El Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, que acompaña a esta Orden Ministerial, regula el marco de actuación, y crea los organismos necesarios, para poner estos procesos de evaluación y certificación al alcance de la industria y de la Administración; todo ello basado en el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

La carencia actual de un esquema análogo, puede suponer un importante obstáculo para la difusión y aceptación generalizada, tanto a nivel nacional como internacional, de los diferentes productos y sistemas de las Tecnologías de la Información desarrollados en nuestro país.

En el contexto de los programas internacionales, no se puede entender criterios de evaluación y certificación de la seguridad de las TI que no sean homologables con los de otros países participantes. Por ello, es necesario la adopción de criterios internacionales, que permitan negociar el reconocimiento mutuo de certificados, resultando esencial que el Esquema al que se refiere el presente Reglamento, se equipare a los del resto de los países de nuestro entorno.

Desde hace algunos años, en España, se ha venido sintiendo la necesidad de impulsar la creación de un esquema de esta naturaleza, habiéndose llevado a cabo diversas iniciativas para su constitución, desde el Consejo Superior de Informática y para el Impulso de la Administración Electrónica, en colaboración con el Centro Nacional de Inteligencia. También, en la Dirección General de Armamento y Material del Ministerio de Defensa, se creó un esquema orientado a satisfacer necesidades puntuales del Ministerio de Defensa.

Asimismo, se creó un laboratorio de evaluación, el Centro de Evaluación de la Seguridad de las Tecnologías de la Información (CESTI) del Instituto Nacional de Técnica Aeroespacial (INTA). Este laboratorio fue acreditado, siguiendo este mismo Reglamento, como laboratorio de evaluación de la seguridad de las Tecnologías de la Información, por Resolución 1AO/38272/2005, de 13 de octubre, del Centro Criptológico Nacional, y ha contribuido, de manera decisiva, a la creación y puesta en marcha de un esquema de funcionalidad completa.

Paralelamente, España, como país consumidor de certificados, y a través del Ministerio de Administraciones Públicas, ha estado presente en el Arreglo de Reconocimiento Mutuo de Certificados Common Criteria (CCRA), desde su creación.

En ese Ministerio, se ha sentido la necesidad de crear un único esquema nacional que abarcara todo el ámbito de la actividad de evaluación y certificación y que potenciase a España a la categoría de país productor de certificados Common Criteria.

Por todo ello, la creación de un esquema nacional va a gozar, desde el principio, de aportaciones experimentadas y se va a encajar en un foro en el que su presencia es demandada.

Por otra parte, se hace necesaria la participación de un organismo de certificación, que partiendo de un conocimiento de las Tecnologías de la Información y de las amenazas y vulnerabilidades existentes, proporcione una garantía razonable a los procesos de evaluación y certificación.

Dicho organismo se constituye al amparo de la Ley 11/2002, de 6 de mayo, Reguladora del Centro Nacional de Inteligencia, que encomienda a este Centro el ejercicio de las funciones relativas a la seguridad de las Tecnologías de la Información, y según lo dispuesto en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, entre

cuyas funciones está la de constituir el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

En virtud de los preceptos indicados anteriormente, consultados los fabricantes e importadores del sector, y a propuesta conjunta de los Ministros de Defensa y de Industria, Turismo y Comercio, con la aprobación previa de la Ministra de Administraciones Públicas, **dispongo**:

#### **Artículo único. Aprobación del Reglamento.**

Se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, cuyo texto se inserta a continuación.

#### **Disposición Adicional única. Naturaleza y establecimiento de la contraprestación exigida por las acreditaciones y certificaciones**

1. Al amparo de lo dispuesto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos, los ingresos procedentes de las acreditaciones de laboratorios y de las certificaciones de productos, tienen la naturaleza de tasas.

2. Según lo establecido en el artículo 2.3 del Real Decreto 1287/2005, de 28 de octubre, por el que se modifica el Real Decreto 593/2002, de 28 de junio, que desarrolla el régimen económico presupuestario del Centro Nacional de Inteligencia, el establecimiento o modificación de la cuantía de los ingresos que tengan la naturaleza de tasas, así como la fijación de los diversos elementos de la correspondiente relación jurídico-tributaria, se harán con arreglo a lo dispuesto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos.

#### **DISPOSICIONES FINALES**

##### **Disposición Final primera. Facultades de ejecución y aplicación**

Se faculta al Secretario de Estado Director del Centro Criptológico Nacional del Centro Nacional de Inteligencia, para dictar cuantas instrucciones sean necesarias para la ejecución y aplicación de lo establecido en esta Orden Ministerial.

##### **Disposición Final segunda. Entrada en vigor**

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

#### **REGLAMENTO DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN.**

##### **CAPÍTULO I. Disposiciones generales**

###### **Artículo 1. Objeto.**

El presente Reglamento tiene por objeto la articulación del Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) en el ámbito de actuación del Centro Criptológico Nacional, según lo dispuesto en la Ley 11/2002, de 6 de mayo, Reguladora del Centro Nacional de Inteligencia, y en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, respectivamente.

###### **Artículo 2. Definiciones.**

En el marco del presente Reglamento, los conceptos que a continuación se indican, se entenderán como están definidos.

**Acreditación.-**Declaración de conformidad de los laboratorios solicitantes, emitida por el Organismo de Certificación, en base al cumplimiento de los requisitos establecidos en el Capítulo III, y según el procedimiento establecido en el Capítulo IV, del presente Reglamento.

**Acreditación de competencia técnica.-**Es aquella acreditación que concede una entidad de acreditación reconocida a un laboratorio, conforme a lo regulado en la Ley 21/1992, de 16 de julio, de Industria y en el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la Infraestructura para la Calidad y Seguridad Industrial, y en base al cumplimiento, por parte del laboratorio, de la norma UNE-EN ISO/IEC 17025. En su alcance se deberán incluir las normas de evaluación de la seguridad de los productos y sistemas de Tecnologías de la Información aprobadas por el Organismo de Certificación.

**Certificación.-**Es la determinación, obtenida mediante un proceso metodológico de evaluación, de la conformidad de un producto con unos criterios preestablecidos.

**Declaración de seguridad.-**Conjunto de requisitos y especificaciones de las propiedades de seguridad de un producto o sistema de las Tecnologías de la Información.

**Evaluación.-**Es el análisis, realizado mediante un proceso metodológico, de la capacidad de un producto o sistema de las Tecnologías de la Información para proteger las condiciones de la información de acuerdo a unos criterios establecidos, con objeto de determinar si puede ser certificado.

**Información de las evaluaciones.-**Es todo asunto, acto, documento, dato u objeto relacionado con la actividad de evaluación de la seguridad de un producto. La información de las evaluaciones incluye toda la documentación, programas de ordenador, esquemas, planos y demás datos suministrados por el fabricante, los programas de ordenador, planes, pruebas, análisis y resultados de la evaluación elaborados por el laboratorio, así como toda la documentación administrativa y contractual y las comunicaciones del laboratorio con el fabricante del producto y con el Organismo de Certificación, además de los registros de la actividad del laboratorio, incluyendo los de seguridad.

**Producto a evaluar.-**Es el producto, sistema de información o perfil de protección para el que se solicita una certificación de sus propiedades de seguridad.

**Producto clasificado.-**Son aquellos productos con requisitos específicos para manejar con seguridad materias clasificadas, o cuya información de especificación, diseño o desarrollo está clasificada, incluso parcialmente, según lo dispuesto en la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales, modificada por la Ley 48/1978, de 7 de octubre.

**Laboratorio de evaluación.-**Es un laboratorio de ensayo, según se define en el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la Infraestructura para la Calidad y Seguridad Industrial.

**Sistema de información.-**Es el conjunto de elementos «hardware», «software», datos y usuarios que, relacionados entre sí, permiten el almacenamiento, transmisión, transformación y recuperación de la información.

### **Artículo 3. Ámbito de aplicación.**

El ámbito de actuación del Organismo de Certificación comprende las entidades públicas o privadas que quieran ejercer de laboratorios de evaluación de la seguridad de las TI en el marco del Esquema.

También comprende a estas entidades cuando sean fabricantes de productos o sistemas de TI que quieran certificar la seguridad de dichos productos, en el marco del Esquema.

Todo ello, siempre que dichos productos o sistemas sean susceptibles de ser incluidos en el ámbito de actuación del Centro Criptológico Nacional.

## **CAPÍTULO II. Estructura y funciones del organismo de certificación**

### **SECCIÓN 1ª. Estructura del organismo de certificación**

#### **Artículo 4. Estructura.**

A los efectos de funcionamiento del Organismo de Certificación, su estructura será la siguiente:

- a) Director del Organismo de Certificación, que será el Secretario de Estado Director del Centro Criptológico Nacional.
- b) Secretario General del Organismo de Certificación, que será el Secretario General del Centro Criptológico Nacional.
- c) Subdirector de Certificación, que será un funcionario del Centro Nacional de Inteligencia, con rango de Subdirector General, designado por el Director del Organismo de Certificación.
- d) Jefe del Área de Certificación, que será un funcionario del Centro Criptológico Nacional, con rango de Subdirector General Adjunto, designado por el Subdirector de Certificación.
- e) Los correspondientes Responsables, Técnico de Certificación, de Calidad, de Seguridad, y de Registro, que serán funcionarios del Centro Criptológico Nacional designados por el Jefe del Área de Certificación.
- f) Personal técnico de certificación, que serán funcionarios del Centro Criptológico Nacional designados por el Jefe del Área de Certificación.
- g) Personal de enlace con los servicios de Secretaría, y demás personal de soporte administrativo a las actividades del Organismo de Certificación, que serán funcionarios del Centro Criptológico Nacional designados por el Jefe del Área de Certificación.

Figura 1. Estructura del Organismos de Certificación.pdf

### **SECCIÓN 2ª. Funciones de los cargos del organismo de certificación**

#### **Artículo 5. Director del Organismo de Certificación.**

Corresponde al Director del Organismo de Certificación:

- a) Aprobar y hacer cumplir las políticas, manuales y procedimientos que regulan la actuación del Organismo de Certificación, garantizando la adecuación de la organización y de los medios materiales y humanos a los fines propuestos.
- b) Dictar las resoluciones sobre las solicitudes de acreditación de laboratorios y de certificación de la seguridad de productos y sistemas de las Tecnologías de la Información.
- c) Establecer los acuerdos oportunos con otros organismos similares en el ámbito de su competencia.

#### **Artículo 6. Secretario General del Organismo de Certificación.**

Corresponde al Secretario General del Organismo de Certificación:

- a) Apoyar y asistir al Director del Organismo de Certificación en el ejercicio de sus funciones.
- b) Establecer los mecanismos y sistemas de organización del Organismo de Certificación y determinar las actuaciones precisas para su actualización y mejora.
- c) Dirigir el funcionamiento de los servicios comunes del Organismo de Certificación a través de las correspondientes instrucciones y órdenes de servicio.
- d) Desempeñar la jefatura superior del personal del Organismo de Certificación, elaborar la propuesta de relación de puestos de trabajo y determinar los puestos vacantes a proveer durante cada ejercicio.

#### **Artículo 7. Subdirector de Certificación.**

Corresponde al Subdirector de Certificación:

- a) Presidir el Consejo de Acreditación y Certificación, conforme a lo establecido en el presente Reglamento.
- b) Representar al Organismo de Certificación en aquellos foros de índole técnica, de normalización y de divulgación de las actividades del citado organismo, de las normas aplicables y en los de arreglos y acuerdos de reconocimiento mutuo.
- c) Revisar las políticas, manuales y procedimientos que regulan la actuación del Organismo de Certificación.
- d) Proponer los presupuestos y planes de formación anuales del Organismo de Certificación.

#### **Artículo 8. Jefe del Área de Certificación.**

Corresponde al Jefe del Área de Certificación:

- a) Desempeñar la dirección de los servicios técnicos del Organismo de Certificación.
- b) Dirigir las instrucciones y procedimientos de acreditación de laboratorios y de certificación de productos.
- c) Elevar las correspondientes propuestas de resolución a las mencionadas solicitudes de acreditación y certificación.
- d) Instruir, de oficio, los procedimientos de mantenimiento de la acreditación de los laboratorios.

#### **Artículo 9. Responsable Técnico de Certificación.**

Corresponde al Responsable Técnico de Certificación:

- a) Apoyar y asistir al Jefe del Área de Certificación en el ejercicio de sus funciones.
- b) Coordinar y dirigir la actuación diaria del personal técnico del Organismo de Certificación.
- c) Realizar la asignación de personal técnico a la instrucción de cada solicitud de acreditación de laboratorio y de certificación de producto.
- d) Dictaminar las interpretaciones técnicas de normas, métodos y procedimientos de evaluación empleados, bien de oficio, o a instancia de los laboratorios.



e) Elaborar o proponer las políticas, manuales y procedimientos que regulan la actuación del Organismo de Certificación.

#### **Artículo 10. Responsable de Calidad del Organismo de Certificación.**

Corresponde al Responsable de Calidad del Organismo de Certificación:

- a) Garantizar y auditar la ejecución del sistema de gestión de la calidad del Organismo de Certificación, con las funciones específicas en él indicadas.
- b) Proponer, al Jefe del Área de Certificación, las mejoras convenientes para la eficacia del sistema de gestión de calidad, tras su evaluación.

#### **Artículo 11. Responsable de Seguridad del Organismo de Certificación.**

Corresponde al Responsable de Seguridad del Organismo de Certificación:

- a) Garantizar y auditar la ejecución del sistema de gestión de la seguridad del Organismo de Certificación, con las funciones específicas en él indicadas.
- b) Proponer, al Jefe del Área de Certificación, las mejoras convenientes para la eficacia del sistema de gestión de la seguridad, tras su evaluación.

#### **Artículo 12. Responsable de Registro del Organismo de Certificación.**

Corresponde al Responsable de Registro del Organismo de Certificación, la gestión y custodia de los registros de calidad, seguridad, certificación y acreditación, manejados por el Organismo de Certificación.

#### **Artículo 13. Personal técnico del Organismo de Certificación.**

Corresponde al personal técnico del Organismo de Certificación, el desarrollo de la instrucción de los expedientes de acreditación de laboratorio y de certificación de productos, practicando las pruebas conforme a los medios y procedimientos establecidos por el Organismo de Certificación.

