PROCEDIMIENTO GENERAL
DE CERTIFICACIÓN
PARA EL ESQUEMA NACIONAL DE SEGURIDAD
(ENS)

Fecha	*Motivo de la modificación*
18/09/17	Creación del documento
19/11/18	Aclaración del proceso de toma de decisiones y cierre de no conformidades, mejora de la redacción del apartado 6.2, aclaración de la documentación a analizar en la planificación, erratas menores y repaginado
10/01/20	Introducción legislación protección y privacidad de los datos y Resolución de 27 de marzo de 2018 de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información y guía CCN con criterios adicionales de auditorías y certificación.
19/02/20	Revisión proceso de apelaciones
17/11/20	Adecuación a la Guía CCN CERT IC-01/19 de criterios adicionales de auditorías y certificación (agosto 2020 (PAC, Clasificación NC Mayores y Menores, obligatoriedad del uso de las Guías CCN-STIC, detalle del alcance de la certificación, auditorías en modalidad remota, uso de servicios compartidos, concesión certificación y uso de certificaciones y distintivos de conformidad)
01/10/21	Revisión por cambio de estructura de Cámara Certifica. Inclusión apartado de confidencialidad y adecuación Guía CCN CERT IC-01/19 de criterios adicionales de auditorías y certificación (mayo 2021) (PAC)
06/07/22	Revisión de legislación que afecta al ENS.
17/10/22	Revisión por nuevo ENS (RD 311/2022), nueva versión CCN CERT IC-01/19 (marzo 2022) y del CCN-STIC 809 (octubre)

Preparado por: Pablo Sotres **Firma/ Fecha: 13/10/2022**	**Aprobado por: Maite Muñoz** **Firma/Fecha: 17/10/2022**	**Rev. nº: 7** **Fecha:**
		Copia nº:17/10/2022

INDICE

1. OBJETO Y ÁMBITO DE APLICACIÓN

La finalidad del Esquema Nacional de Seguridad (ENS) es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para la garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Según establece el Real Decreto (RD) 3/2010 el objeto último de la seguridad de la información es asegurar que una organización administrativa pueda cumplir sus objetivos utilizando sistemas de información, que deberán tener en cuenta los principios básicos de: seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica y función diferenciada. Estos principios básicos son reescritos por el Real Decreto (RD) 311/2022 quedando: a)Seguridad como proceso integral; b) Gestión de la seguridad basada en los riesgos; c) Prevención, detección, respuesta y conservación; d) Existencia de líneas de defensa; e) Vigilancia continua; f) Reevaluación periódica y g) Diferenciación de responsabilidades.

Los artículos nº 34 del RD 3/2010 y nº 31 del RD 311/2022 establecen, que los sistemas de información a los que se refiere el RD deben ser objeto de una auditoría regular ordinaria, al menos cada 2 años, que verifique el cumplimiento de los requisitos del ENS. Con carácter extraordinario deberá hacerse dicha auditoría cuando se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas.

Los citados artículos especifican que la auditoría, en el caso del Real Decreto (RD) 3/2010 se realizará en función de la categoría del sistema, determinada según lo dispuesto en el anexo I y de acuerdo con lo previsto en el anexo III y para el Real Decreto (RD) 311/2022 se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información .

Este procedimiento describe el sistema implantado por Cámara Certifica para llevar a cabo la certificación del Esquema Nacional de Seguridad (ENS) según uno de los siguientes Reales Decretos:

- RD 3/2010 (de acuerdo con los siguientes contenidos legales: Artículo 34 y Anexo III del Real Decreto 3/2010, de 8 de enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica) y
- RD 311/2022 (Artículo 31).
  Nota: RD 3/2010 y RD 951/2015 se entienden implícitamente derogados por el RD 311/2022 (fecha de derogación 5/5/2022) y teniendo en cuenta la disposición transitoria única del RD 311/2022 con respecto a la validez de los certificados emitidos contra RD 3/2010.

El presente procedimiento se aplica a las certificaciones otorgadas por Cámara Certifica según RD 3/2010 y RD 311/2022, tras las auditorias para los sistemas de categoría Básica, Media o Alta.

Los requisitos contenidos en este procedimiento tienen carácter contractual entre Cámara Certifica y las organizaciones solicitantes de las certificaciones mencionadas y según el Real Decreto del que se trate.

