



Esquema de evaluación y certificación de la seguridad de las tecnologías de información

Consideraciones generales para la
certificación LINCE

24/10/2019

Versión 1.0

IT-011

Documento del esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información.

Copia no controlada en soporte papel.

Índice

1	OBJETO	4
2	RESTRICCIÓN DE USO DE LA METODOLOGÍA LINCE	5
3	PROCESO DE CUALIFICACIÓN Y CERTIFICACIÓN LINCE	6
3.1	Solicitud de Cualificación	8
3.2	Solicitud de Certificación.....	8
3.3	Fase de evaluación.....	9
3.4	Fase de cualificación.....	9
4	EMISIÓN Y TRATAMIENTO DE INFORMES DE OBSERVACIÓN (ORS)	10
5	TRATAMIENTO DE NO CONFORMIDADES Y PLAZO MÁXIMO DE LA FASE DE EVALUACIÓN	11
6	PROCEDIMIENTO PARA AUTORIZACIÓN DE RE-EVALUACIÓN DE UN PRODUCTO	12
7	PLANIFICACIÓN DE TAREAS DE EVALUACIÓN EN PARALELO	14
8	VALIDACIÓN DE LAS GUÍAS DE OPERACIÓN Y CONFIGURACIÓN SEGURA.....	15

1 Objeto

La presente Instrucción Técnica tiene por objeto aclarar algunos puntos procedimentales y técnicos relacionados con los procesos de certificación LINCE en el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

2 Restricción de uso de la metodología LINCE

Por el momento, la metodología LINCE puede ser empleada exclusivamente para la cualificación de productos para el CPSTIC (Catálogo de Productos de Seguridad TIC) conforme a las guías CCN-STIC-106 y CCN-STIC-140.

Por todo ello, la metodología LINCE puede emplearse para realizar:

- Certificaciones LINCE que permitirán la inclusión de productos en el CPSTIC para su uso en sistemas de categoría media del Esquema Nacional de Seguridad (ENS).
- Evaluaciones STIC complementarias a las certificaciones Common Criteria para productos que optan a su inclusión en el CPSTIC para sistemas de categoría alta del ENS.

3 Proceso de cualificación y certificación LINCE

Teniendo en cuenta el apartado anterior, para que el Organismo de Certificación del CCN (OC) tramite una certificación LINCE o evaluación STIC complementaria, será necesario que el solicitante previamente haya solicitado la cualificación del producto para su inclusión en el CPSTIC (Catálogo de productos de seguridad TIC).

Como parte de la valoración de la idoneidad de un producto para su inclusión en el CPSTIC el Departamento de Productos y Tecnologías del CCN (CCN-PYTEC) debe verificar el cumplimiento de las características de seguridad especificadas en la declaración de seguridad del producto candidato contra los requisitos marcados para la familia de productos definidos en la CCN-STIC-140, por lo que será necesaria la revisión de la declaración de seguridad del producto para su inclusión en el CPSTIC por parte de CCN-PYTEC.

Por lo tanto, el procedimiento de certificación del producto contra la metodología LINCE, sólo podrá comenzarse si, CCN-PYTEC requiere una certificación LINCE o evaluación STIC complementaria al solicitante y éste cuenta con el visto bueno de la declaración de seguridad por parte de CCN-PYTEC.

Si en el transcurso de la evaluación, el solicitante quisiera modificar la declaración de seguridad, esta modificación deberá ser autorizada previamente por CCN-PYTEC, antes de que sea considerada por el laboratorio como evidencia de evaluación.