### **SECCIÓN 3ª. Consejo de acreditación y certificación**

#### **Artículo 14. Naturaleza.**

El Consejo de Acreditación y Certificación es un órgano colegiado, distinto e independiente del Organismo de Certificación, regido por lo establecido en el Capítulo II del Título II, de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y, por lo establecido en el presente Reglamento.

#### **Artículo 15. Composición.**

Corresponde al Subdirector de Certificación la presidencia del Consejo de Acreditación y Certificación.

Formarán parte como miembros del Consejo, los siguientes:

- a) El Jefe del Área de Certificación, que podrá asumir la presidencia del Consejo por delegación del Subdirector de Certificación.
- b) El Responsable Técnico de Certificación, que hará las veces de Secretario del Consejo.

- c) Un representante del Ministerio de Defensa, cuyo nombramiento y asistencia solicitará el Organismo de Certificación a dicho Ministerio.
- d) Un representante del Ministerio de Industria, Turismo y Comercio, cuyo nombramiento y asistencia solicitará el Organismo de Certificación a dicho Ministerio.
- e) Un representante del Consejo Superior de Administración Electrónica, cuyo nombramiento y asistencia solicitará el Organismo de Certificación a dicho Consejo.
- f) Un representante de cada laboratorio acreditado, nombrado por dicho laboratorio.
- g) Dos representantes de los sectores empresariales de fabricantes, importadores e integradores de productos y sistemas de las Tecnologías de la Información, a propuesta razonada y acordada de dichos sectores.

#### **Artículo 16. Fines.**

Corresponde al Consejo de Acreditación y Certificación:

- a) Vigilar que la normativa del Organismo de Certificación se corresponda y equipare con los términos y referencias de esquemas de certificación equivalentes, que pudieran existir en el ámbito de la Unión Europea en particular, y en el ámbito internacional, en general.
- b) Asesorar al Organismo de Certificación en la evolución de sus procedimientos documentados, orientando la gestión de éste, al mejor servicio del tejido industrial y empresarial de fabricantes, importadores e integradores de productos y sistemas de Tecnologías de la Información.
- c) Asesorar al Organismo de Certificación en la identificación de esquemas, arreglos o acuerdos, donde la defensa de la validez y reconocimiento mutuo de los certificados emitidos sea de interés para la Administración y el sector privado español.

#### **Artículo 17. Atribuciones.**

Las atribuciones del Consejo de Acreditación y Certificación son las siguientes:

- a) Estar permanentemente informado de la normativa que regula el funcionamiento del Organismo de Certificación, incluyendo sus normas de evaluación y certificación, manuales, procedimientos e instrucciones técnicas.
- b) Estar permanentemente informado de la relación de laboratorios acreditados y de productos certificados.
- c) Estar permanentemente informado de la relación de esquemas de certificación de la seguridad de los productos y sistemas de información, con los que el Organismo de Certificación tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.
- d) Proponer directrices y recomendaciones al Organismo de Certificación, que serán recogidas en las correspondientes actas de las reuniones del Consejo, a las que deberá dar cumplida respuesta el Director del Organismo de Certificación.

#### **Artículo 18. Periodicidad de las reuniones.**

El Consejo de Acreditación y Certificación se reunirá, como mínimo, una vez al año, sin perjuicio de que en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.



Las reuniones se convocarán a requerimiento del Organismo de Certificación, o por acuerdo del propio Consejo de Acreditación.

#### **SECCIÓN 4ª. Acreditación y certificación**

##### **Artículo 19. Acreditación de laboratorios.**

El Organismo de Certificación acredita a los laboratorios solicitantes, en base al cumplimiento de los requisitos establecidos en el Capítulo III, y según el procedimiento establecido en el Capítulo IV de este Reglamento.

##### **Artículo 20. Certificación de productos.**

El Organismo de Certificación certifica la seguridad de los productos y sistemas de Tecnologías de la Información, según lo establecido en el procedimiento del Capítulo V, y atendiendo a los criterios, métodos y normas de evaluación de la seguridad, establecidos en el Capítulo VI.

##### **Artículo 21. Publicaciones del Esquema.**

El Organismo de Certificación mantendrá actualizada la relación de laboratorios acreditados y la de productos y sistemas de las Tecnologías de la Información certificados. Dicha relación se podrá consultar en la siguiente dirección electrónica: <http://www.oc.ccn.cni.es>.

#### **CAPÍTULO III. Requisitos de acreditación de laboratorios**

##### **Artículo 22. Requisitos generales para la acreditación de laboratorios.**

1. Para la acreditación de los laboratorios de evaluación de la seguridad de las Tecnologías de la Información se requerirá el cumplimiento de los siguientes requisitos:

a) Capacidad para la evaluación de la seguridad de productos de las Tecnologías de la Información, demostrada mediante la acreditación de la competencia técnica en vigor, conforme a la norma UNE-EN ISO/IEC 17025, cuyo alcance incluya los criterios, métodos y normas de evaluación recogidos en el Capítulo VI.

b) Cumplimiento de los requisitos de seguridad establecidos en la Sección 1ª o en la Sección 2ª de este Capítulo, según corresponda.

c) Desarrollo de las evaluaciones de acuerdo a procedimientos que recojan las obligaciones de información y coordinación con el Organismo de Certificación, indicadas en la Sección 3ª de este mismo Capítulo.

2. La comprobación del cumplimiento de estos requisitos se realizará mediante el procedimiento de auditoría y seguimiento indicado en las Secciones 4ª y 5ª del Capítulo IV.

En todo caso, el alcance de la acreditación, otorgada por el Organismo de Certificación, estará limitado por el alcance de la acreditación de la competencia técnica del laboratorio, y cualificado por el nivel de seguridad del mismo.

3. Salvo en los casos en que haya una compartimentación organizativa, de medios y de procedimientos, aprobada por el Organismo de Certificación, el laboratorio deberá cumplir con los requisitos de gestión de seguridad, necesarios para la acreditación, incluso en el desarrollo de aquellas evaluaciones cuyo objeto final no sea la certificación del producto evaluado por parte del Organismo de Certificación.

## **SECCIÓN 1ª. Requisitos de seguridad para laboratorios que evalúen productos clasificados**

### **Artículo 23. Requisitos de laboratorios que evalúen productos clasificados.**

Los laboratorios, tanto de titularidad pública como privada, que pretendan evaluar productos clasificados deberán cumplir, además de los requisitos establecidos para los laboratorios que evalúen productos no clasificados, lo dispuesto en la Orden Ministerial Comunicada 17/2001, de 29 de enero, por la que se aprueba el Manual de Protección de Materias Clasificadas del Ministerio de Defensa en poder de las empresas.

Asimismo, deberán tener suscrito, y en vigor, Acuerdo de Seguridad, con un grado de calificación de seguridad igual o superior al grado de calificación de seguridad de la información del producto a evaluar.

## **SECCIÓN 2ª. Requisitos de seguridad para laboratorios que evalúen productos no clasificados**

### **Artículo 24. Requisitos de laboratorios que evalúen productos no clasificados.**

Los laboratorios, tanto de titularidad pública como privada, que evalúen productos no clasificados, cumplirán con los requisitos de gestión de la seguridad, aplicables a la información de las evaluaciones, establecidos en esta Sección.

## **SUBSECCIÓN 1ª. Responsabilidades del laboratorio**

### **Artículo 25. Derecho de acceso a la información de las evaluaciones.**

El laboratorio facilitará al Organismo de Certificación el acceso a toda la información de las evaluaciones que lleve a cabo.

El laboratorio deberá obtener, del Organismo de Certificación, autorización escrita antes de permitir a terceros, incluido el fabricante del producto evaluado, cualquier tipo de acceso a la información de las evaluaciones, tales como, planes, pruebas, análisis y resultados de la evaluación.

El Organismo de Certificación podrá prohibir la difusión de determinada información originada por el laboratorio.

### **Artículo 26. Plan de protección.**

1. El laboratorio deberá elaborar, poner en práctica y mantener al día un Plan de Protección de la Información de las evaluaciones.

2. Este plan incluirá, al menos, la siguiente información:

a) Una descripción del laboratorio, con indicación expresa de la ubicación, actividades empresariales distintas a las de evaluación, en su caso, organigrama, recursos humanos, factorías, sucursales y dependencias autónomas, incluyendo un plano con leyenda de las instalaciones del laboratorio.

b) Los fundamentos del Plan, que deberán comprender los objetivos concretos que han de alcanzarse con el mismo y que estarán dirigidos a prevenir, detectar y rehabilitar el daño causado por la manifestación del riesgo, así como la identificación de los riesgos contra los que se pretende la protección.

La confidencialidad, integridad y disponibilidad de la información de las evaluaciones serán del máximo interés para el Organismo de Certificación.

c) La descripción de la organización, donde se debe documentar la estructura de seguridad del laboratorio, la matriz de responsabilidades donde se establece la identificación exacta de los responsables en lo referente a la toma de decisiones, y la definición detallada de las misiones de cada componente del sistema, así como la coordinación del apoyo potencial de organismo exteriores, tales como empresas de seguridad privada, centrales receptoras de alarmas, servicios de custodia de información, etcétera.

d) La descripción de las medidas de protección física, y el establecimiento de zonas de acceso restringido en las distintas dependencias del laboratorio.

e) Los Procedimientos Operativos de seguridad.

f) La descripción de las reacciones específicas a cada incidente de seguridad, desarrollando la matriz de responsabilidades en los cometidos y misiones que este plan asigne a la dirección del laboratorio, a los que formen parte del Servicio de Protección del laboratorio y al resto de personal, en lo que respecta a decisiones y actuaciones ante los riesgos de seguridad que se manifiesten y que se hayan considerado.

g) Los requisitos específicos de seguridad y los Procedimientos Operativos de seguridad de los sistemas de información del laboratorio.

#### **Artículo 27. Procedimientos Operativos de seguridad.**

1. Los Procedimientos Operativos de seguridad incluirán, en forma de directivas, los detalles específicos de actuación encaminados a la prevención de riesgos.

2. Estas actuaciones se deben corresponder con la matriz de responsabilidades, tratando de forma concreta y específica los siguientes aspectos, relativos a requisitos de seguridad establecidos por las condiciones de acreditación del laboratorio:

a) Las normas para el manejo y custodia de la información de las evaluaciones.

b) El tratamiento de las visitas, verificando periódicamente la eficacia del control de visitas al laboratorio, así como el correcto uso del libro de visitas o sistema alternativo.

c) La entrada en las zonas de acceso restringido.

d) El acceso, transmisión, reproducción, archivo y destrucción de información de las evaluaciones, con el establecimiento de los mecanismos necesarios que permitan identificar, en todo momento, al responsable de la tenencia de la información.

e) La regulación de las necesarias comprobaciones de seguridad, tanto durante la jornada de trabajo como al término de la misma.

f) La descripción del sistema de control de llaves.

g) El establecimiento del sistema de recibo interno, para control de información de las evaluaciones.

h) La operativa de actuación ante una incidencia de la central receptora de alarmas.

i) Los procedimientos de actuación de los vigilantes de seguridad.

#### **Artículo 28. Personal del laboratorio.**

El laboratorio deberá mantener actualizado un registro de seguridad de todo el personal afecto al mismo.

El laboratorio regulará, en base a la necesidad de conocer, el acceso de dicho personal a la información de las evaluaciones. Las autorizaciones de acceso a la información de las evaluaciones se comunicarán y revocarán por escrito, adjuntándose dichas comunicaciones al registro de seguridad del personal.

#### **Artículo 29. Comunicaciones preceptivas al Organismo de Certificación.**

El laboratorio deberá informar al Organismo de Certificación, en el plazo más breve posible, de lo siguiente:

- a) Sobre toda información que llegue a su conocimiento en relación con accesos, o intentos de acceso, no autorizados a información de las evaluaciones; actos de sabotaje, o actividades que supongan un riesgo para dicha información.
- b) Sobre toda anomalía, extravío, robo o manipulación relacionada con la información de las evaluaciones.
- c) Sobre la presunción de que una transmisión de información de las evaluaciones haya sufrido vulneración o retraso injustificado.
- d) Sobre las modificaciones que pretenda realizar en las zonas de acceso restringido.
- e) Sobre las visitas que reciba conforme a lo que se expresa en la Subsección 5ª, presente Capítulo y Sección.
- f) Sobre las modificaciones del Plan de Protección, así como de las altas y bajas de personal y sobre la composición y cambios del Servicio de Protección.

#### **Artículo 30. Relaciones del laboratorio con contratistas.**

Los requisitos de seguridad requeridos por la acreditación del laboratorio, son también de aplicación a los contratistas del mismo que vayan a acceder a información de las evaluaciones.

El laboratorio deberá obtener, del Organismo de Certificación, autorización escrita antes de proporcionar al contratista el acceso a información de las evaluaciones. En su solicitud, comunicará los datos de identificación del contratista, así como la información de las evaluaciones a las que pudiera tener acceso, y el objeto y condiciones específicas de dicho acceso.

Como norma general, para la concesión de la autorización de acceso, el contratista deberá demostrar el cumplimiento de los requisitos de seguridad establecidos en el presente Reglamento mediante auditoría del Organismo de Certificación, conforme al procedimiento establecido en el Capítulo IV, salvo en los casos en que el Organismo de Certificación determine la aplicación de condiciones o limitaciones particulares a dicho acceso.

### **SUBSECCIÓN 2ª. Tratamiento de la información de las evaluaciones**

#### **Artículo 31. Distintivos.**

1. Toda información de las evaluaciones llevará, de forma clara y visible, un signo distintivo de tal condición, que indicará la evaluación a la que corresponde.

2. Si se trata de documentos sueltos, se pondrá el signo distintivo en la parte superior e inferior de cada una de las páginas, centrado en las mismas, de tal forma que no pueda quedar oculto por dobleces, grapas, cubiertas, etcétera.

3. Si se trata de documentos permanentemente unidos o encuadernados, se pondrá el mencionado distintivo en la cubierta anterior y posterior, así como en todas sus páginas, conforme a lo indicado anteriormente.

4. Si se trata de planos, diagramas, esquemas o documentos similares, dicho distintivo se situará en la carátula y en la parte que identifique el documento.