2. DOCUMENTOS DE REFERENCIA

El presente documento se ha elaborado siguiendo las directrices del Manual de la Calidad de Cámara Certifica, basándose en los criterios establecidos en los siguientes documentos:

- Norma UNE EN ISO/IEC 17065 "Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios".
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 951/2015, de 23 de octubre, de modificación del RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Resolución 13/10/2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 11/2007, de 22 junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Guías CCN-STIC – Serie 800
- MC Manual de la Calidad.
- PG-CC-ENS-33. Procedimiento específico de certificación de ENS
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/ce (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- CCN-CERT IC-01/19 Criterios adicionales de Auditoría y Certificación

3. TERMINOLOGÍA

Para el propósito de este documento son de aplicación las definiciones recogidas en los documentos de referencia anteriormente citados y las incluidas en los siguientes documentos:

- UNE-EN ISO/IEC 17000. Evaluación de la conformidad. Vocabulario y principios generales.
- Guía de seguridad (CCN-STIC-800) Esquema Nacional de Seguridad glosario de términos y abreviaturas

Adicionalmente, se incluyen las siguientes definiciones:

Auditoría de sistemas de información

La Auditoría de sistemas de información es el proceso metodológico, realizado con independencia de los elementos auditados y con objetividad, de recoger, agrupar y evaluar evidencias para determinar si los sistemas o tecnologías de la información salvaguardan los activos, mantienen la integridad de los datos, contribuyen al logro de los fines de la organización y utilizan eficientemente los recursos.

Auditoría ordinaria:

Aplicable al RD 3/2010: auditoria requerida para dar cumplimiento a lo establecido en el artículo 34 y en el Anexo III, y por lo tanto, verificar el cumplimiento de los requisitos establecidos por el RD 3/2010 en los capítulos II y III y en los Anexos I y II.

Aplicable al RD 311/2022: auditoria requerida para dar cumplimiento a lo establecido en el artículo 31, realizada en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

Su objetivo final es sustentar la confianza que merece el sistema auditado en materia de seguridad; es decir, calibrar su capacidad para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida.

Se consideran auditorías ordinarias las iniciales para la obtención de la certificación y las renovaciones para su mantenimiento.

Auditoria extraordinaria: Aquella que se realiza como consecuencia de la detección de fallos de seguridad en el sistema que ponen en riesgo la información contenida en el mismo o siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas.

Las desviaciones detectadas se clasificarán como:

No conformidad menor: ausencia o fallo en la implantación o mantenimiento de uno o más de los requisitos del ENS, incluyendo cualquier situación que pudiese, en base a una evidencia objetiva, sustentar una duda significativa sobre la conformidad del sistema de información con uno o más de tales requisitos. En concreto:

- Ante un incumplimiento parcial de algún artículo del Real Decreto del Esquema Nacional de Seguridad que sea objeto de auditoría y/o el incumplimiento parcial de alguna

medida/control (o algún requisito de alguna medida/control) del ANEXO II en función de la categorización del sistema.

- Cuando, sin afectar a la capacidad del sistema de protección para lograr los resultados previstos; los requisitos se satisfacen de forma manifiestamente mejorable o se aprecian incoherencias entre requisitos que deberían estar alineados.

No Conformidad Mayor:

- Ante un incumplimiento de algún artículo del Real Decreto del Esquema Nacional de Seguridad que sea objeto de auditoría y/o el incumplimiento total de un conjunto de medidas/controles pertenecientes a un dominio del Anexo II, en función de la categorización del sistema.
- Cuando existen incumplimientos de carácter legal relacionados con la seguridad de la información.
- Cuando la desviación afecta significativamente a la capacidad del sistema de información para atender sus funciones esenciales.
- Cuando exista una duda razonable de que se haya implementado un control eficaz de proceso, o de que las medidas de seguridad cumplan los requisitos especificados.
- Cuando se evidencie un número significativo de no conformidades menores asociadas al mismo requisito.
- Cuando el número de no conformidades menores detectadas impidan deducir la adecuación del sistema a los principios básicos y requisitos mínimos del Esquema Nacional de Seguridad.
- Cuando se detecte un uso inadecuado de la marca de empresa certificada (distintivo y certificado)

Observación: Evidencias de, una debilidad, una vulnerabilidad o una situación que, sin comprometer cualquier área del sistema definido en el ENS o por la organización, pueda, en la actualidad o en el futuro, derivar en un problema.