El procedimiento de cualificación y certificación LINCE se resume en el siguiente gráfico:

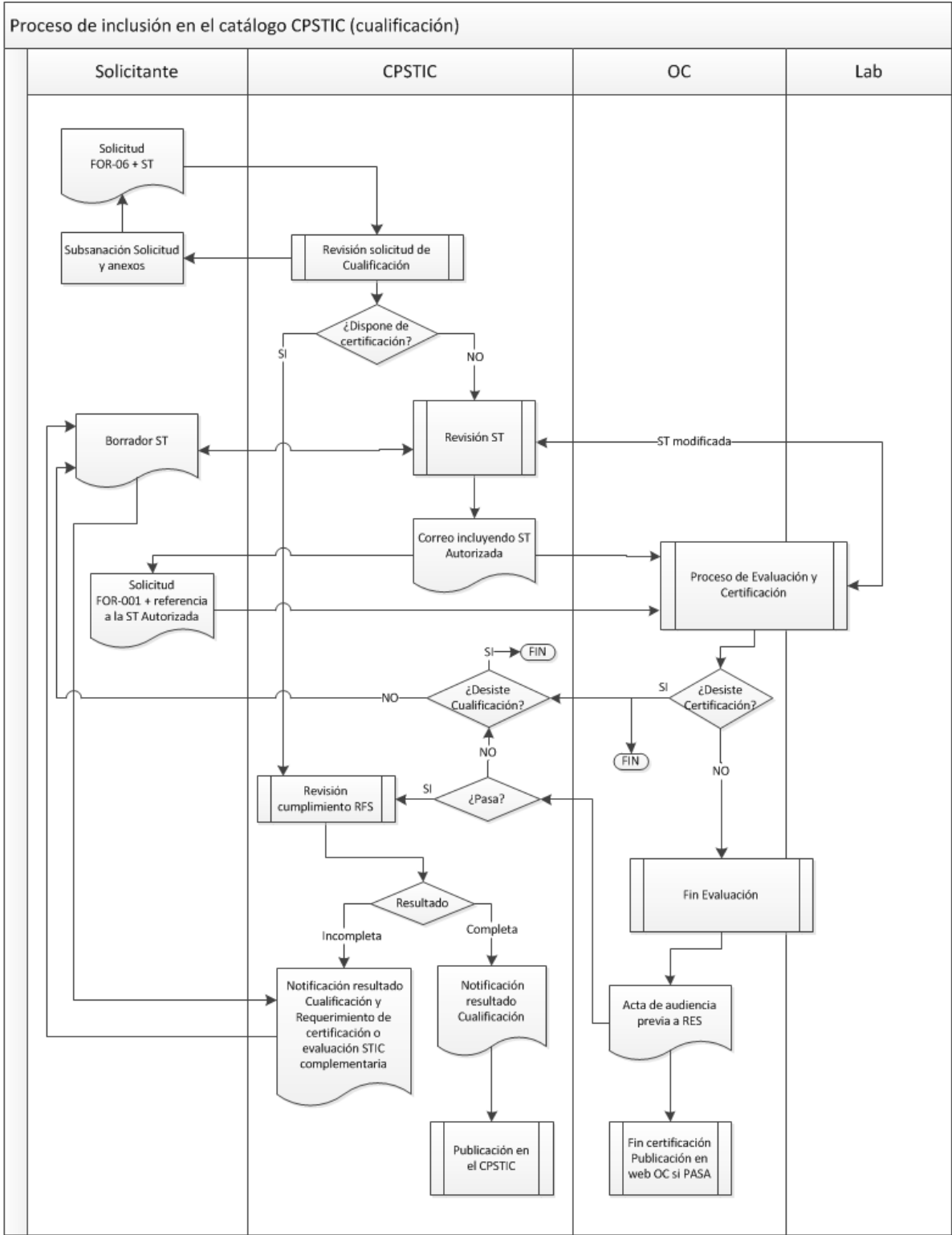


Ilustración 1 - Procedimientos de cualificación y certificación

3.1 Solicitud de Cualificación

El solicitante, previamente a solicitar la certificación LINCE de un producto o evaluación STIC complementaria, solicitará la cualificación¹ siguiendo los procedimientos marcados por la CCN-STIC-106 y los procedimientos PO-005 y PO-009, mediante la remisión del formulario FOR-006 y una declaración de seguridad conforme a los requisitos marcados en la CCN-STIC-140.