5. Los soportes y sistemas informáticos que contengan o procesen información de las evaluaciones, se marcarán con los distintivos apropiados, para lo cual podrán emplearse etiquetas o cintas adhesivas.

6. Se seguirán procedimientos análogos para la protección de la información de las evaluaciones soportada en cualquier elemento, o conjunto de elementos, físicamente separables.

### **Artículo 32. Libro registro de información de las evaluaciones.**

1. En cada dependencia del laboratorio donde se custodie información de las evaluaciones, existirá un registro donde figurará toda la información de las evaluaciones que haya tenido entrada o salida, las reproducciones y destrucciones, así como el acceso a dicha información por personal, tanto propio, como ajeno al laboratorio, con independencia de si esta información se almacena o transmite en papel o en soporte electrónico.

2. El registro se podrá mantener en soporte informático, en soporte papel (en forma de libro) o en una combinación de ambos soportes.

3. Estos registros deberán ser custodiados con la debida protección electrónica, si están en soporte informático, o en los muebles de seguridad ubicados en la zona de acceso restringido, si están en soporte papel.

4. El laboratorio deberá implementar los mecanismos correspondientes para que el registro de entrada/salida mediante soporte electrónico no se pueda eludir por el personal del mismo.

### **Artículo 33. Recepción y recibo de la información de las evaluaciones.**

Cuando se reciba cualquier información de las evaluaciones, se seguirá el siguiente proceso:

a) Se examinará el envío para asegurarse de que no ha sido violado, comprobándose el contenido contra recibo. La evidencia de violación y las anomalías que se observen en el contenido deberán notificarse, cuanto antes, al remitente y al Organismo de Certificación.

b) Cuando el envío esté en orden, se firmará el recibo y se devolverá debidamente cumplimentado al remitente, realizando de manera inmediata la anotación en el libro registro.

### **Artículo 34. Transmisión de la información de las evaluaciones.**

1. Se entiende por transmisión de la información de las evaluaciones, su traslado, comunicación, envío, entrega o divulgación a terceros.

2. Será necesario que la transmisión y custodia de la información de las evaluaciones sea controlada por un sistema de recibos, incluso dentro de las dependencias del laboratorio, con el fin de identificar, en cualquier momento, al responsable de su tenencia.

3. Cuando se trate de transmisión no electrónica de información de las evaluaciones, se realizará de la siguiente forma:

a) Por entrega directa del personal del laboratorio.

b) Por correo certificado nacional.

c) Por transportistas comerciales.

d) El embalaje de la información se llevará a cabo de forma que se pueda detectar su apertura; con cubiertas opacas que impidan desvelar su contenido, de tal naturaleza y resistencia, que aseguren su integridad durante el transporte; y, dicho embalaje, no tendrá ninguna indicación externa de la información contenida.

4. Cuando se trate de transmisión electrónica de información de las evaluaciones, se realizará utilizando las medidas técnicas y operacionales de protección de su confidencialidad que determine, en cada caso, el Organismo de Certificación.

#### **Artículo 35. Reproducción de la información de las evaluaciones.**

1. El número de reproducciones de la información de las evaluaciones, será el mínimo imprescindible. Se controlará mediante una correlativa numeración, que se recogerá en el registro, como anotación suplementaria del correspondiente original, indicando todos los datos referentes a dichas reproducciones y a la situación de cada una de ellas.

2. Cada reproducción, total o parcial, de información de las evaluaciones deberá ser numerada y tratada, a todos los efectos, como el original.

3. La reproducción de información de las evaluaciones deberá realizarse directamente por el laboratorio, sin recurrir a contratistas de artes gráficas. Se deberá comprobar, después de realizar las reproducciones, que en el mecanismo de reproducción no queda registro de la información reproducida.

#### **Artículo 36. Custodia y destrucción de la información de las evaluaciones.**

1. El laboratorio custodiará, por un plazo mínimo de cinco años, toda la información de cada evaluación, a contar desde la fecha de emisión del certificado correspondiente, o de la emisión del último informe técnico de evaluación, en el caso de productos no certificados.

2. En el caso de reevaluaciones, mantenimiento o extensiones del certificado, el cómputo de cinco años se referirá siempre al último certificado o informe técnico de evaluación aplicable.

3. Pasado dicho plazo, y tras obtener del Organismo de Certificación autorización escrita, procederá a su destrucción, de forma que se garantice que la información de las evaluaciones queda irreconocible y se impida su reconstrucción, total o parcial.

4. El Organismo de Certificación, previo a la autorización de destrucción, podrá requerir al laboratorio el traslado de cuanta información de las evaluaciones sea de su interés.

#### **Artículo 37. Inventario anual.**

El laboratorio presentará ante el Organismo de Certificación, antes del diez de enero de cada año, un inventario anual de toda la información de las evaluaciones que obran en su poder a fecha treinta y uno de diciembre del año anterior.

### **SUBSECCIÓN 3ª. Servicio de Protección de la información de las evaluaciones**



### **Artículo 38. Miembros del Servicio de Protección.**

1. En la organización del laboratorio, el Servicio de Protección de la información de las evaluaciones estará constituido, al menos, por el jefe del Servicio de Protección, el director del Servicio de Protección y el administrador de seguridad del sistema de información.
2. Los miembros del Servicio de Protección nombrados en el párrafo anterior son los responsables, ante el Organismo de Certificación, de la correcta aplicación de los requisitos de seguridad indicados, por ello deben contar con el adecuado grado de representatividad y autoridad, dentro de la organización del laboratorio.
3. Sus funciones de seguridad no podrán quedar disminuidas en ningún momento, aun cuando desempeñen otros cometidos en el laboratorio, debiendo contar con los medios necesarios para realizar sus funciones con eficacia.

### **Artículo 39. Condiciones personales y nombramiento.**

1. Los responsables del Servicio de Protección deberán tener dependencia directa de la dirección del laboratorio, una relación laboral estable sobre la base de continuidad en su función y se les reconocerá, dentro del laboratorio, la debida autoridad en el desempeño de sus cometidos.

Deberán gozar de prestigio personal y profesional, y tener un amplio conocimiento de la organización del laboratorio.

2. El nombramiento y cese de los responsables del Servicio de Protección se comunicará por escrito, reconocido expresamente, en el que constarán las misiones de la responsabilidad asignada.
3. La inadecuación en el desarrollo, o la inobservancia, de las misiones encomendadas a los responsables del Servicio de Protección, podrá motivar su cese, cuando el Organismo de Certificación así lo demande, previa notificación por escrito, y sin perjuicio de la exigencia de otras responsabilidades que se pudieran derivar.

### **Artículo 40. Director del Servicio de Protección.**

1. Cuando el laboratorio designe varios jefes del Servicio de Protección de la información de las evaluaciones, uno por cada una de las sedes donde se maneje o custodie información de las evaluaciones, deberá nombrar un director del Servicio de Protección, cuya misión principal será coordinar la actuación de dichos jefes, así como de los distintos administradores de seguridad del sistema de información, sin que esto suponga merma alguna de las responsabilidades que a éstos corresponde.
2. El cargo de director del Servicio de Protección se podrá compatibilizar con el de jefe de dicho Servicio, en las dependencias donde se ubiquen las oficinas centrales del laboratorio.

### **Artículo 41. Misiones del jefe del Servicio de Protección.**

1. Corresponde al jefe del Servicio de Protección la misión de organizar, dirigir y controlar el sistema de protección para salvaguarda de la información de las evaluaciones, y la obligación de cumplir y hacer cumplir, en todas sus partes, estos requisitos de seguridad para la acreditación del laboratorio.
2. Entre los cometidos del jefe del Servicio de Protección se encuentran:
  - a) Asegurar la protección de la información de las evaluaciones en poder del laboratorio.

b) Regular el acceso a la información de las evaluaciones conforme a los criterios y procedimientos establecidos.

c) Llevar a cabo un programa de formación del personal del laboratorio, con una periodicidad mínima de treinta (30) meses, cuyo principal objetivo será sensibilizar a dicho personal sobre la importancia de cumplir los procedimientos de protección de la información de las evaluaciones y el deber de discreción.

d) Controlar la recepción, custodia, reproducción, destrucción y devolución de la información de las evaluaciones, conforme a los procedimientos establecidos.

e) Velar, especialmente, para que ninguna información de las evaluaciones sea transmitida indebidamente, o sea manejada o custodiada en lugar distinto a las zonas protegidas.

f) Elaborar, implantar y mantener el Plan de Protección conforme a lo establecido en este Reglamento.

g) Mantener actualizados los registros de seguridad.

#### **Artículo 42. Misión del administrador de seguridad del sistema de información.**

1. El administrador de seguridad del sistema de información tendrá como misión organizar, dirigir y controlar la seguridad del sistema de información del laboratorio. Este administrador podrá ser el propio jefe del Servicio de Protección, cuando tenga la formación adecuada.

2. Entre los cometidos del administrador de seguridad del sistema de información se encuentran:

a) Elaborar, organizar e implementar los requisitos y procedimientos relativos a la seguridad de los sistemas de información del laboratorio, debiendo revisar, periódicamente, la eficacia de todos los componentes.

b) Controlar que todo el personal que tiene acceso al sistema de información está debidamente autorizado.

c) Investigar los incidentes de seguridad que pudieran afectar al sistema de información, evaluando en su caso, los daños causados e informando de las conclusiones al jefe del Servicio de Protección.

d) Llevar a cabo un programa de formación continua de los usuarios del sistema de información, sobre la observancia de los procedimientos de seguridad.

e) Gestionar y proporcionar los códigos de acceso u otros dispositivos de control de acceso al sistema de información. Llevará un registro de asignación de códigos a los usuarios, que serán cambiados con una periodicidad mínima de tres meses, y cada vez que se produzca, o se sospeche que haya ocurrido, un incidente de seguridad que comprometa dichos códigos.

f) Realizar la gestión de claves del sistema de información del laboratorio, incluidos los sistemas de cifra que estuvieran en el ámbito de su competencia, así como la de los sistemas de soporte a la evaluación. Para ello, controlará su generación, almacenamiento, distribución, expiración y destrucción. En la recepción de nuevos equipos modificará todas las claves que, por defecto, vengan de fábrica.

g) Controlar tanto las modificaciones que se realicen en cualquier componente del sistema de información, asegurándose que no se vea afectada la seguridad del sistema, como los aspectos de la gestión de la configuración de dichas modificaciones.

h) Comprobar que el mantenimiento del sistema de información se realiza conforme a los procedimientos y requisitos operativos de seguridad.

i) Verificar que los soportes de almacenamiento que incluyan información de las evaluaciones se custodian debidamente.

j) Evaluar los registros de seguridad del sistema de información, asegurándose que son suficientes para llevar a cabo un control eficaz. Deberán incluir aquellas actividades, con indicación del usuario, hora y fecha, en que se produzcan hechos que puedan afectar a la seguridad del sistema, como finalizaciones anormales del trabajo, cierres indebidos del sistema, fallos en los mecanismos de seguridad, intentos no autorizados de acceso a datos de la evaluación, uso del sistema de un modo no autorizado, copias e impresiones de la información de las evaluaciones, etcétera.

k) Controlar y registrar las copias periódicas de seguridad.

#### **SUBSECCIÓN 4ª. Inspecciones de seguridad**

##### **Artículo 43. Inspectores de seguridad.**

Los inspectores de seguridad son los representantes del Organismo de Certificación, ante el laboratorio, para la comprobación de la correcta aplicación de los requisitos de seguridad exigidos en el proceso de acreditación.

El laboratorio les reconocerá las competencias que les atribuyen estos requisitos, asumiendo el compromiso de facilitarles su labor, y dispondrá los medios precisos para que realicen sus funciones con eficacia.

##### **Artículo 44. Nombramiento.**

El Organismo de Certificación notificará al laboratorio la identidad del inspector de seguridad correspondiente, así como los cambios que se produzcan.

El nombramiento de inspector de seguridad, para un mismo laboratorio, podrá recaer en varias personas, si el Organismo de Certificación así lo estima oportuno.

##### **Artículo 45. Misiones del inspector de seguridad.**

Corresponde al inspector de seguridad:

a) La observancia del exacto cumplimiento de las obligaciones y compromisos que contrae el laboratorio en el proceso de acreditación.

b) Asesorar al laboratorio en la puesta en práctica de los procedimientos de seguridad, que garanticen la protección de la información de las evaluaciones.

##### **Artículo 46. Inspecciones.**

1. La inspección constituye uno de los medios por los que el Organismo de Certificación comprueba el cumplimiento, por parte del laboratorio, de los requisitos de seguridad para la acreditación.

2. Las inspecciones serán ordinarias cuando se realizan de forma periódica, por los inspectores de seguridad nombrados específicamente para cada laboratorio. Las inspecciones ordinarias no precisan concertación previa.

3. Las inspecciones extraordinarias se realizarán cuando el Organismo de Certificación lo estime conveniente, y serán llevadas a cabo por las personas que éste designe. Las inspecciones extraordinarias se comunicarán previamente al laboratorio.

4. En las inspecciones estarán obligados a estar presentes, el jefe del Servicio de Protección, o quien le sustituya, debidamente acreditado en el caso justificado de que el primero no pudiera asistir, y el personal dependiente del laboratorio que designe el Organismo de Certificación.

5. El inspector de seguridad, en las inspecciones ordinarias, o el jefe de la comisión del Organismo de Certificación, en las inspecciones extraordinarias, deberá anotar en el registro del laboratorio, un resumen del resultado de la inspección. En el caso de presentar aspectos negativos, se remitirá al laboratorio la correspondiente comunicación, en la que se deberá reflejar el plazo de corrección para solventar las anomalías observadas por la inspección.

## **SUBSECCIÓN 5ª. Visitas**

### **Artículo 47. Consideración de visita.**

Se considera visita, el acceso físico y circunstancial de una o varias personas, sin relación de dependencia directa con el laboratorio, a las dependencias o instalaciones del mismo.

### **Artículo 48. Registro de visitas.**

Las visitas se anotarán en el registro de visitas, antes de efectuar la visita. Se deberán recoger, como mínimo, los siguientes datos: fecha de la visita, nombre completo del visitante, número del DNI o pasaporte, nacionalidad, empresa/organismo o dirección del visitante, y nombre de la persona visitada.