Oportunidad de Mejora: Aspectos que, a juicio del auditor, aporten valor a la auditoría y puedan contribuir a la mejora del marco de gestión de seguridad de los sistemas de información concernidos.

En relación con la obligatoriedad del uso de las Guías CCN-STIC, éstas deben considerarse como "Mejores Prácticas", que pueden ser consideradas por los operadores jurídicos en materias de carácter preferentemente dispositivo y que incluye recomendaciones, principios, etc., que podrían influir en el desarrollo legislativo pudiendo asimismo ser utilizadas como referentes específicos en la actuación judicial o arbitral. Aun no tratándose exactamente de normas imperativas, su cumplimiento no resulta obligatorio, aunque su inobservancia, caso de producirse algún incidente que pueda poner en riesgo la seguridad de los sistemas de información concernidos, podría derivar en responsabilidad. Por lo tanto, la inadecuación total o parcial del sistema de información evaluado a lo dispuesto en la Guía CCN-STIC que resultare de aplicación en cada caso (https://www.ccn.cni.es/index.php/es/menu-guias-ccn-stic-es), podría ser calificada por el Equipo Auditor como una Observación, No Conformidad Menor o No

Conformidad Mayor, atendiendo al impacto que su incumplimiento pudiera tener en la seguridad de dicho sistema de información.

Para la clasificación de los sistemas de los sistemas que soportan el ENS se considera:

- Categoría de un sistema de seguridad. Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema de seguridad a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

Por su aplicación se consideran la categoría del sistema de seguridad:

- Básica: si alguna de las dimensiones de seguridad alcanza el nivel bajo y ninguna alcanza el nivel superior.

- Media: si alguna de sus dimensiones de seguridad alcanza el nivel medio y ninguna alcanza el nivel superior

- Alta: si alguna de sus dimensiones de seguridad alcanza el nivel alto.

Para el establecimiento de la categoría del sistema, se tendrán en cuenta las siguientes dimensiones de seguridad:

a) Disponibilidad [D]. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren
El nivel de seguridad requerido en el aspecto de disponibilidad se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera acceder a la información cuando la necesita.

b) Autenticidad [A]. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

   El nivel de seguridad requerido en el aspecto de autenticidad se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.

c) Integridad [I]. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

   El nivel de seguridad requerido en el aspecto de integridad se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.

d) Confidencialidad [C]. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

   El nivel de seguridad requerido en el aspecto de confidencialidad se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.

e) Trazabilidad [T]. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad:

El nivel de seguridad requerido en el aspecto de trazabilidad se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido a o modificado una cierta información.

4. ALCANCE DE LA CERTIFICACIÓN

El alcance de la certificación, que será reflejado en el correspondiente certificado y en la oferta/contrato de certificación, hará referencia a:

a. Determinación precisa de los sistemas de información comprendidos en la misma y los servicios prestados por medio de tales sistemas. Tanto unos (los sistemas de información) como los otros (los servicios sustentados en dichos sistemas) deberán aparecer explícitamente mencionados en el Certificado de Conformidad con el ENS.

b. Cuando el alcance de la Certificación de Conformidad con el ENS comprenda sistemas de información utilizados para la prestación de servicios comercializados bajo signos distintivos (marcas y nombres comerciales), la denominación de tales signos deberá figurar, explícitamente, en la Certificación de Conformidad.

c. La organización que haya sido certificada, con indicación de la ubicación geográfica de los centros de trabajo en los que se aplica el sistema que soporta el Esquema Nacional de Seguridad (ENS).

d. Las actividades desarrolladas en cada uno de sus centros de trabajo y que están cubiertas por el sistema que soporta el ENS.

e. Los documentos normativos frente a los cuales se declara conformidad del sistema que soporta el ENS.

En función del objetivo de la certificación, el alcance se adecuará a una de las siguientes tipologías:

- Certificación de conformidad con el ENS de categoría básica
- Certificación de conformidad con el ENS de categoría media
- Certificación de conformidad con el ENS de categoría alta.

5. CRITERIOS DE CERTIFICACIÓN

Las actividades de certificación en el esquema ENS por Cámara Certifica están abiertas a cualquier solicitante (público o privado), por lo que podrán solicitar la certificación todas aquellas empresas o particulares que lo deseen, cuyas actividades estén dentro del alcance de las operaciones de Cámara Certifica, independientemente de su tamaño, sector, campo de

actividad y de su pertenencia o no a determinados Grupos o Asociaciones, siempre que cumplan los requisitos definidos en los documentos normativos para la certificación en el esquema ENS.