Si CCN-PYTEC, después de la valoración de la solicitud de cualificación y la declaración de seguridad considera necesaria una certificación LINCE o una evaluación STIC complementaria, notificará al solicitante de este hecho. El solicitante elaborará las evidencias necesarias para la certificación LINCE (declaración de seguridad y/o guías de operación y configuración), que presentará para su valoración a CCN-PYTEC. En caso de que CCN-PYTEC dé su visto bueno, notificará la autorización de la declaración de seguridad al solicitante enviado la declaración de seguridad autorizada y proporcionará la versión aprobada al Organismo de Certificación. El solicitante proporcionará la declaración de seguridad autorizada al laboratorio evaluador para planificar su plan de evaluación.

CCN-PYTEC, en la valoración de la declaración de seguridad, prestará especial atención a:

- El problema de seguridad definido en la Declaración de Seguridad. Las hipótesis, políticas de seguridad y amenazas deben ser acordes al caso de uso declarados para las familias de productos declaradas en la CCN-STIC-140.
- La funcionalidad de seguridad declarada en la ST refleje exactamente los Requisitos Fundamentales de Seguridad definidos para las familias de productos declaradas en la CCN-STIC-140. En esta revisión no se entrará a valorar la implementación específica que haga el fabricante de los RFS, siendo este punto objeto de evaluación por parte del laboratorio.

3.2 Solicitud de Certificación

En el caso de ser necesaria la certificación o evaluación STIC complementaria, el solicitante hará una solicitud de certificación² mediante el formulario FOR-001. La declaración de seguridad referenciada en la solicitud de certificación deberá ser la misma que haya aprobado CCN-PYTEC y que habrá remitido al Organismo de Certificación. En este caso concreto el solicitante no es necesario que envíe la declaración de seguridad al Organismo de Certificación, ya que será recibida por el OC por parte de CCN-PYTEC.

El OC, conforme al procedimiento PO-005, valorará la solicitud de certificación y en su caso autorizará y notificará al solicitante el comienzo del proceso administrativo de certificación LINCE o evaluación STIC complementaria.

El Organismo de Certificación, solicitará subsanación y en su caso desestimar la certificación, si la versión de la declaración de seguridad referenciada en el FOR-001 no se corresponde a la versión aprobada y remitida por CCN-PYTEC.

¹ Solicitará la cualificación a la dirección de correo electrónico: cpstic.ccn@cni.es

² Solicitará la certificación a la dirección de correo electrónico: organismo.certificacion@ccn.cni.es

3.3 Fase de evaluación

La evaluación y certificación LINCE o evaluación STIC complementaria se realizará conforme al procedimiento de certificación PO-005.

Como excepción al procedimiento citado, el OC notificará a los laboratorios en la reunión de comienzo de evaluación la obligatoriedad de notificar al OC de las posibles modificaciones sobre la declaración de seguridad aprobada por CCN-PYTEC. En el caso de que se produzcan modificaciones en esta evidencia, el laboratorio informará al OC de este hecho y el OC notificará a CCN-PYTEC para que proceda a analizar la nueva declaración de seguridad y en su caso proceda a su autorización. El laboratorio no deberá tener en cuenta la declaración de seguridad modificada en la evaluación hasta que se notifique la autorización de la versión por parte de CCN-PYTEC.

3.4 Fase de cualificación

Una vez que el Organismo de Certificación valide el Informe Técnico de Evaluación, se convocará al solicitante y al laboratorio a la reunión de audiencia previa a la resolución, tal y como marca el PO-005, de forma que el proceso de evaluación finalizará formalmente en esta reunión. Una vez que se produzca esta reunión, el Organismo de Certificación, notificará a CCN-PYTEC de la finalización del proceso de evaluación y sobre el sentido de la resolución de certificación (estimatoria o desestimatoria) mediante el envío del acta de audiencia previa a la resolución.

En el caso de que la resolución sea estimatoria, CCN-PYTEC procederá a continuar con el procedimiento de inclusión en el CPSTIC, evitando de esta forma las demoras relacionadas con los trámites administrativos de la certificación.