Este registro estará a disposición del Organismo de Certificación, para su consulta.

### **Artículo 49. Normas para el control de visitas.**

Para el control de las visitas, se seguirán las siguiente normas:

a) El laboratorio controlará el movimiento de las visitas que entren en sus dependencias, para garantizar la debida seguridad de la información de las evaluaciones que custodie.

b) Se prohibirá al visitante efectuar cualquier tipo de registro o reproducción de la información de las evaluaciones, que deberá solicitarse al personal del laboratorio y ser efectuado mediante los procedimientos correspondientes.

c) Toda entrega al visitante de información de las evaluaciones será anotada en el registro.

### **Artículo 50. Visitas de larga duración.**

Tendrán consideración de visitas de larga duración, las realizadas sobre la base de continuidad o reiteración, por un período de doce meses. Tales visitas se anotarán en el registro de seguridad de personal, incluyendo las autorizaciones de acceso a la información de evaluaciones que se pudieran conceder.

## **SUBSECCIÓN 6ª. Zonas de acceso restringido**

### **Artículo 51. Sistema de protección.**

1. El laboratorio implantará un sistema de protección, integrado en la estructura empresarial, que permita proteger la información de las evaluaciones contra los riesgos que puedan implicar una amenaza para la misma.

2. El sistema de protección puede entenderse como el conjunto de recursos y procedimientos que, interactuando coordinadamente, tienen como finalidad proteger la información de las evaluaciones de los riesgos que puedan afectar a su integridad, confidencialidad o disponibilidad.

#### **Artículo 52. Características del sistema de protección.**

El documento donde se definen las características que presenta el sistema de protección es el Plan de Protección, definido en el Artículo 26.

El laboratorio deberá adjuntar, al Plan de Protección, un proyecto del subsistema de protección física, que estará compuesto por una memoria justificativa de los criterios de diseño, la descripción detallada de todos los componentes de la instalación y los planos que especifiquen la ubicación física de los mencionados componentes.

#### **Artículo 53. Subsistema de protección física.**

El subsistema de protección física, que ha de instalarse, obligatoriamente, en las dependencias del laboratorio donde se vaya a manejar información de las evaluaciones, ha de mantenerse en un óptimo grado de eficacia y utilidad para el cumplimiento de las condiciones de acreditación del laboratorio. La valoración de dicha eficacia y utilidad corresponde al Organismo de Certificación.

Las áreas de acceso restringido, que deberá considerar el subsistema de protección física, están compuestas por las zonas de evaluación y las zonas de protección.

#### **Artículo 54. Zonas de evaluación.**

Las zonas de evaluación son las constituidas por aquellas dependencias del laboratorio en las que, únicamente, se debe manejar y custodiar información de las evaluaciones, con las siguientes características:

a) Ha de estar construida de forma que quede limitado, materialmente, el acceso a la misma, y de manera que se pueda apreciar, con una simple inspección, una intrusión a través de las paredes, suelo, puertas o ventanas que delimiten la zona. Estos elementos no deben permitir la observación desde el exterior.

b) Las puertas de acceso deben disponer de una cerradura de bloque con llave, cuyo mecanismo será obligatoriamente accionado, cuando en el interior se esté trabajando con información de las evaluaciones, así como cuando no haya nadie en la misma. También dispondrán de un dispositivo que obligue a la puerta a permanecer cerrada, cuando no se esté franqueando, y dispondrán de detector de apertura.

c) Si se incluyen ventanas, deben colocarse dispositivos que detecten su apertura, en el caso de ser practicables, así como detectores de rotura de cristales. Los elementos translúcidos deberán estar acondicionados para impedir la observación desde el exterior. En el caso de que las ventanas tengan fácil acceso desde el exterior, estarán físicamente protegidas.

d) Se implantarán medidas físicas y organizativas para impedir el acceso a la zona de evaluación, al personal que no tenga derecho de acceso a la información de las evaluaciones y, en el caso en que se divida esta zona por evaluaciones, al personal que no tenga derecho de acceso, en particular, a la información de la evaluación asociada a cada división.

e) Deberá contar con una caja fuerte Nivel IV, conforme a la norma UNE-EN 1143-1-98, equipada con cerradura Clase B, según norma EN 1300, donde se custodiará, obligatoriamente, la información de las evaluaciones durante los periodos de tiempo en que no se esté manejando. Deberá reunir, además, las características siguientes:

Si se trata de caja fuerte autónoma, ha de estar anclada si su volumen es inferior a 500 litros, o si su peso no supera los 1.000 kg.

Si se trata de caja fuerte empotrada, el grado de seguridad del alojamiento donde se ubique ésta ha de proporcionar, como mínimo, el atribuido al de la puerta y marco de la caja.

Doble sistema de apertura, uno de los cuales ha de ser, ineludiblemente, de combinación electrónica.

#### **Artículo 55. Zonas de protección.**

Las zonas de protección son las constituidas por el entorno de las zonas de evaluación en el que no se podrá manejar o custodiar información de las evaluaciones, pero que estarán dotadas de medidas de seguridad, con la finalidad de incrementar la seguridad de las zonas de evaluación y tendrán las siguientes características:

a) Su ubicación dependerá de las características constructivas y de la situación de la zona de evaluación.

b) En cualquier caso, se implementarán las medidas físicas y organizativas suficientes para que el personal que acceda a la zona de protección esté identificado.

#### **Artículo 56. Central de alarmas.**

Además de los requisitos establecidos en los artículos 54 y 55, las zonas de evaluación y de protección dispondrán de las siguientes medidas de seguridad:

a) Todos los medios activos de seguridad deben estar conectados físicamente a un centro de control de alarmas, que disponga de una autonomía mínima de setenta y dos horas, provista de un dispositivo antisabotaje y ubicada de manera oculta.

b) Este centro de control quedará activado, obligatoriamente, fuera del horario laboral y estará conectado con una central receptora de alarmas, que pueda gestionar cualquier alarma de forma oportuna.

c) La conexión con la central receptora de alarmas debe permitir la verificación automática de la línea de comunicación, para poder conocer oportunamente una interrupción en la misma, a través de la correspondiente señal de alarma. La operativa de la gestión de la central receptora de alarmas deberá estar incluida en el Plan de Protección.

d) Los códigos de acceso de la central de alarmas, que permiten su programación y control, deberán ser conocidos, únicamente, por el jefe del Servicio de Protección y las personas por él designadas. Dicha designación quedará anotada en el registro de seguridad del personal. Los códigos deberán modificarse con los criterios indicados en el artículo 57, referido a «Combinaciones, códigos de acceso y control de llaves», que sigue.

### **SUBSECCIÓN 7ª. Procedimiento de seguridad**

#### **Artículo 57. Combinaciones, códigos de acceso y control de llaves.**

1. Sólo tendrán conocimiento de los códigos de acceso a las zonas de evaluación, de las claves de control de la central de alarmas, así como de las combinaciones de los lugares de



custodia de la información de las evaluaciones, el jefe del Servicio de Protección y las personas que él designe, que serán las mínimas imprescindibles.

2. Las llaves de las cajas fuertes no podrán salir de la sede del laboratorio bajo ningún concepto, debiendo guardarse de forma oculta y segura, y en distinto lugar al que se custodien las claves de combinación para la apertura de las mismas.

3. Deberá ocultarse la identificación del fabricante, modelo, año de construcción u otros datos que puedan facilitar un conocimiento de las características de las cajas fuertes a las que se refieren.

4. Las claves de combinación para la apertura de las cajas fuertes y los códigos de control de la central de alarmas no deben conservarse en claro, sino de manera cifrada, debiendo ser modificados, obligatoriamente, en los siguientes casos:

a) Al recibirse los muebles de seguridad e instalarse la central de alarmas, modificando las claves y códigos que traen de fábrica.

b) Cada seis meses.

c) Cuando se produzca un cambio en las personas que hayan tenido acceso a las mismas, incluido el personal de las empresas de mantenimiento.

d) Cada vez que se produzca, o se sospeche que haya ocurrido, un incidente de seguridad que comprometa las claves o los códigos.

#### **Artículo 58. Acceso físico a la información de las evaluaciones.**

Cuando se precise el acceso físico a la información de las evaluaciones, el jefe del Servicio de Protección de la información, o persona designada por él, pondrá dicha información a disposición de los empleados del laboratorio que cuenten con las debidas autorizaciones de acceso a la misma, la cual deberá ser manejada exclusivamente en la zona de evaluación, estando bajo la responsabilidad de estas personas su custodia y control.

Una vez finalizado el manejo, se devolverá inmediatamente a la persona que hizo entrega de la misma, siendo almacenada en su lugar de custodia, donde permanecerá obligatoriamente.

#### **Artículo 59. Dispositivos técnicos de identificación.**

Siempre que el laboratorio lo considere necesario, podrá emplear dispositivos personales que faciliten y controlen el acceso, por su personal, a las zonas de acceso restringido. Los dispositivos serán diseñados de forma que se impida su empleo no autorizado, por lo que, cada uno de ellos se asignará a un empleado determinado, con su correspondiente código personalizado, que será conocido únicamente por el interesado.

De estos dispositivos no podrán determinarse las evaluaciones a cuya información tiene acceso el empleado al que se le asigna.

En su caso, deberá notificarse al Organismo de Certificación el sistema adoptado, debiéndose plasmar la operativa del mismo en el Plan de Protección.

### **SUBSECCIÓN 8ª. Seguridad de los sistemas de información**

#### **Artículo 60. Seguridad de la información sobre evaluaciones.**

1. La información de las evaluaciones es un bien que debe ser protegido de manera que se garantice su confidencialidad, su integridad y disponibilidad, a lo largo de toda su existencia,

con independencia del medio, soporte o formato en el que permanezca o se transmita. Para ello, también es necesario asegurar la integridad y disponibilidad de los servicios y recursos que sustentan dicha información.

2. Los mecanismos de seguridad del sistema de información que procese, almacene o transmita información de las evaluaciones, tienen como finalidad evitar accesos, destrucciones y modificaciones no permitidas, asegurando, al mismo tiempo, que la información es utilizada cuándo y cómo lo requieran los usuarios autorizados.

3. Los factores que se han de evaluar en la protección de la información de las evaluaciones serán los siguientes:

a) Confidencialidad, como servicio de seguridad que pretende que una información sea revelada exclusivamente a los usuarios, entidades o procesos autorizados.

b) Integridad, como medida que asegura que la información sea creada, modificada o borrada sólo por personas, entidades o procesos autorizados.

c) Disponibilidad, para que la información sea utilizable en el lugar, momento y forma que lo requieran los usuarios, entidades o procesos autorizados.

4. El laboratorio deberá concretar los principios y reglas básicas de seguridad, exigidos para la acreditación, en unos procedimientos específicos para la protección de la información de las evaluaciones tratadas en su sistema de información, cuya seguridad deberá estar necesariamente integrada en el sistema de protección del laboratorio.

5. La seguridad del sistema de información requiere la adecuada aplicación de procedimientos y normas que posibiliten el control de acceso al sistema, la distribución de responsabilidades, la segregación de funciones y la compartimentación de los entornos correspondientes a las evaluaciones y a la administración y gestión del laboratorio.

#### **Artículo 61. Usuario del sistema de información.**

1. El usuario del sistema de información que maneje información de las evaluaciones dependerá directamente, en todo lo referente a la seguridad del sistema, del administrador de seguridad del sistema de información, al que informará inmediatamente del menor indicio o conocimiento de cualquier hecho que afecte a la seguridad de la información de las evaluaciones.

2. La responsabilidad de cada usuario es básica para la seguridad del sistema. Por ello es imprescindible la autenticación del usuario. Se entenderá por autenticación el proceso que confirma su identidad.

Bajo ningún concepto este usuario podrá emplear equipos y medios particulares para el tratamiento de la información de las evaluaciones.

El usuario se asegurará que su código personal no es utilizado por otra persona, recomendándose la memorización del mismo, sin dejar constancia escrita o, en su caso, guardando el registro de forma oculta y segura; no hacer uso del código cuando se está siendo observado y no compartir, en ningún caso, el código personal con otros usuarios del sistema.

3. En los sistemas que lo permitan, el usuario realizará copias periódicas de seguridad de la información de las evaluaciones, bajo la supervisión del administrador de seguridad del sistema de información, quien llevará el control y registro oportuno.

#### **Artículo 62. Soportes de almacenamiento de información de las evaluaciones.**

1. Los soportes removibles reutilizables, que hayan contenido información de las evaluaciones, podrán volverse a emplear una vez que se haya efectuado el borrado seguro mediante procedimientos que garanticen el mismo.

Esto también se aplicará a los soportes fijos de los equipos utilizados en las pruebas de evaluación, así como en los destinados a la instalación, o recreación, del producto a evaluar y a su entorno de pruebas, que deberán borrarse de manera segura al término de cada evaluación.

El resto de soportes fijos de información del laboratorio deberán ser tratados según procedimientos específicos, que serán reseñados en los Procedimientos Operativos de seguridad, de forma que se imposibilite la extracción de información por personal no autorizado.

2. Toda información que tenga entrada mediante comunicaciones electrónicas, o soporte removable, deberá ser comprobada en un sistema aislado, previamente a su inclusión en el sistema de información del laboratorio, a fin de detectar la posible presencia de elementos extraños, dañinos o de mal funcionamiento. Dicha comprobación, y su resultado, quedarán anotados en el libro registro del laboratorio junto con la anotación de la entrada de la información.

#### **Artículo 63. Características físicas de las instalaciones.**

1. El sistema de información que se utilice para el tratamiento de la información de las evaluaciones deberá estar situado en la zona de evaluación y, obligatoriamente, ubicado en territorio nacional.

2. Los equipos periféricos de impresión de documentos estarán insonorizados, cuando las características de los mismos lo requieran, y así lo determine el Organismo de Certificación.

3. No se podrá realizar ningún cambio en la ubicación física de los elementos del sistema de información, sin el control del administrador de seguridad, y la aprobación del jefe del Servicio de Protección de la información de las evaluaciones.

#### **Artículo 64. Procedimientos operativos de seguridad.**

1. El administrador de seguridad del sistema de información del laboratorio elaborará unos Procedimientos Operativos de seguridad, donde se describirán, detalladamente, las operaciones necesarias para proteger dicho sistema.