Cámara Certifica se reserva el derecho de declinar la aceptación de una solicitud de certificación ENS si existen razones fundamentadas o demostradas, tales como, la participación del cliente en actividades ilegales, incumplimiento grave reiterado de los requisitos de certificación o temas similares relacionados.

Los requisitos de aplicación, evaluación, revisión y toma de decisión en el proceso de certificación se limitarán a aquellos asuntos relacionados específicamente con el alcance de certificación.

El proceso de certificación se estructura en ciclos que comenzará con la concesión certificación de conformidad inicial. Con carácter bienal se realizarán auditorias de renovación de la certificación de conformidad, cuyo objetivo será verificar el mantenimiento de la certificación otorgada. Deberá hacerse auditoria extraordinaria cuando se produzcan modificaciones sustanciales en el sistema de información. Tras esta auditoria extraordinaria se iniciará un ciclo bienal.

Los requisitos para obtener la certificación en el esquema ENS no son otros que haber superado el proceso de certificación descrito en el apartado 6 “Proceso de Certificación” y, en su caso, haber planteado acciones correctivas adecuadas a las desviaciones detectadas durante las evaluaciones, de forma que se asegure el cumplimiento de los requisitos descritos en los documentos normativos (bien RD 3/2010, de 8 de enero, y en el Real Decreto 951/2015, de 23 de octubre, de modificación del RD 3/2010 o RD 311/2022, según aplique).

Con la entrada en vigor del RD 311/2022, cualquier certificado emitido contra el RD 3/2010 tendrá como fecha máxima de validez el 5 de mayo de 2024. Vencida esta fecha, el certificado dejará de tener validez.

Cualquier cambio en los requisitos de certificación será comunicado por escrito a las empresas, detallando el periodo de adaptación decidido, así como la forma en que el Cámara Certifica evaluará los nuevos requisitos.

La entidad solicitante de la certificación deberá comprometerse a cumplir con los plazos establecidos en las distintas fases del proceso de certificación, así como, con las obligaciones descritas en el presente procedimiento y contrato de certificación. Cualquier cambio sustancial que afecte al sistema certificado deberá notificarse a Cámara Certifica.

5.1 Gestión de la Imparcialidad

Las actividades de certificación desarrolladas por Cámara Certifica se realizarán con total imparcialidad, reconociendo su importancia mediante una declaración accesible a las organizaciones certificadas, por la cual se constata su importancia en la realización de sus actividades, se gestionan los conflictos de interés y se asegura la objetividad en sus actividades,

de conformidad con lo exigido en la ITS de Auditoría, en la ITS de Conformidad con el ENS y la ISO/IEC 17065, evitando los conflictos de intereses.

Para asegurar dicha imparcialidad, Cámara Certifica ha realizado un análisis para identificar conflictos de intereses y gestionarlos de manera adecuada. Dicho análisis ha sido aprobado por el Director de Certificación y ratificado por el Comité de Partes de Cámara Certifica, cuya composición de sus miembros está a disposición de cualquier empresa u organismo interesado.

La Declaración de Imparcialidad está a disposición de las organizaciones certificadas en la página web de Cámara Certifica (http://camaracertifica.es/) y ha sido, así mismo, aprobada por el Director Gerente y ratificada por el Comité de Partes de Cámara Certifica.

6. PROCESO DE CERTIFICACIÓN

El proceso de certificación tiene un carácter bienal, de forma que cada dos años se realizará una auditoría ordinaria iniciando el ciclo de certificación con la concesión de la certificación y finalizando con la renovación de la certificación.

La primera auditoría se denomina auditoría inicial. Las sucesivas auditorías que demuestren el mantenimiento de la certificación se denominan auditorías de renovación.

A continuación, se describe un proceso completo de certificación, desde la fase de solicitud de información para la elaboración de la oferta hasta la fase final de la certificación con la toma de decisión:

6.1. Recogida de datos, elaboración de ofertas y envío inicial de Información

La organización interesada en recibir una oferta de certificación deberá facilitar al departamento comercial de Cámara Certifica información relativa, entre otros aspectos, al alcance y categoría de la certificación, características generales de la organización, aspectos significativos de sus sistemas, información relativa a todos los procesos contratados externamente, y cualquier otra información pertinente para dimensionar y planificar el proceso de auditoría.