4 Emisión y tratamiento de Informes de Observación (ORs)

Teniendo en cuenta las restricciones temporales y de esfuerzo definidas en la metodología de evaluación CCN-LINCE-002, se debe establecer un procedimiento para la gestión de la emisión y tratamiento de los Informes de Observación (ORs)³ emitidos por los laboratorios.

El procedimiento de gestión de ORs en las certificaciones LINCE, debe tener en cuenta las restricciones de carga de trabajo del laboratorio y el plazo temporal máximo establecido en la metodología, por lo tanto, el tratamiento de las ORs por el solicitante no debe interferir con estos requisitos de la metodología.

Teniendo en cuenta lo anterior, el laboratorio no admitirá el tratamiento de las ORs por el solicitante, salvo que se dé una situación en que la observación pueda ser solventada en un plazo de tiempo que no afecte a la carga de trabajo máxima planificada y al tiempo máximo de evaluación fijado. Se recuerda que el solicitante puede solicitar al Organismo de Certificación el desistimiento de la evaluación en cualquier momento al ser un procedimiento administrativo común.

En el caso en el que el laboratorio deba emitir una OR, lo hará siempre informando a la vez al solicitante y al Organismo de Certificación del CCN (OC). Se espera que el laboratorio consensue con el solicitante los plazos para el tratamiento de la OR, siempre teniendo en cuenta la carga de trabajo y plazos máximos de la certificación LINCE.

Se espera que el laboratorio suspenda las actividades de evaluación que se vean afectadas por la OR que va a ser tratada por el solicitante, de forma que no se consuman recursos de manera innecesaria hasta que no se reciba la propuesta de tratamiento de la OR por parte del solicitante. Así mismo, el laboratorio debe estar dispuesto a ajustar su planificación conforme a los límites máximos establecidos intentando proporcionar el tiempo necesario para poder solventar el mayor número de ORs durante el período máximo de evaluación.

En todo caso, la valoración de la consideración del tratamiento de la OR será realizada por el laboratorio conforme a su plan de evaluación y consensuada con el OC. El laboratorio justificará al OC que la posible solución no afecta al plazo máximo de evaluación o carga planificada, por lo que junto la descripción del tratamiento de la OR deberá enviar una justificación del plazo de resolución previsto por el solicitante y una replanificación de la evaluación que tenga en cuenta el impacto a la evaluación del tratamiento de la OR por parte del solicitante.

A modo de resumen, aunque la planificación de la evaluación sea menor al tiempo máximo de la evaluación (8 semanas), en caso de aparecer ORs, el solicitante podría dilatar el tiempo total al máximo marcado por la metodología de evaluación (8 semanas más 2 semanas por módulo opcional declarado) con el fin de poder disponer de tiempo extra para solventar estas ORs. Todo esto, teniendo en cuenta el esfuerzo previo realizado por el laboratorio, la planificación de las ORs y el esfuerzo total limitado a realizar por el laboratorio (25 jornadas + 5 jornadas por módulo opcional declarado en la ST).

³ La emisión de un Informe de Observación (ORs) por parte de un laboratorio se motivará por el incumplimiento de TOE con respecto a los requisitos marcados por la metodología de evaluación.

5 Tratamiento de no conformidades y plazo máximo de la fase de evaluación

Si, como consecuencia de la validación del informe técnico de evaluación por parte del Organismo de Certificación, se detecta alguna desviación en el cumplimiento de la norma por parte del laboratorio que impactase al TOE o evidencias de evaluación responsabilidad del solicitante, el laboratorio deberá emitir la OR correspondiente y realizar su tratamiento de forma adecuada dentro del proceso de evaluación.

El esfuerzo correspondiente a este caso no será computado como parte del esfuerzo de la evaluación y el laboratorio deberá realizar el esfuerzo necesario para solventar la no conformidad u observación emitida por el Organismo de Certificación, siempre teniendo en cuenta que el plazo máximo para la entrega de la versión corregida del nuevo informe técnico de evaluación no debe superar 15 días naturales desde la fecha de validación, de forma que si no se cumple este plazo se convocará la reunión de audiencia previa a la resolución, y el laboratorio deberá tratar las desviaciones detectadas dentro de su plan de calidad y serán objeto de revisión en las auditorías de seguimiento de la acreditación.