2. Estos procedimientos operativos de seguridad han de cumplir los requisitos de seguridad para la acreditación del laboratorio, incluirse en el Plan de Protección y, adicionalmente, contemplarán lo siguiente:

a) La revisión bianual del grado de cumplimiento de la eficacia de los propios procedimientos operativos, y del cumplimiento de los requisitos de seguridad para la acreditación del laboratorio.

b) La aplicación de medidas de protección contra elementos dañinos o maliciosos (virus, caballos de Troya, gusanos, etc.).

c) El cambio trimestral de los códigos de acceso de los usuarios.

d) La aplicación de un sistema de borrado rápido o destrucción de la información de las evaluaciones, para casos de emergencia.

e) La utilización de un sistema de alimentación ininterrumpida, de duración suficiente, para salvaguardar los procesos en curso.

#### **Artículo 65. Interconexión de sistemas.**

1. Como norma general, el sistema de información donde se trate información de las evaluaciones, deberá estar aislado.

Excepcionalmente pueden existir situaciones en las que el sistema necesite estar interconectado con otros, bien para comunicar varias zonas de evaluación del laboratorio, separadas físicamente, en las que se realice la misma evaluación, o para permitir la comunicación en situaciones de naturaleza análoga.

En estas situaciones, la interconexión deberá ser autorizada por el Organismo de Certificación, que determinará los requisitos de seguridad que se deben implantar.

2. El acceso del laboratorio a redes públicas, para la consulta y descarga de información de vulnerabilidades, programas de uso en las evaluaciones y demás información relevante a las evaluaciones, no se podrá realizar en las áreas de evaluación o de protección, debiendo tramitarse la incorporación de esta información al sistema de información del laboratorio, conforme a lo requerido en el artículo 32, «Libro registro de información de las evaluaciones».

### **SECCIÓN 3ª. Requisitos de los procedimientos de evaluación**

#### **Artículo 66. Reconocimiento de actuaciones del laboratorio de evaluación.**

La certificación de la seguridad de un producto se inicia a instancias del solicitante ante el Organismo de Certificación, lo cual no obsta para que, independientemente, se puedan solicitar, por parte del mismo interesado, trabajos de evaluación equivalentes a los que requiere el Organismo de Certificación para la certificación de dicho producto.

En cualquier caso, el Organismo de Certificación únicamente reconocerá las actuaciones del laboratorio de evaluación que se realicen, completamente, bajo su conocimiento y seguimiento, conforme al procedimiento establecido en el Capítulo V del presente Reglamento.

#### **Artículo 67. Procedimientos de evaluación.**

Los procedimientos de evaluación del laboratorio que solicite la acreditación, deberán contemplar las obligaciones de coordinación e información con el Organismo de Certificación, indicadas en esta Sección.

Igualmente, y para la defensa de la validez y reconocimiento mutuo de certificados de la seguridad de los productos, el Organismo de Certificación trasladará al laboratorio las obligaciones requeridas, tanto al procedimiento de evaluación, como a los propios laboratorios de evaluación, en los acuerdos, convenios o contratos de reconocimiento mutuo en los que el solicitante de la certificación del producto quiera hacer valer la misma y el Organismo de Certificación opere.

#### **Artículo 68. Obligaciones de coordinación e información.**

El laboratorio deberá cumplir, en el desarrollo de sus trabajos de evaluación, con los requisitos de coordinación e información con el Organismo de Certificación que se incluyen en esta Sección.

#### **Artículo 69. Aprobación previa.**

1. El laboratorio de evaluación estará obligado a obtener aprobación previa, y por escrito, del Organismo de Certificación para comenzar los trabajos de evaluación.

En la aprobación previa deberá constar la asignación del responsable de la certificación del producto, por parte del Organismo de Certificación, a quien se dirigirán las comunicaciones relativas a la evaluación.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

2. Dicha aprobación se solicitará por el laboratorio mediante escrito, al que se acompañará lo siguiente:

a) Plan detallado de la evaluación, con las fases, tareas y unidades de trabajo correspondientes, la asignación e identificación del personal afecto a la evaluación y su responsabilidad en la misma.

b) Copia del contrato, o documento similar, que regule las relaciones entre el laboratorio y el solicitante de la certificación, en las que el laboratorio incluirá, obligatoriamente, las cláusulas necesarias para el cumplimiento de los requisitos para la acreditación del laboratorio.

#### **Artículo 70. Inicio y fin de los trabajos de evaluación.**

El laboratorio de evaluación estará obligado a comunicar, al Organismo de Certificación, el comienzo y término de cada fase, actividad, acción y unidad de trabajo de la evaluación, según se definan en la metodología y procedimientos de evaluación a aplicar. En función de su relevancia, el Organismo de Certificación podrá rebajar este requisito a la comunicación de fases, actividades o hitos señalados.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

#### **Artículo 71. Desviaciones del plan de evaluación.**

El laboratorio de evaluación estará obligado a comunicar, al Organismo de Certificación, las desviaciones con respecto al plan de evaluación, con análisis de las causas de la desviación, las medidas correctivas aplicadas por el laboratorio, y el nuevo plan de evaluación actualizado.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

#### **Artículo 72. Dificultades en la evaluación.**

El laboratorio de evaluación estará obligado a comunicar, al Organismo de Certificación, cualquier dificultad surgida en la aplicación o interpretación de las normas utilizadas, así como cualquier dificultad que condicione el normal transcurso de una evaluación.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

#### **Artículo 73. Informes de observación.**

El laboratorio estará obligado a remitir, al Organismo de Certificación, todos los informes de observación y de disconformidad emitidos e informará de su cierre, cuando ocurra, y de las medidas correctivas aplicadas por el solicitante de la certificación.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

#### **Artículo 74. Información técnica adicional.**

El laboratorio de evaluación estará obligado a facilitar toda información técnica adicional que sea necesaria para el análisis, por parte del Organismo de Certificación, de la información de las evaluaciones, incluyendo acceso y formación sobre programas y sistemas de evaluación, elaborados o adquiridos por el laboratorio, así como aquellos métodos y técnicas de análisis de vulnerabilidades empleados.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

#### **Artículo 75. Reuniones entre el solicitante y el laboratorio.**

El laboratorio de evaluación estará obligado a comunicar, e invitar a su asistencia, al Organismo de Certificación, de cuantas reuniones celebre dicho laboratorio con el solicitante de la certificación, con indicación de su naturaleza y objeto.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

#### **Artículo 76. Reuniones de seguimiento.**

El laboratorio de evaluación estará obligado a atender cuantas reuniones de seguimiento convoque el Organismo de Certificación. Dichas reuniones se convocarán por el responsable de la certificación del producto del Organismo de Certificación, y serán atendidas por el personal requerido para explicar e interpretar la información de las evaluaciones objeto de seguimiento. En el caso de información de las evaluaciones elaborada por el laboratorio, se podrá requerir la asistencia a la reunión de los autores de la misma.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

#### **Artículo 77. Puesta a disposición de dependencias y sistemas.**

El laboratorio de evaluación estará obligado a poner sus dependencias y sistemas de evaluación a disposición del Organismo de Certificación, para la realización, por parte del personal del mismo, de las tareas de verificación de la actividad de evaluación que se consideren oportunas.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

### **CAPÍTULO IV. Acreditación de laboratorios**

#### **SECCIÓN 1ª. Acreditación**

##### **Artículo 78. Acreditación.**

El Organismo de Certificación acreditará a los laboratorios solicitantes siguiendo el procedimiento establecido en la Sección 4ª de este Capítulo y en base al cumplimiento de los requisitos establecidos en el Capítulo III.

##### **Artículo 79. Solicitantes.**



Pueden solicitar esta acreditación cualesquiera laboratorios de evaluación de la seguridad de los sistemas de información, con independencia de su naturaleza jurídica, pública o privada, sin más limitación que la de realizar su actividad de evaluación en territorio español.

#### **Artículo 80. Contenido de la acreditación.**

La acreditación de un laboratorio supone el reconocimiento de su competencia técnica, de la adecuación de la gestión de la seguridad del mismo a las particularidades de la evaluación de la seguridad de las Tecnologías de la Información, y de la consideración de los requisitos de coordinación e información al Organismo de Certificación, que permitirá a éste basar su dictamen de certificación de un producto, entre otros factores, en el informe de evaluación del laboratorio acreditado.

La acreditación de un laboratorio no presupone, sin embargo, aceptación incondicional de los resultados de la actuación de evaluación de un producto determinado. Dicha aceptación se otorgará tras el análisis inicial de la solicitud de certificación, mediante el seguimiento de la labor de evaluación y tras el análisis del correspondiente informe técnico de evaluación, tal y como se define en el Capítulo V.

#### **Artículo 81. Duración de la acreditación.**

La acreditación, una vez concedida, se mantiene de manera indefinida, salvo cambios en las condiciones que motivaron su concesión, incumplimiento de dichas condiciones o renuncia expresa del laboratorio. Para el mantenimiento de la acreditación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del laboratorio y de su actuación, conforme se regula en este Capítulo.

### **SECCIÓN 2ª. Alcance de la acreditación**

#### **Artículo 82. Alcance de la acreditación.**

La acreditación se cualifica mediante el alcance, que limitará el reconocimiento de las actuaciones del laboratorio con relación al nivel de calificación de seguridad y con relación a las normas y niveles de evaluación.

#### **Artículo 83. Alcance con relación al nivel de calificación de seguridad.**

Con relación al nivel de calificación de seguridad se distinguen aquellos laboratorios con capacidad para manejar información y productos clasificados, de aquellos otros que operan en el régimen de la información y productos no clasificados.

#### **Artículo 84. Alcance con relación a las normas y niveles de evaluación.**

La certificación de la seguridad de los productos y sistemas de las Tecnologías de la Información puede requerir la evaluación de los mismos atendiendo a diferentes criterios, métodos y normas de evaluación.

Adicionalmente, dichas normas pueden distinguir niveles de evaluación y niveles de seguridad.

El Organismo de Certificación mantiene una relación actualizada de normas aplicables, según se establece en el Capítulo VI.

El laboratorio solicitante deberá indicar, en el alcance de la acreditación, aquellas normas y niveles, de la mencionada relación, en las que demuestra competencia técnica y experiencia acreditada.

### **SECCIÓN 3ª. Criterios de acreditación**

## **Artículo 85. Criterios generales.**

1. La competencia técnica del laboratorio solicitante se determinará, en primera instancia, por la correspondiente acreditación de esta competencia, conforme a lo regulado en la Ley 21/1992, de 16 de julio, de Industria, y en el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la Infraestructura para la Calidad y Seguridad Industrial, y en base al cumplimiento, por parte del laboratorio, de la Norma UNE-EN ISO/IEC 17025.

2. La acreditación de competencia técnica, que deberá ser concedida por una entidad de acreditación reconocida, ha de incluir, en su alcance, las normas de evaluación de la seguridad de los productos y sistemas de Tecnologías de la Información, aprobados por el Organismo de Certificación, y demás limitaciones requeridas por éste.

En particular, se reconocen las acreditaciones de competencia técnica emitidas por la Entidad Nacional de Acreditación, sin perjuicio de las acreditaciones emitidas por otras entidades de acreditación que satisfagan los requisitos establecidos en el Capítulo II del Reglamento de la Infraestructura para la Calidad y Seguridad Industrial.

3. Los requisitos adicionales, de gestión de la seguridad de la información de las evaluaciones, así como los de coordinación e información al Organismo de Certificación, se incluyen en el Capítulo III.

Los requisitos indicados en el párrafo anterior, se verificarán mediante la aplicación del procedimiento establecido en la siguiente Sección, sobre la base de una auditoría del laboratorio solicitante, que incluye el seguimiento de una evaluación de prueba bajo los procedimientos y requisitos del Organismo de Certificación.

## **Artículo 86. Criterios complementarios.**

Para aquellos casos que lo requieran, los criterios generales mencionados podrán ser completados o precisados por otros complementarios de carácter técnico, específicos para cada tipo de producto a evaluar, criterios, métodos y normas de evaluación de cada acreditación, o modificación del alcance de la solicitada, recogidos y publicados en los correspondientes documentos del Organismo de Certificación.

## **SECCIÓN 4ª. Procedimiento de acreditación**

### **Artículo 87. Proceso de acreditación.**

Aquellos laboratorios que deseen ser acreditados por el Organismo de Certificación, deberán someterse al proceso de acreditación establecido en la presente Sección.

### **Artículo 88. Solicitud de acreditación.**

La solicitud de acreditación deberá remitirse al Director del Organismo de Certificación adjuntando, como mínimo, la siguiente información, debidamente documentada:

- a) Personalidad jurídica de la entidad solicitante, con su número de identificación fiscal.
- b) Nombre del responsable del laboratorio y de la persona, o personas, con capacidad suficiente para obrar, que serán signatarias y, por tanto, responsables de la veracidad de las evaluaciones para las que el laboratorio solicita ser acreditado.
- c) Compromiso de cumplir los requisitos de acreditación del Organismo de Certificación, indicados en el Capítulo III, así como declaración de disponibilidad para la realización de la auditoría y actividades derivadas del proceso de acreditación.

- d) Relación y ubicación de las dependencias, delegaciones e instalaciones donde se realiza la actividad de evaluación de la seguridad de los productos y sistemas de las Tecnologías de la Información.
- e) Alcance de la acreditación solicitada, indicando el nivel de calificación de seguridad y las normas y niveles de evaluación.
- f) Relación y copia de los documentos del sistema de gestión de la calidad del laboratorio.
- g) Relación y copia de los documentos del sistema de gestión de la seguridad del laboratorio.
- h) Relación y copia de los manuales y procedimientos de evaluación del laboratorio.
- i) Certificado de acreditación de la competencia técnica emitido por ENAC, o entidad de acreditación reconocida, según lo indicado en el artículo 85 o, en su caso, certificado de haber iniciado dicho proceso de acreditación con la entidad correspondiente.
- j) Justificante del pago de las tasas de acreditación vigentes.
- k) Alcance y descripción de las evaluaciones de prueba que el solicitante pretende llevar a cabo, bajo las condiciones y procedimientos de este esquema, para la demostración del cumplimiento de los requisitos de acreditación, y que han de ser de alcance igual, o superior, al de la acreditación solicitada.