Posteriormente a la toma de datos y una vez revisada la información facilitada por el solicitante y comprobada la capacidad y disponibilidad de Cámara Certifica para aceptar la solicitud de certificación, se remitirá al solicitante como mínimo la información siguiente:

a) Procedimiento general de certificación de sistemas de gestión (PG-CC-ENS-32)
b) Una oferta/contrato que contendrá como mínimo: referencia a la certificación en el Esquema Nacional de Seguridad, datos de identificación de la organización, número y fecha de oferta, alcance, días de auditoría, condiciones económicas, condiciones generales de certificación, vigencia de la oferta y forma de pago.

Además, proporcionará bajo petición al solicitante que lo solicite información sobre el marco normativo vigente.

6.2. Solicitud de certificación

La oferta/contrato que una vez aceptada y cumplimentada constituye la solicitud de certificación, deberá ser firmada por el representante legal[1] de la organización.

Mediante la aceptación de la oferta/contrato, la organización:

- Efectúa la demanda oficial de certificación.
- Declara que conoce las condiciones generales de certificación.
- Describe el alcance (actividades y centros de trabajo) al que es aplicable su sistema, así como la/s norma/s de referencia.
- Confirma la información aportada por la organización en su solicitud de información ("SI SG"– datos generales más anexos específicos de 27001 y ENS)

Dicha solicitud deberá enviarse a Cámara Certifica para poder elaborar la oferta de certificación.

El periodo de validez de la solicitud de certificación será de un año desde la apertura del proceso hasta el inicio de este, pasado ese periodo Cámara Certifica cancelará el expediente.

6.3. Revisión de solicitud y documentación inicial

Aceptada la oferta/contrato, Cámara Certifica acusará recibo de recepción, realizando la apertura del proceso correspondiente y asignando un número de expediente al sistema ENS objeto de certificación.

El Jefe Técnico de Área llevará a cabo la revisión de la solicitud con objeto de comprobar su adecuación conforme a los documentos normativos y que ésta es completa, adecuada y suficiente para desarrollar el proceso de certificación.

Previo al inicio del proceso, se habrá resuelto cualquier diferencia sobre el alcance de certificación o información aportada, entre Cámara Certifica y la organización solicitante.

De igual forma, el Jefe Técnico de Área confirmará si se dispone de los recursos humanos necesarios (auditores y expertos técnicos) para llevar a cabo la certificación solicitada, comprobación realizada previamente a la emisión de la oferta de certificación.

En caso de rechazar la solicitud de certificación se informará al solicitante de las razones de dicho rechazo.

La oferta de certificación podrá sufrir modificaciones en cuanto a días de auditoría en función de la información recabada en cada una de las fases de la evaluación.

[1] Nota: se entiende por representante legal de la organización, la persona dentro de la gerencia de la organización, facultada para tomar decisiones relativas a los recursos económicos, técnicos y administrativos de la misma con poder de firma.

6.4. Designación del equipo auditor

El Jefe Técnico de Área designará, de entre los auditores cualificados[2], un auditor jefe competente para el proceso y objetivos de la auditoría y tantos auditores y expertos como sean necesarios, en función de los sistemas de información de la organización solicitante.

Una vez designado, Cámara Certifica procederá a comunicar al solicitante con tiempo suficiente la composición del equipo auditor, indicando la procedencia de cada uno de sus miembros y permitiéndole su recusación si existieran motivos, desconocidos por la Entidad, que pudieran comprometer su imparcialidad de actuación.

Cámara Certifica pondrá a disposición de la organización cuando se le solicite por escrito, los antecedentes profesionales del equipo auditor.

Las funciones y responsabilidades, a lo largo de la auditoría, de los miembros del equipo auditor quedan recogidas en el plan de auditoría enviado a la organización previa a su realización.

6.5. Proceso de evaluación

Una vez la solicitud y la documentación presentada son completas y se ha resuelto cualquier diferencia entre Cámara Certifica y la organización solicitante, se inicia el proceso de evaluación poniéndose en contacto el auditor jefe con la organización para planificar la auditoria.

Con el propósito de agilizar y acortar en lo posible los tiempos de auditoría presencial en la entidad auditada y así para poder realizar la planificación en detalle, el Auditor Jefe debe analizar con suficiente antelación la siguiente documentación:

• Documentos firmados por el órgano superior correspondiente que muestren el conocimiento y la aprobación formal de las decisiones en materia de política de seguridad.