Por lo tanto, la duración máxima de la fase de evaluación de un expediente serán 8 semanas (más dos semanas por módulo opcional declarado), a los que se añadirán 15 días naturales en caso de existir no conformidades en la validación, junto con el tiempo de validación del Organismo de Certificación, que no debería exceder de un mes desde la entrega del ETR, es decir, aproximadamente 14 semanas sin contar con las semanas adicionales por la adición de módulos opcionales.

6 Procedimiento para autorización de re-evaluación de un producto

Puede darse el caso de que el TOE, al finalizar el plazo máximo de evaluación establecido no cumpla con todos los requisitos marcados en su declaración de seguridad, por lo tanto, el laboratorio, cumpliendo con la metodología LINCE, asignará el veredicto FALLA a la evaluación, por lo que el Organismo de Certificación del CCN deberá proceder a la resolución desestimatoria del expediente de Certificación.

El ENECSTI es sensible a los esfuerzos que suponen los procesos de certificación por parte de los solicitantes, por lo que considera necesario establecer un procedimiento de re-utilización de los resultados de las actividades de evaluación de procesos de certificación que han resultado desestimados.

El proceso de re-evaluación de un producto es de aplicación a aquellos productos que, habiendo pasado un primer proceso de certificación LINCE, han resultado desestimados después de la reunión de audiencia previa y siempre y cuando no hayan transcurrido más de seis meses desde la reunión de audiencia previa a la resolución.

En estos casos, el Organismo de Certificación, podrá aceptar un nuevo procedimiento de certificación conforme al procedimiento PO-005 en el que se autorice al laboratorio encargado de la evaluación inicial la reutilización de los resultados de la evaluación previa y podrá autorizar un esfuerzo inferior para las nuevas actividades de evaluación al marcado en la metodología LINCE en el caso de que sea justificado por los cambios introducidos por el fabricante en el TOE.

Se debe aclarar, que no se admitirá la reutilización de actividades o re-evaluación del TOE, si no se produce el final formal de la evaluación, es decir si no se llega a la convocatoria de la audiencia previa a la resolución, en la que el OC informará al solicitante sobre el resultado de su validación y el sentido de la resolución del expediente de certificación.

El proceso de re-evaluación LINCE comenzará con el proceso habitual de solicitud de certificación LINCE, en el que se añade la entrega de una evidencia adicional que se denomina Informe de Análisis de Impacto. En este informe el solicitante debe informar al Organismo de Certificación sobre los cambios introducidos en el TOE con respecto al TOE empleado en la certificación original desestimada. Se espera que este informe sea lo suficientemente detallado, de forma que tanto el Organismo de Certificación como el laboratorio evaluador, puedan estimar los esfuerzos necesarios para realizar la nueva evaluación y puedan estimar el nivel de pruebas de regresión que se deben ejecutar en el transcurso de la nueva evaluación. El contenido mínimo necesario de este informe será:

- Identificación del TOE
- Referencia al expediente de certificación original.
- Descripción general de los cambios
- Listado de evidencias del solicitante afectadas por los cambios
- Descripción de los cambios introducidos en las evidencias
- Conclusiones y estimación del impacto

Una vez que se analicen los cambios, el OC los tendrá en cuenta para analizar el nuevo plan de evaluación que remita el laboratorio en la solicitud de comienzo de evaluación conforme al PO-005.

En este nuevo plan de evaluación el laboratorio debe justificar conforme al Informe de Análisis de Impacto presentado por el solicitante, las actividades de evaluación que planea reutilizar y aquellas que considera necesaria aplicar una regresión. Teniendo en cuenta las justificaciones proporcionadas por el laboratorio, y atendiendo al Informe de Análisis de Impacto, el Organismo de Certificación podrá autorizar nuevas actividades de evaluación LINCE con una carga de esfuerzo menor a las 25 jornadas/evaluador marcadas por la metodología LINCE, y por lo tanto autorizar la reutilización de las actividades previas. En todo caso, el esfuerzo máximo serán 25 jornadas/evaluador + 5 jornadas/evaluador por módulo opcional declarado en la ST, teniendo en cuenta las actividades re-utilizadas del expediente anterior y las nuevas actividades de evaluación planificadas.