Esta solicitud podrá presentarse en cualquiera de los lugares previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

#### **Artículo 89. Modelo de solicitud de acreditación.**

Las solicitudes de acreditación de laboratorio se presentarán en los impresos establecidos al efecto, que estarán publicados en la dirección electrónica del Organismo de Certificación (<http://www.oc.ccn.cni.es>).

#### **Artículo 90. Subsanación y mejora de la solicitud de acreditación.**

A la recepción de la solicitud de acreditación, el Organismo de Certificación realizará una comprobación inicial de la información en ella contenida.

En caso de ser necesaria la subsanación o mejora de la solicitud de acreditación, se estará a lo dispuesto en el artículo 71 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Se admitirá durante la instrucción de la solicitud de acreditación la equivalencia del certificado de acreditación de la competencia técnica por certificado de encontrarse incurso en el proceso de acreditación de dicha competencia, siendo requisito definitivo para la acreditación del laboratorio, la certificación de su competencia técnica conforme a lo indicado en el artículo 85.

#### **Artículo 91. Notificación al solicitante.**

El Organismo de Certificación notificará al solicitante el inicio del procedimiento administrativo de acreditación, incluyendo en dicha notificación:

- a) El nombre y datos de contacto del responsable del procedimiento de acreditación, que será igualmente responsable de la dirección de la auditoría inicial del cumplimiento de los requisitos para la acreditación.

b) La fecha propuesta de comienzo de la auditoría indicada.

#### **Artículo 92. Preparación de la auditoría.**

Los técnicos designados por el Organismo de Certificación, con carácter previo a la auditoría, realizarán un estudio preliminar de la documentación recibida junto con la solicitud, relativa a los sistemas de calidad, seguridad y evaluación del laboratorio solicitante.

Las conclusiones de dicho estudio, en términos de observaciones sobre el cumplimiento e identificación de desconformidades de los requisitos para la acreditación, se remitirán al solicitante con una antelación no inferior a un mes de la fecha de comienzo de la auditoría. Junto a dichas conclusiones, y a la vista del estudio realizado, el Organismo de Certificación indicará la duración estimada de la auditoría, cuyo calendario definitivo se acordará en la fecha de comienzo de la misma.

El laboratorio solicitante podrá subsanar y mejorar la solicitud de acreditación en base a las conclusiones del estudio preliminar, con carácter previo a la realización de la auditoría.

#### **Artículo 93. Instrucción de la auditoría.**

La instrucción de la auditoría se realizará en tres fases: reunión inicial, desarrollo de la auditoría y reunión final.

a) Reunión inicial. En la fecha indicada por el Organismo de Certificación, se celebrará la reunión inicial de auditoría entre los representantes del laboratorio solicitante y el equipo auditor, designado por el Organismo de Certificación. En esta reunión se harán las presentaciones oportunas, se confirmará el plan y calendario de la auditoría y se revisarán las conclusiones del estudio preliminar de la solicitud.

b) Desarrollo de la auditoría. Durante esta fase se procederá a la observación del laboratorio solicitante durante la evaluación de prueba, y a la investigación del cumplimiento de los requisitos para la acreditación.

c) Reunión final. El equipo auditor se reunirá con los representantes de la entidad solicitante, con objeto de presentar un informe verbal de los resultados del desarrollo de la auditoría.

#### **Artículo 94. Informe del equipo auditor.**

El equipo auditor, en un plazo no superior a diez días contados desde la fecha de la reunión final de la auditoría, elaborará un informe con los resultados y con la información recopilada durante el desarrollo de la misma. Este informe será remitido al laboratorio solicitante para su conocimiento.

#### **Artículo 95. Audiencia previa.**

1. Una vez instruido el procedimiento de auditoría, se le pondrá de manifiesto al laboratorio solicitante y se le convocará a una reunión de audiencia previa a la resolución.

2. En dicha reunión, el Organismo de Certificación indicará la naturaleza, gravedad y consecuencias de las observaciones y desconformidades identificadas durante el procedimiento de auditoría, si las hubiere, con las implicaciones de las mismas en la resolución de la solicitud de acreditación.

3. El laboratorio solicitante, en un plazo no inferior a diez días ni superior a quince, podrá alegar y presentar los documentos y alegaciones que estime pertinentes.

4. Si antes del vencimiento del plazo, el laboratorio manifiesta su decisión de no efectuar alegaciones ni aportar nuevos documentos o justificaciones, se tendrá por realizado el trámite.

#### **Artículo 96. Resolución de la solicitud de acreditación.**

1. La resolución de la solicitud de acreditación se dictará de acuerdo con lo indicado en este artículo y en los plazos establecidos en el artículo 107, «Plazos y actos presuntos».

2. Esta Resolución, de acuerdo con lo previsto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, podrá ser objeto de recurso potestativo de reposición ante el Director del Organismo de Certificación, cuya resolución pone fin a la vía administrativa, o ser impugnada directamente ante el orden jurisdiccional contencioso-administrativo.

3. La resolución de desestimación será motivada. La resolución de acreditación contendrá adicionalmente los siguientes extremos:

a) Alcance de la acreditación concedida.

b) La fecha en vigor de la acreditación y referencia a su vigencia.

#### **Artículo 97. Vigencia de la acreditación.**

1. La acreditación se concederá por plazo indefinido, salvo cambios en las condiciones que motivaron su concesión, incumplimiento de dichas condiciones o renuncia expresa del laboratorio.

2. Para el mantenimiento de la acreditación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del laboratorio y de su actuación, conforme a lo establecido en el presente Reglamento.

#### **Artículo 98. Certificación del producto evaluado en el proceso de auditoría.**

Las evaluaciones utilizadas como prueba, en el proceso de auditoría del laboratorio, podrán servir de base para la correspondiente certificación de la seguridad de los productos evaluados, conforme a lo indicado en el Capítulo V.

### **SECCIÓN 5ª. Seguimiento de la actividad de evaluación**

#### **Artículo 99. Seguimiento continuo de la actividad de evaluación.**

El Organismo de Certificación, conforme al procedimiento de certificación de productos, establecido en el Capítulo V, realizará un seguimiento continuo de la actividad del laboratorio, a los efectos de la resolución de las solicitudes de certificación de productos.

Todas aquellas observaciones y disconformidades sobre los requisitos de acreditación del laboratorio, detectadas durante el seguimiento de las evaluaciones, serán comunicadas al laboratorio para su subsanación.

En el caso de disconformidad, o de no atender las observaciones realizadas, se estará a lo dispuesto en los artículos 104, 105 y 106.

#### **Artículo 100. Auditorías de seguimiento.**

1. De forma periódica, se realizarán auditorías de seguimiento a los laboratorios acreditados.

2. Los objetivos de las auditorías de seguimiento serán los siguientes:

- a) Comprobar que la entidad ha respetado, durante el período transcurrido desde la última auditoría, los criterios establecidos para la concesión de la acreditación.
- b) Verificar el cierre de las desviaciones detectadas en auditorías previas.
- c) Examinar cualquier cambio en la organización, procedimientos y recursos de la entidad, para la realización de las actividades incluidas en el alcance de su acreditación.
- d) Comprobar que se han respetado las obligaciones resultantes de la acreditación.
- e) Comprobar la actividad de la entidad para el alcance acreditado.

3. La frecuencia de las auditorías se establecerá en función de los resultados de visitas previas.

4. La primera auditoría de seguimiento se programará en un plazo no superior a doce meses desde la fecha inicial de acreditación. Las siguientes auditorías de seguimiento se realizarán antes de transcurridos dieciocho meses desde la realización de la última visita.

5. Las auditorías de seguimiento se realizarán con el mismo grado de detalle y rigor que la auditoría inicial de acreditación.

6. En la instrucción y resolución de la auditoría de seguimiento se seguirá lo dispuesto en los artículos 93 y 94 y, en todo caso, se atenderá al procedimiento general administrativo.

#### **Artículo 101. Ampliación del alcance de una acreditación.**

Cuando un laboratorio, ya acreditado, desee ampliar el alcance de su acreditación deberá solicitar formalmente dicha ampliación. Para ello, deberá utilizar el formulario de solicitud correspondiente. Se aplicará el procedimiento indicado en el artículo 78 adaptado, según proceda, en función del volumen y carácter de dicha ampliación.

#### **Artículo 102. Notificación de cambios.**

1. El laboratorio deberá comunicar, al Organismo de Certificación, cualquier cambio que se proponga efectuar sobre las condiciones iniciales en que se concedió la acreditación y, en particular, los que afecten a lo siguiente:

- a) Situación jurídica, comercial u organizativa del laboratorio.
- b) Organización y gestión, cuando afecten a personal directivo o a puestos clave en la organización del laboratorio o de la empresa.
- c) Políticas y procedimientos, cuando proceda.
- d) Locales de ubicación del laboratorio.
- e) Personal y otros recursos, cuando sean relevantes.
- f) Documentos normativos incluidos en el alcance de la acreditación.

2. Ante una comunicación de cambio, el Organismo de Certificación procederá a su revisión y establecerá las actividades necesarias para el mantenimiento de la acreditación del laboratorio. Dichas actividades podrán consistir en acciones de auditoría, por parte del



Organismo de Certificación, para comprobar el grado de cumplimiento de los requisitos de acreditación tras los cambios efectuados, así como en la actualización, por parte del laboratorio, de la documentación presentada en el proceso de acreditación.

#### **Artículo 103. Publicidad de las acreditaciones.**

El Organismo de Certificación podrá hacer pública la relación de laboratorios en proceso de acreditación, así como la de laboratorios acreditados incluyendo, en esta relación, la información del alcance de cada acreditación.

### **SECCIÓN 6ª. Formulación de observaciones, plazos y recursos**

#### **Artículo 104. Formulación de observaciones y retirada de la acreditación.**

El incumplimiento de las obligaciones derivadas de la acreditación, por parte de la entidad titular de la misma, dará lugar a la adopción de medidas, por parte del Organismo de Certificación, contra la entidad incumplidora.

Las medidas irán en función de la gravedad del incumplimiento y podrán consistir en formulación de observaciones, retirada parcial o retirada total de la acreditación.

#### **Artículo 105. Actuaciones irregulares e incumplimientos.**

Se entenderá por actuaciones irregulares e incumplimientos leves, aquellas actuaciones que, sin adecuarse a lo establecido en el presente Reglamento, no afecten a la validez final de la actividad de evaluación de la entidad ni a la seguridad de terceros.

Las actuaciones irregulares y los incumplimientos leves serán objeto de observación, que podrá notificarse por los equipos de auditoría y seguimiento de las evaluaciones. El laboratorio deberá subsanar la causa que dio lugar a las observaciones, en el plazo de diez días.

#### **Artículo 106. Retirada de la acreditación.**

El incumplimiento reiterado de los requisitos de acreditación, o la no subsanación reiterada de las observaciones recibidas, darán lugar a la retirada, total o parcial, de la acreditación a la que se refiera.

La resolución de retirada de acreditación se dictará, de oficio, por el Organismo de Certificación.

La retirada de la acreditación obligará al solicitante al cese inmediato del uso de la condición de laboratorio acreditado, así como a la retirada de esta condición en todos los documentos o información en los que éste la haga manifiesta.

#### **Artículo 107. Plazos y actos presuntos.**

El plazo para resolver la solicitud de acreditación de laboratorio, y notificar la correspondiente resolución, será de seis meses. Este mismo plazo se aplicará a las solicitudes de ampliación del alcance de una acreditación previa.

A los efectos previstos en el artículo 43 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, las solicitudes de acreditación se entenderán estimadas de no recaer resolución expresa en los plazos establecidos en cada caso, con las salvedades y excepciones indicadas en dicho precepto.

#### **Artículo 108. Recursos.**

La actuación del Organismo de Certificación debe siempre atenerse a los principios generales de actuación recogidos en el artículo 3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

De acuerdo con lo previsto en los artículos 116 y 117 de la citada Ley, así como en los artículos 10, 14 y 46 de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa, frente a la actuación del Organismo de Certificación, en materia de acreditación, se podrá interponer:

- a) En el plazo de un mes, recurso potestativo de reposición ante el Director de dicho organismo, cuya resolución pone fin a la vía administrativa, o
- b) directamente, en el plazo de dos meses, recurso contencioso-administrativo, ante la Sala de dicha índole, del Tribunal Superior de Justicia de Madrid.

## **CAPÍTULO V. Certificación de productos y sistemas**

### **SECCIÓN 1ª. Certificación**

#### **Artículo 109. Certificación de seguridad de productos y sistemas.**

El Organismo de Certificación certificará la seguridad de los productos y sistemas de Tecnologías de la Información, siguiendo el procedimiento establecido en este Capítulo y tras considerar, entre otras pruebas de la instrucción del procedimiento, los informes de evaluación emitidos por los laboratorios acreditados conforme a lo establecido en el Capítulo IV, y realizados atendiendo a los criterios, métodos y normas de evaluación de la seguridad indicados en el Capítulo VI.

#### **Artículo 110. Reconocimiento de veracidad de propiedades de seguridad.**

La certificación de la seguridad de un producto o sistema de las Tecnologías de la Información supone el reconocimiento de la veracidad de las propiedades de seguridad de su correspondiente declaración de seguridad.

#### **Artículo 111. Valoración de idoneidad.**

La certificación de la seguridad de un producto o sistema no presupone declaración de idoneidad de uso en cualquier escenario o ámbito de aplicación. Para valorar la idoneidad de un producto o sistema deberán tenerse en cuenta otras circunstancias, incluidas las restricciones establecidas en su declaración de seguridad para la correcta interpretación del certificado.

#### **Artículo 112. Vigencia de la certificación.**

La certificación, una vez concedida, se mantiene de manera indefinida, salvo cambios en las condiciones que motivaron su concesión, tales como avances tecnológicos, aparición de nuevas vulnerabilidades explotables, incumplimiento de las condiciones de uso del certificado, cambios en el propio producto o renuncia expresa del solicitante. Para la vigilancia de la vigencia de la certificación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del producto, de su entorno y del uso del certificado.

### **SECCIÓN 2ª. Alcance de la certificación**

#### **Artículo 113. Alcance de la certificación.**

La certificación se limita mediante el correspondiente alcance, que incluye la definición del producto evaluado y las normas y niveles de evaluación.