• Organigrama de los servicios o áreas afectadas, con descripción de funciones y responsabilidades.

• Identificación de los responsables: de la información, de los servicios, de la seguridad y del sistema.

• Descripción detallada del sistema de información a auditar (software, hardware, comunicaciones, equipamiento auxiliar, ubicaciones y similares).

• Categoría del sistema según el Anexo I del ENS, incluyendo los criterios de identificación y valor de los niveles de las dimensiones de seguridad que serán de aplicación al sistema.

• En el caso de ser de aplicación, indicación de qué Perfil de Cumplimiento es el utilizado (entendido como el conjunto de medidas de seguridad, comprendidas o no en el anexo II del Real Decreto 311/2022, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el CCN).

[2] Los auditores cualificados podrán ser tanto del personal de la plantilla de Cámara Certifica como contratados externamente.
Cámara Certifica tiene implantado un programa de supervisión continua de la actuación de sus auditores con el objeto de asegurar la eficacia y homogeneidad de sus actuaciones.
La utilización de expertos no reduce el número mínimo de auditores día previstos. Así mismo, la presencia de observadores acompañando al equipo auditor no reduce el tiempo de auditoria

• Descripción detallada del sistema de gestión de la seguridad y la documentación que lo sustenta.

• La Política de Seguridad y Normativa de Seguridad.

• La Política de Firma Electrónica y Certificados (si aplica).

• Informes con el desarrollo y resultado de la apreciación del riesgo, incluyendo la identificación de escenarios de riesgo, su análisis y evaluación.

• La Declaración de Aplicabilidad.

• Decisiones adoptadas para tratar los riesgos.

• Relación de las medidas de seguridad implantadas por requisitos legales o como resultado de la apreciación del riesgo.

• Relación de registros de actividad en lo relativo a las medidas de seguridad implantadas y estado de implantación.

• Informes de otras auditorías previas de seguridad relacionados con los sistemas y servicios incluidos en el alcance de la auditoría (por ejemplo informes de la auditoría de protección de datos de carácter personal o de auditorías previas con el mismo objetivo y alcance que la auditoría a comenzar (ISO 27001, vulnerabilidades, etc...)

• Informes de seguimiento de deficiencias detectadas en auditorías previas de seguridad y relacionadas con el sistema a auditar.

• Lista de proveedores externos cuyos servicios se ven afectados o entran dentro del alcance de la auditoría, y evidencias del control realizado sobre estos servicios.

• Sistemas de métricas e indicadores necesarios para la realización del "Informe Nacional del Estado de la Seguridad" (si aplica).

• Informes de auditorías internas.

Según la disponibilidad de esta documentación, y de acuerdo con los Responsables de la Información, del Servicio, del Sistema y del Responsable de la Seguridad, el Auditor Jefe determinará si es necesario recibir una copia, o bien, según el caso, es suficiente con una presentación de esta documentación, por parte de estos responsables, durante la ejecución de la auditoría.

Una vez establecida su planificación se procederá a la ejecución de la auditoría y que, constará de tres partes:

a) Reunión Inicial: entre los representantes de la organización y el equipo auditor, durante la cual se harán las presentaciones oportunas, se confirmará el plan de la auditoría y el alcance de la misma y se describirá la sistemática a seguir, entre otros aspectos que se comunicarán en el plan de trabajo.

b) Desarrollo de la auditoría: en esta fase se procederá a la evaluación del sistema que soporta el ENS de la organización a través del estudio de la documentación, registros, pruebas y procediendo a la observación de actividades y a la entrevista del personal afectado.

c) Reunión final del equipo auditor con los representantes de la organización con objeto de presentar a los responsables de la misma de forma detallada los resultados de la

investigación, indicando cualquier desviación respecto a los requisitos de la norma de referencia de la certificación que se hubiesen puesto de manifiesto y aquellos otros aspectos indicados en el plan de trabajo. Se requerirá la presencia del responsable del sistema y del de seguridad.

A continuación, se describe el proceso de realización de una auditoría inicial:

El auditor jefe, tras haber acordado con la organización las fechas de realización de la auditoría elaborará y enviará por correo electrónico a la organización el plan de auditoria detallado con, al menos, una semana de antelación a la fecha de su realización, y en el que se incluyen, entre otros aspectos, los criterios y objetivos de la auditoría a realizar.