Si tras el transcurso de la evaluación, el laboratorio verifica que las propiedades de seguridad establecidas en la Declaración de Seguridad se cumplen conforme a la metodología LINCE, el Organismo de Certificación podrá proponer una resolución estimatoria del expediente de certificación que culmine con la emisión del certificado LINCE para el TOE solicitado.

Los casos de renovación, re-certificación y mantenimiento será realizados conforme a lo establecido en el PO-005, la IT-002 y el documento de apoyo *Assurance Continuity: CCRA requirements*, que se consideran de aplicación a las evaluaciones LINCE.

7 Planificación de tareas de evaluación en paralelo

La metodología de evaluación CCN-LINCE-002, establece una carga de trabajo de 25 jornadas laborables de una persona en un plazo máximo de dos meses, añadiendo 5 jornadas de una persona por cada módulo opcional declarado.

El laboratorio, en su plan de evaluación y previa justificación, podrá proponer la ejecución de etapas, actividades o pruebas de evaluación en paralelo por varios evaluadores. La justificación proporcionada deberá basarse en la independencia de estas actividades con otras y que los evaluadores han adquirido el conocimiento necesario del TOE para su ejecución. El Organismo de Certificación del CCN en el acta de la reunión de comienzo de evaluación podrá autorizar este punto en base a las justificaciones proporcionadas y el plan de evaluación proporcionado.

En todo caso, la ejecución de tareas de evaluación en paralelo computará en base a los esfuerzos dedicados por cada una de las personas que estén ejecutando esta tarea de forma que, si se emplean dos evaluadores en una jornada, el cómputo de esfuerzo para el plan de evaluación será de 2 jornadas.

En el que caso que se autorice la ejecución de tareas en paralelo, el laboratorio tiene que ser consciente que el solicitante tiene derecho a que la evaluación se ejecute en un plazo máximo de dos meses, por lo que el laboratorio deberá tener en cuenta en todo caso que el solicitante puede decidir tratar ORs en ese plazo, si no se ha superado el esfuerzo máximo en el momento de la emisión de la OR.

8 Validación de las guías de operación y configuración segura

Las guías de operación y configuración segura evaluadas conforme a la metodología LINCE establecen las condiciones bajo las cuales se desarrollará la evaluación del TOE. Puede darse el caso de que un producto o su entorno operacional pueda ser configurado de diferentes maneras y en base a esta configuración se puedan ver afectadas las propiedades de seguridad del producto.

Se debe tener en cuenta que la certificación LINCE cubre exclusivamente las configuraciones detalladas en las versiones de las guías de operación y uso seguro declaradas en la declaración de seguridad y, por lo tanto, cualquier modificación sobre estas configuraciones supone que el producto no se encuentra en su configuración evaluada y por lo tanto no estará cubierto por el certificado emitido por el Organismo de Certificación.

Teniendo en cuenta que las certificaciones LINCE son de uso exclusivo como requisito de entrada para el CPSTIC, se debe tener en cuenta que las guías de evaluación proporcionadas durante el transcurso de la evaluación deben cumplir con todos los requisitos marcados en los Requisitos Fundamentales de Seguridad definidos para la familia de productos en la CCN-STIC-140.

Relacionado con este punto se redefine⁴ el término TOE en la metodología CCN-LINCE-002 para que sea tenido en cuenta por los laboratorios en su actividad de evaluación:

- Objeto a evaluar (TOE): producto o partes de un producto que se someten a una evaluación de seguridad conforme a la configuración o configuraciones definidas en las guías de operación e instalación seguras referenciadas en su declaración de seguridad.

⁴ Esta definición será incorporada a la siguiente versión de la metodología que se publique.