El Organismo de Certificación, en la determinación del alcance, realizará la definición más precisa posible del mismo, al objeto de evitar confusión alguna entre el producto comercial y el producto evaluado, en el supuesto de que ambos no coincidan exactamente.

#### **Artículo 114. Alcance con relación al producto o sistema evaluado.**

La certificación deberá hacer referencia, e identificar inequívocamente, al producto evaluado, así como a su declaración de seguridad.

Dicha declaración de seguridad también deberá contener la identificación precisa del producto evaluado, así como la especificación de su entorno de uso, incluyendo las amenazas previstas, políticas de seguridad e hipótesis aplicables al caso, además de los objetivos de seguridad del producto o sistema y la relación de requisitos de seguridad exigibles al mismo.

Los detalles de la declaración de seguridad podrán variar conforme a las normas aplicadas en la evaluación, pero toda declaración deberá ser un reflejo cierto, claro y preciso de las propiedades de seguridad del producto o sistema evaluado.

#### **Artículo 115. Alcance con relación a las normas y niveles de evaluación.**

La certificación incluirá en su alcance los criterios, métodos y normas de evaluación empleados en la evaluación del producto o sistema, así como el nivel que se haya alcanzado, de los definidos en cada norma, y la relación de interpretaciones e instrucciones técnicas aplicadas.

### **SECCIÓN 3ª. Criterios de certificación**

#### **Artículo 116. Informe técnico de evaluación.**

La principal prueba en la instrucción del procedimiento de certificación es el Informe Técnico de Evaluación, emitido por el laboratorio acreditado y realizado cumpliendo con el procedimiento de certificación, establecido en la siguiente Sección.

#### **Artículo 117. Criterios complementarios.**

1. En el ejercicio de su función evaluadora, el Organismo de Certificación podrá, a su criterio, realizar análisis, pruebas, inspecciones y auditorías al laboratorio, al producto a evaluar y al solicitante de la certificación, en los aspectos y requisitos de garantía de seguridad que les sean de aplicación según los criterios y métodos de evaluación utilizados.
2. En particular, será atribución indelegable del Centro Criptológico Nacional el análisis, valoración y acreditación de los algoritmos y medios de cifra que utilice el producto a evaluar.
3. Igualmente, el seguimiento de la evaluación permitirá, al Organismo de Certificación, determinar el ajuste de la evaluación a los procedimientos derivados de las normas aplicables y, por tanto, el ajuste del Informe de Evaluación a las mismas.

### **SECCIÓN 4ª. Procedimiento de certificación**

#### **Artículo 118. Proceso de certificación.**

Aquellos interesados que deseen certificar la seguridad de un producto o sistema de Tecnologías de la Información, deberán someterse al proceso establecido en la presente Sección.

#### **Artículo 119. Solicitud de certificación.**

1. La solicitud de certificación deberá remitirse al Director del Organismo de Certificación incluyendo en la misma, como mínimo, la siguiente información debidamente documentada:

- a) Personalidad jurídica de la entidad solicitante, con su número de identificación fiscal.
- b) Nombre del responsable del solicitante y de la persona, o personas, con capacidad suficiente para obrar, que serán signatarias y, por tanto, responsables de la veracidad de las evidencias y pruebas documentales aportadas.
- c) Declaración responsable de conocer y aceptar los términos y requisitos aplicables a la certificación solicitada, incluyendo los derechos de acceso, publicación y limitación de la información de las evaluaciones por parte del Organismo de Certificación.
- d) Identificación del laboratorio, acreditado por el Organismo de Certificación, que realizará la evaluación técnica de la seguridad del producto o sistema cuya certificación se solicita.
- e) Relación y ubicación de las dependencias, delegaciones e instalaciones donde se realiza la actividad de desarrollo o integración del producto a evaluar.
- f) Alcance de la certificación solicitada, indicando el producto a evaluar y su versión, así como las normas y niveles de evaluación aplicables.
- g) Justificante del pago de las tasas de certificación en vigor.

Esta solicitud podrá presentarse en cualquiera de los lugares previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. Junto a la solicitud de certificación, se remitirá al Organismo de Certificación la declaración de seguridad, o perfil de protección en su caso, del producto a evaluar y, cuando esto sea posible, una unidad, copia o ejemplar de este último.

3. Paralelamente a la solicitud, el solicitante gestionará con el laboratorio acreditado elegido, el plan detallado de la evaluación, así como el contrato o documento similar que regule las relaciones entre el laboratorio y el solicitante.

#### **Artículo 120. Modelo de solicitud de certificación.**

Las solicitudes de certificación de la seguridad de productos o sistemas de Tecnologías de la Información se presentarán en los impresos establecidos al efecto, que estarán publicados en la dirección electrónica del Organismo de Certificación (<http://www.oc.ccn.cni.es>).

#### **Artículo 121. Subsanación y mejora de la solicitud de certificación.**

1. A la recepción de la solicitud de certificación, el Organismo de Certificación realizará una comprobación inicial de la información en ella contenida.

2. En caso de ser necesaria la subsanación o mejora de la solicitud de certificación, se estará a lo dispuesto en el artículo 71 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Se podrá, igualmente, requerir al solicitante el suministro de unidades, copias o ejemplares adicionales del producto a evaluar, conforme a la naturaleza del mismo y a las necesidades derivadas de los criterios complementarios de certificación indicados en el artículo 117.

4. Será obligación del solicitante mantener actualizados el material y la documentación incluidos en la solicitud de certificación, en poder del Organismo de Certificación, en el caso de que alguno de éstos se modifique a resultados del proceso de evaluación correspondiente.

#### **Artículo 122. Notificación al solicitante.**

El Organismo de Certificación notificará al solicitante el inicio del procedimiento administrativo de certificación, incluyendo en dicha notificación el nombre y los datos de contacto del responsable del procedimiento de certificación.

#### **Artículo 123. Aprobación del comienzo de la evaluación.**

1. El laboratorio solicitará, al Organismo de Certificación, la autorización para comenzar la actividad de evaluación. La solicitud irá acompañada de:

a) El plan detallado de la evaluación, con las fases, tareas y unidades de trabajo correspondientes, la asignación e identificación del personal afecto a la evaluación y su responsabilidad en la misma.

b) La copia del contrato o documento similar que regule las relaciones entre el laboratorio y el solicitante de la certificación, en las que el laboratorio incluirá, obligatoriamente, las cláusulas necesarias para el cumplimiento de los requisitos de seguridad para la acreditación del laboratorio.

2. Para la resolución de la solicitud de autorización, se convocará una reunión con el laboratorio a la que asistirá el personal del laboratorio asignado a la evaluación y el equipo de certificación, designado por el Organismo de Certificación.

En esta reunión se harán las presentaciones oportunas y, por parte del laboratorio, se expondrá el plan y calendario de evaluación, así como los aspectos técnicos más relevantes de la misma.

3. El laboratorio deberá demostrar la adecuación y suficiencia de los medios materiales y humanos asignados a la evaluación, en particular, en lo referente a la formación del personal evaluador en los detalles del alcance de la certificación.

4. El Organismo de Certificación resolverá sobre la autorización del comienzo de la actividad de evaluación, incluyendo la designación del responsable del procedimiento de certificación.

#### **Artículo 124. Instrucción de la evaluación.**

1. La instrucción de la evaluación comenzará con el desarrollo de los trabajos de evaluación por parte del laboratorio, durante el cual, el Organismo de Certificación realizará el seguimiento de la actividad de evaluación del producto o sistema cuya certificación se ha solicitado.

Para la realización de este seguimiento, el Organismo de Certificación recibirá, del laboratorio, la información de la evaluación indicada en la Sección 3ª del Capítulo III, a la vista de la cual convocará las reuniones de seguimiento que considere oportunas. En particular, será de especial atención el ajuste de la ejecución de la evaluación al correspondiente plan de evaluación.

2. La instrucción de la evaluación terminará con el Informe Técnico de Evaluación, que remitirá el laboratorio al Organismo de Certificación, en los siguientes casos:

a) Al término del plazo de evaluación.

b) Por solicitud del Organismo de Certificación. Dicha solicitud se podrá cursar cuando se haya superado, sin subsanar, el plazo de tres meses de cualquier observación o disconformidad, notificada al solicitante de la certificación, o a los tres meses de retraso no justificado del plan de evaluación.

#### **Artículo 125. Informe de certificación.**

El Organismo de Certificación, en un plazo no superior a treinta días contados desde la fecha de la recepción del Informe Técnico de Evaluación, elaborará un informe con los resultados y conclusiones de la evaluación, así como de la actividad de seguimiento, que será enviado al solicitante de la certificación para su conocimiento.

#### **Artículo 126. Audiencia previa a la resolución.**

1. Terminada la instrucción de la evaluación, se pondrá de manifiesto al solicitante de la certificación, convocándole a una reunión de audiencia previa a la resolución.

2. En dicha reunión, el Organismo de Certificación indicará la naturaleza, gravedad y consecuencias de las observaciones y disconformidades, identificadas durante la instrucción del expediente de certificación, si las hubiere, con las implicaciones de las mismas en la resolución de la solicitud de certificación.

3. El solicitante de la certificación, en un plazo no inferior a diez días ni superior a quince, podrá alegar y presentar los documentos y alegaciones que estime pertinentes.

4. Si antes del vencimiento del plazo, el solicitante manifiesta su decisión de no efectuar alegaciones ni aportar nuevos documentos o justificaciones, se tendrá por realizado el trámite.

#### **Artículo 127. Resolución de la solicitud de certificación.**

1. La resolución de la solicitud de certificación se dictará de acuerdo con lo indicado en este artículo, y en los plazos establecidos en el artículo 137, del presente Reglamento.

Esta resolución, de acuerdo con lo previsto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, podrá ser objeto de recurso potestativo de reposición ante el Director del Organismo de Certificación, cuya resolución pone fin a la vía administrativa, o ser impugnada directamente ante el orden jurisdiccional contencioso-administrativo.

2. Las resoluciones de desestimación serán motivadas. La resolución de certificación contendrá, adicionalmente, los siguientes extremos:

a) Alcance de la certificación concedida.

b) La fecha de la entrada en vigor de la certificación y referencia a su vigencia.

#### **Artículo 128. Vigencia de la certificación.**

La certificación se concederá por plazo indefinido, salvo cambios en las condiciones que motivaron su concesión, incumplimiento de dichas condiciones o renuncia expresa del solicitante.

Para el mantenimiento de la certificación, el Organismo de Certificación realizará, de oficio, las necesarias revisiones de su vigencia y actividades de vigilancia del uso del certificado, conforme a lo establecido en el artículo 129 siguiente.

#### **Artículo 129. Revisiones de vigencia.**

Cada dos años se realizará una revisión de la vigencia de cada certificado emitido. El objeto 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.

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.

## **SECCIÓN 5ª. Seguimiento del uso de los certificados**

### **Artículo 130. Seguimiento continuo del uso del certificado.**

El Organismo de Certificación realizará 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.

El incumplimiento de las condiciones de uso del certificado, reguladas en el Capítulo VII, podrá dar lugar a la anulación del certificado, mediante resolución expresa del Director del Organismo de Certificación.

### **Artículo 131. Ampliación del alcance de la certificación.**

Cuando se desee ampliar el alcance de la certificación de un producto o sistema, el interesado solicitará formalmente dicha ampliación. Para ello deberá utilizar el formulario de solicitud correspondiente. Se aplicará el procedimiento de certificación, indicado en el Capítulo V, adaptado, según proceda, en función del volumen y carácter de dicha ampliación.

### **Artículo 132. Notificación de cambios.**

El solicitante de la certificación deberá comunicar al Organismo de Certificación los cambios que identifique, relativos al entorno de seguridad del producto certificado, así como cualquier otro cambio fundamental que se produjese en las condiciones iniciales en que se concedió la certificación.

### **Artículo 133. Publicidad de las certificaciones.**

El Organismo de Certificación podrá hacer pública la relación de productos en proceso de evaluación y la de productos certificados, incluyendo en esta relación la declaración de seguridad de los mismos, así como información derivada del informe de certificación establecido en el artículo 125.

## **SECCIÓN 6ª. Formulación de observaciones, plazos y recursos**

### **Artículo 134. Observaciones y retirada de la certificación.**

El incumplimiento, por un solicitante, de las obligaciones derivadas de la certificación dará lugar, en función de la gravedad de la infracción, a la formulación de observaciones o a la retirada de la certificación.

### **Artículo 135. Actuaciones irregulares e incumplimientos.**

Las actuaciones irregulares y los incumplimientos leves, entendiéndose por tales los que no desvirtúen las restricciones y obligaciones derivadas del uso de la condición de producto certificado, serán objeto de observación, que se notificará, de oficio, al solicitante de la certificación.



El solicitante de la certificación deberá subsanar la causa de tales observaciones en un plazo de diez días.

#### **Artículo 136. Retirada de la certificación.**

1. La disconformidad sostenida, en relación con las restricciones y obligaciones del uso de la condición de producto certificado o con los requisitos para la certificación, así como la falta de subsanación de las observaciones recibidas, darán lugar a la retirada, total o parcial, de la certificación a la que se refiera.

2. La resolución de retirada de certificación se dictará, de oficio, por el Organismo de Certificación.

3. La retirada de la certificación obligará al solicitante al cese inmediato del uso de la condición de producto certificado, en todos los documentos o información en los que la haga manifiesta, y a la retirada del mercado de los productos así etiquetados.

#### **Artículo 137. Plazos y actos presuntos.**

1. El plazo para resolver la solicitud de certificación de productos, y notificar la correspondiente resolución, será de dos meses, contados a partir de la fecha de recepción del Informe Técnico de Evaluación del laboratorio.

Este mismo plazo se aplicará a las solicitudes de ampliación del alcance de una certificación previa.

2. El plazo para resolver la solicitud de comienzo de evaluación, y notificar la correspondiente resolución, será de un mes.

3. A los efectos previstos en el artículo 43 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, las solicitudes de certificación se entenderán estimadas de no recaer resolución expresa en los plazos establecidos en cada caso, con las salvedades y excepciones indicadas en dicho precepto.