Este plan podrá ser reeditado si se detectan errores tras la revisión realizada por Cámara Certifica

La auditoría se desarrollará en las instalaciones del cliente y consistirá en la comprobación, revisión y evaluación de los siguientes aspectos:

- Base documental del sistema que soporta el ENS mediante el análisis de la documentación desarrollada por la organización (políticas y normativas de seguridad)

De detectarse ausencia de documentación o una falta generalizada de la información requerida considerada como crítica a juicio del equipo auditor, el auditor jefe contactará con Cámara Certifica, quien indicará si procede continuar con la fase operativa o interrumpir el proceso de certificación.

A continuación, se procederá a la evaluación del sistema de la organización, a través del estudio de la documentación, registros, y procediendo a la observación de actividades y pruebas y a la entrevista del personal afectado. El equipo auditor deberá verificar que las medidas de seguridad para el sistema auditado se ajustan a los principios básicos del RD 3/2010 (artículo 4) o si se trata de una auditoría contra el RD 311/2022 (artículo 5), y satisfacen los requisitos mínimos de seguridad (artículo 11 del RD 3/2010 o artículo 12 del RD 311/2022 según sea el marco que se esté auditando).

A modo de ejemplo, durante esta fase de auditoría se comprobarán, los siguientes aspectos:

- La información y evidencias de conformidad con todos los requisitos del RD 3/2010 o RD 311/2022 que apliquen a la organización.
- La realización de actividades de seguimiento, medición, informe y revisión con relación a los objetivos y metas de la organización y su desempeño en relación con el cumplimiento de requisitos legales, reglamentarios y contractuales aplicables.
- Aplicación de las medidas de seguridad, según categorización, del Anexo II del ENS (y, en su caso, y según recoge el RD 311/2022 del perfil de cumplimiento específico que corresponda) en grado adecuado.
- La responsabilidad de la dirección con sus políticas.

Las revisiones y pruebas de auditoría se realizarán tomando como base las recomendaciones del apartado “3.4 Evidencias de la auditoría” de la guía “CCN-STIC-802 Auditoría del ENS”.

La implantación del sistema a fecha de la auditoría debe ser la necesaria para permitir una adecuada evaluación basada en la revisión de los registros necesarios, así como en el intercambio de información con el personal de la organización.

La organización (con independencia de la realización de las preceptivas auditorías de certificación, al menos de carácter bienal). con sistemas de categorías MEDIA y ALTA deberá realizar al menos auditorías internas anuales completas para demostrar que el sistema es capaz de ir mejorando.

Las auditorías internas anuales de seguimiento de las medidas de seguridad del Anexo II del ENS -especialmente, en los años que no haya que realizar auditorías de certificación-, asegurándose de que cada auditoría de seguimiento cubre el análisis de al menos el 50% de las medidas que le apliquen del Anexo II, y de que entre las dos auditorías internas del ciclo bienal se cubre el 100% de dichas medidas, resultando especialmente de aplicación en el caso de preverse auditorías de certificación iniciales o cualesquiera otras, a realizar sobre sistemas de categoría MEDIA o ALTA dentro del principio básico de mejora continua del proceso de seguridad que requiere todo SGSI.

Como resultado de la auditoria se generará un informe que será entregado a la organización al finalizar la visita o en un plazo máximo de una semana desde el último día de la realización de la auditoria. Este informe tiene una validez de 6 meses a partir de la fecha de emisión.

Dicho informe de auditoría incluirá información relativa a:

- Grado de cumplimiento del RD 3/2010 o RD 311/2022 (según sea el texto legal seleccionado)
- La existencia de un sistema que soporte el ENS documentado y con un proceso regular de aprobación por la dirección.
- La Política de Seguridad que debe responder a la misión y objetivos de seguridad de la organización.
- La definición de los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información. Se incluirá información sobre los procedimientos para la resolución de conflictos entre dichos responsables.
- La identificación del riesgo, incluyendo la identificación de escenarios de riesgo, el análisis de las consecuencias y su probabilidad, y la evaluación de su aceptabilidad o inaceptabilidad por la organización, con su revisión y aprobación regular, según lo establecido en las medidas aplicables del Anexo II del RD 3/2010 o RD 311/2022.
- La categoría del sistema, con detalle del nivel de seguridad en cada una de las dimensiones recogidas en el ENS.
- El cumplimiento de las medidas de seguridad descritas en el Anexo II (o del perfil de cumplimiento, en su caso), en función de las condiciones de aplicación en cada caso.
- Una referencia a la versión de la Declaración de Aplicabilidad y el nivel en cada dimensión para cada medida de seguridad del ENS aplicable.
- Referencia al proceso de mejora continua de la gestión de la seguridad.
- Las áreas organizativas, módulos o funciones del sistema de información cubiertas por la auditoría, incluyendo los requisitos de certificación y las ubicaciones que fueron auditadas, las pistas de auditoría seguidas y las metodologías de auditoría utilizadas.