#### **Artículo 138. Recursos.**

La actuación del Organismo de Certificación se atenderá a los principios generales de actuación recogidos en el artículo 3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

De acuerdo con lo previsto en los artículos 116 y 117 de la citada Ley, y en los artículos 10, 14 y 46 de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa, frente a la actuación del Organismo de Certificación, en materia de certificación, los interesados podrán interponer:

a) En el plazo de un mes, recurso potestativo de reposición, ante el Director del dicho organismo, cuya resolución pone fin a la vía administrativa, o

b) directamente, en el plazo de dos meses, recurso contencioso-administrativo, ante la Sala de dicha índole, del Tribunal Superior de Justicia de Madrid.

### **CAPÍTULO VI. Criterios y metodologías de evaluación**

#### **Artículo 139. Estado del arte.**

El Organismo de Certificación certificará la seguridad de los productos y sistemas de Tecnologías de la Información conforme al estado del arte más avanzado en materia de evaluación de la seguridad. Dicho estado del arte se ha de combinar con el debido reconocimiento de los certificados emitidos.

A tal fin, el Organismo de Certificación exigirá a los laboratorios acreditados la realización de su actividad conforme a criterios, métodos y normas bien establecidos y reconocidos. Tales normas se podrán ver complementadas por interpretaciones o instrucciones técnicas emitidas por el Organismo de Certificación.

#### **Artículo 140. Normas de evaluación.**

1. El Organismo de Certificación, a los efectos de su utilización y cumplimiento por parte de los laboratorios, elevará a carácter de norma cualquier documento de orden técnico que sea de su interés, mediante la publicación del mismo en su dirección electrónica (<http://www.oc.ccn.cni.es>) y su comunicación a los laboratorios acreditados.

2. La publicación de una nueva norma, o la actualización de una existente, y la determinación de su entrada en vigor, se realizarán previa presentación a los laboratorios acreditados de las nuevas normas y de sus diferencias técnicas con respecto a las normas vigentes, a los efectos que pudieran derivarse sobre las acreditaciones en vigor.

3. Las normas relacionadas en el artículo 141 siguiente, se entienden de aplicación en su última versión disponible al comienzo de cada solicitud de certificación. No obstante lo anterior, se podrá consultar la relación de normas, criterios, metodologías y requisitos, así como su aplicabilidad, en la dirección electrónica del Organismo de Certificación (<http://www.oc.ccn.cni.es>).

#### **Artículo 141. Criterios de evaluación.**

Los criterios de evaluación serán los recogidos en las siguientes normas:

- a) «Common Criteria for Information Technology Security Evaluation» (abreviado, CC).
- b) ISO/IEC 15408, «Evaluation Criteria for IT Security».
- c) «Information Technology Security Evaluation Criteria» (abreviado, ITSEC). Office for Official Publications of the European Communities.

#### **Artículo 142. Metodologías de evaluación.**

Las metodologías de evaluación serán las recogidas en las siguientes normas:

- a) «Common Methodology for Information Technology Security Evaluation» (abreviado, CEM).
- b) ISO/IEC 18045, «Methodology for IT Security Evaluation».
- c) «Information Technology Security Evaluation Manual» (abreviado, ITSEM). Office for Official Publications of the European Communities.

#### **Artículo 143. Requisitos de seguridad específicos.**

Los requisitos de seguridad específicos serán los recogidos en la Norma ISO/IEC 19790, «Requisitos de Seguridad para Módulos Criptográficos».

#### **Artículo 144. Interpretaciones e instrucciones técnicas.**

Se podrá consultar la relación de interpretaciones e instrucciones técnicas en vigor, de aplicación en este Esquema, en la dirección electrónica del Organismo de Certificación (<http://www.oc.ccn.cni.es>), agrupadas por la norma principal a la que afectan y sus versiones aplicables.

## **CAPÍTULO VII. Uso de la condición de laboratorio acreditado y de producto certificado**

### **Artículo 145. Referencia a la condición de laboratorio acreditado.**

La referencia a la condición de laboratorio acreditado, o el uso del distintivo correspondiente, en los informes emitidos como resultado de las actividades de evaluación amparadas por la acreditación, es el medio por el cual los laboratorios acreditados declaran públicamente el cumplimiento de todos los requisitos de acreditación en la realización de dichas evaluaciones.

Cualquier uso que no esté expresamente permitido en este Reglamento deberá ser consultado al Organismo de Certificación.

### **Artículo 146. Informes derivados de la evaluación.**

1. La referencia a la condición de laboratorio acreditado debe ser utilizada en todos los informes emitidos como resultado de las actividades de evaluación, amparadas por la acreditación, como garantía del cumplimiento de los requisitos de dicha acreditación.

2. Cualquier informe o certificado que no incluya la referencia a la condición de laboratorio acreditado, no garantiza el cumplimiento de los requisitos de acreditación y, por tanto, no será aceptado por el Organismo de Certificación, como parte de una evaluación acreditada, ni podrá beneficiarse del reconocimiento de los certificados emitidos por el Organismo de Certificación.

3. En el caso de informes que incluyan, tanto datos amparados por la acreditación, como datos no amparados por la misma, se seguirán las siguientes reglas:

a) Se señalarán los datos no amparados por la acreditación mediante la utilización de un asterisco o similar. Asimismo, se deberá incluir en un lugar visible la siguiente leyenda: «Los ensayos/inspecciones marcados no están incluidos en el alcance de acreditación».

b) Cuando un informe de evaluación contenga interpretaciones, opiniones o cualquier otra información relativa a investigación, que no sea parte de la metodología de ensayo seguida en esa evaluación, se deberá incluir la siguiente advertencia: «Las opiniones, interpretaciones, etc., que se indican a continuación, están fuera del alcance de la acreditación del Organismo de Certificación».

### **Artículo 147. Otros documentos de laboratorio acreditado.**

En documentos de tipo publicitario, folletos o anuncios relacionados con la actividad de evaluación acreditada, o en material de papelería (papel de cartas, impresos tales como facturas o pedidos, sobres, etc.), los laboratorios podrán usar la referencia a la condición de acreditado con las restricciones que se mencionan en el artículo 148.

### **Artículo 148. Restricciones al uso de la condición de laboratorio acreditado.**

La referencia a la condición de laboratorio acreditado no se debe utilizar en los siguientes supuestos:

a) En informes o certificados que no contengan ningún dato obtenido de actividades acreditadas.

b) En documentos en los que no se identifique la organización a la que ha sido concedida la acreditación.

c) De forma que pueda sugerir que el Organismo de Certificación aprueba, acepta o, de alguna manera, se responsabiliza de los resultados contenidos en un informe o certificado (por ejemplo, mediante el uso de sellos con la referencia al Organismo de Certificación).

d) Cuando el laboratorio haya perdido su condición de acreditado, ya sea de forma voluntaria o por retirada de la acreditación.

e) En las tarjetas de visita del personal de los laboratorios acreditados.

f) En cualquier situación que pueda dar lugar a una interpretación incorrecta de la condición del laboratorio acreditado, o que pueda inducir a considerar actividades no acreditadas como cubiertas por la acreditación. Concretamente:

1º Cuando se use en impresos (ofertas, cartas, presentaciones comerciales, material publicitario, páginas Web, etc.), que hagan referencia a actividades no acreditadas, se deberá incluir una mención, con el mismo tamaño de letra que el usado en el cuerpo del documento en cuestión, en la que se aclare este hecho (por ejemplo: «Las actividades recogidas en el presente escrito no están incluidas en el alcance de la acreditación del Organismo de Certificación»).

2º Cuando se use en impresos (ofertas, cartas, presentaciones comerciales, material publicitario, etc.), que incluyan tanto actividades acreditadas como no acreditadas, su uso deberá ser tal, que permita al lector distinguir aquellas actividades que están acreditadas de las que no lo están.

3º Cuando un laboratorio esté compuesto por varios emplazamientos distintos, y no todos ellos hayan sido acreditados, solamente aquellos que sí lo hayan sido podrán hacer uso de la referencia a la condición de acreditado. Cuando se emitan documentos comunes a todo el laboratorio se deberá incluir una cláusula que indique esta condición (por ejemplo: «Se encuentra disponible la lista de emplazamientos acreditados y sus alcances»).

4º Cuando una organización acreditada pertenezca a otra mayor, no deberá existir confusión sobre cual de ellas está acreditada.

g) En cualquier otro supuesto que resulte abusivo, a juicio del Organismo de Certificación.

#### **Artículo 149. Uso de la condición de producto certificado.**

El uso del distintivo especificado en el artículo 155, o la referencia a la condición de producto certificado, es el medio por el cual los solicitantes de la certificación declaran, públicamente, el cumplimiento de todos los requisitos exigibles para dicha certificación, la conformidad con determinados perfiles de protección, en su caso, y el cumplimiento de las disposiciones legales aplicables.

Cualquier uso del certificado que no esté expresamente permitido en este Reglamento, deberá ser consultado al Organismo de Certificación.

#### **Artículo 150. Producto y documentación.**

La referencia a la condición de producto certificado debe ser utilizada en toda la documentación de administración y uso de dicho producto, y que se haya remitido como evidencia de la evaluación.

La referencia a la condición de producto certificado se incluirá también en el propio producto, siguiendo las reglas de marcado indicadas en el artículo 155.

#### **Artículo 151. Otros documentos de producto certificado.**

En documentos de tipo publicitario, folletos o anuncios relacionados con el producto certificado, así como en los contratos públicos y privados, licitaciones y documentación preparatoria, el titular de la certificación podrá usar la referencia a la condición de producto certificado con las restricciones que se mencionan en el artículo 152.

#### **Artículo 152. Restricciones al uso de la condición de producto certificado.**

La referencia a la condición de producto certificado no debe utilizarse en los siguientes supuestos:

a) Sin una referencia completa e inequívoca del alcance del certificado. Como mínimo se citará:

1º Nombre y versión del producto evaluado.

2º La norma utilizada para la evaluación y el nivel alcanzado en la misma (por ejemplo: ISO/IEC 15408 EAL2).

3º Referencia a la declaración de seguridad del producto certificado, indicando el procedimiento para obtener una copia de la misma.

b) De forma que pueda sugerir que el certificado se aplica a todo un sistema o producto, cuando el producto evaluado es sólo una parte del mismo.

c) De forma que se sugieran propiedades de seguridad del producto certificado no reflejadas en su declaración de seguridad.

d) Cuando el certificado haya sido anulado por cualquier motivo.

e) En cualquier otro uso que resulte abusivo a juicio del Organismo de Certificación.

#### **Artículo 153. Otras obligaciones de la condición de producto certificado.**

La referencia a la condición de producto certificado obligará al solicitante de la certificación a:

a) Mantener registro de todas las reclamaciones presentadas al solicitante, relativas a la seguridad del producto certificado, y a tener esta información disponible para el Organismo de Certificación.

b) Tomar las acciones correctoras apropiadas con respecto a tales reclamaciones y a cualquier deficiencia encontrada en los productos, que afecten la conformidad con los requisitos para la certificación.

c) Documentar las acciones tomadas.

#### **Artículo 154. Distintivo de laboratorio acreditado.**

La condición de laboratorio acreditado puede complementarse mediante el uso del distintivo descrito a continuación (figura 2):

a) Color de fondo, diseño y detalles del escudo y tipo de letra, conforme a lo dispuesto en el Real Decreto 1465/1999, de 17 de septiembre, que establece los criterios de imagen institucional y regula la producción documental y el material impreso de la Administración General del Estado, y en la Orden de 27 de septiembre de 1999 por la que se aprueba el Manual de Imagen Institucional de la Administración General del Estado y se dictan normas de desarrollo del Real Decreto 1465/1999 citado (consultar página web «<http://www.060.es>»).

b) Círculo exterior de 180 unidades de medida de diámetro. Tamaño de letra nueve veces inferior al radio, esto es, de 20 unidades de medida.

c) Leyenda exterior, «ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD TI», sobre un arco de 270 grados, 140 unidades de medida de radio, y ángulo inicial de 135 grados, sentido negativo del texto.

d) Leyenda interior, «LABORATORIO ACREDITADO», sobre un arco de radio de 100 unidades de medida, iguales ángulos y recorrido que el exterior.

e) Escudo de España equidistante en sus aristas a la leyenda interior.

f) Si se reduce o amplía el distintivo, deberán respetarse las proporciones de este modelo.

g) La altura del distintivo no será inferior a 15 mm.

Figura 2. Distintivo de laboratorio acreditado.pdf

#### **Artículo 155. Distintivo de producto certificado.**

Los productos certificados deberán llevar un distintivo conforme a lo siguiente (figura 3):

a) Color de fondo, diseño y detalles del escudo y tipo de letra, conforme a lo dispuesto en el Real Decreto 1465/1999, de 17 de septiembre, que establece los criterios de imagen institucional y regula la producción documental y el material impreso de la Administración General del Estado, y en la Orden de 27 de septiembre de 1999 por la que se aprueba el Manual de Imagen Institucional de la Administración General del Estado y se dictan normas de desarrollo del Real Decreto 1465/1999 citado (consultar página web «<http://www.060.es>»).

b) Círculo exterior de 180 unidades de medida de diámetro. Tamaño de letra nueve veces inferior al radio, esto es, de 20 unidades de medida.

c) Leyenda exterior, «ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD TI», sobre un arco de 270 grados, 140 unidades de medida de radio, y ángulo inicial de 135 grados, sentido negativo del texto.

d) Leyenda interior, «PRODUCTO CERTIFICADO», sobre un arco de radio de 100 unidades de medida, iguales ángulos y recorrido que el exterior.

e) Escudo de España equidistante en sus aristas a la leyenda interior.

f) Si se reduce o amplía el distintivo, deberán respetarse las proporciones de este modelo.

g) La altura del distintivo no será inferior a 15 mm, excepto cuando esto no sea posible a causa del tipo de producto.

Figura 3. Distintivo de producto certificado con indicación del alcance.pdf

h) El distintivo deberá colocarse en el producto o en su placa informativa. Además, deberá colocarse en el embalaje, si existe, y en la documentación que le acompañe. En productos «software», se mostrará el distintivo donde se haga referencia a la versión particular del producto.

i) El distintivo deberá colocarse de forma visible, legible e indeleble.

j) Se incluirá un elemento destinado a informar al usuario sobre el alcance de la certificación (norma y nivel aplicados en la evaluación).