- Los detalles de las conformidades y no conformidades identificadas se justificarán mediante evidencias objetivas y su correspondencia con los requisitos del ENS u otros documentos requeridos para la Certificación.

El dictamen final del auditor jefe se reflejará en el informe de Auditoría y será uno de los tres siguientes:

- Favorable: Cuando no se evidencie ninguna "No Conformidad Mayor" o "No Conformidad Menor".
- Favorable con No Conformidades: Cuando se evidencien "No Conformidades menores" y/o "No Conformidades Mayores".
- Desfavorable: Cuando exista un número significativo de No Conformidades Mayores cuya solución no pueda evidenciarse a través de un Plan de Acciones Correctivas y requiere la comprobación in-situ de su correcta implantación a través de una auditoría extraordinaria

6.6. Auditorías de certificación realizadas en modo remoto

Será posible realizar inspecciones en modo remoto durante las Auditorías de Certificación del ENS (iniciales o de renovación, sobre clientes conocidos o desconocidos), usando medios telemáticos (como, por ejemplo, videoconferencia y compartición de escritorio remoto), siempre que se considere dicha actividad como viable por parte de la Entidad de Certificación y acorde con los procedimientos de auditoria establecidos, habiendo previamente analizado el riesgo derivado de evaluar telemáticamente a su cliente y poder justificarlo adecuadamente ante ENAC y el Centro Criptológico Nacional.

6.7. Utilización de servicios compartidos

En tanto los Servicios Compartidos ofrecidos por la Administración General del Estado (AGE) o, en su caso, por las Administraciones Territoriales competentes, que pudieran estar comprendidos en el alcance de la auditoría no dispongan de la preceptiva Certificación de Conformidad con el ENS, la Auditoría de Conformidad con el ENS deberá concentrarse solo en los servicios que puedan satisfacerse a través de los propios sistemas de información de la organización auditada (o en sistemas de información externos que posean la Certificación de Conformidad con el ENS o puedan ser auditados y certificados en tal sentido).

De no ser posible lo anterior, y cuando se trate de la utilización de Servicios Compartidos suministrados por la AGE o, en su caso, por las Administraciones Territoriales competentes, el alcance de la Certificación de Conformidad (y la subsiguiente Certificación de Conformidad) habrá de señalar la parte que ha sido auditada, mencionando, expresamente, que la porción no auditada (ACCEDA o GEISER, por ejemplo) no se encuentra comprendida en tal alcance.

No obstante, cuanto tales servicios compartidos logren la Certificación de Conformidad, Cámara Certifica podrá generar un nuevo Certificado de Conformidad, eliminando la precisión anterior.

6.8. Acciones correctivas/alegaciones

Tras la recepción del informe de auditoría, la organización solicitante deberá presentar a Cámara Certifica un plan detallado con las acciones correctivas.

El plan de acciones correctivas, que deberá cumplimentarse en el modelo de informe de plan de acciones correctivas aportado por el auditor, deberá contener:

- Análisis de las causas que han dado lugar a la apertura de la no conformidad.
- Acción correctiva: se deben plantear acciones que eviten que ésta u otras no conformidades similares se vuelvan a producir eliminando las causas que las originan.

En todos los casos, tanto en no conformidades mayores como menores se deberán adjuntar evidencias para que el auditor jefe verifique que las No Conformidades han sido corregidas. En caso de que la entidad auditada precise de un tiempo para la implantación de unas acciones correctivas que ataquen a la causa del problema, deberá demostrar que se han establecido acciones de remedio para el problema detectado y que el Plan de Acciones Correctivas contiene una planificación concreta de acciones precisas que, en el tiempo adecuado y razonable en función de las no conformidades detectadas y su tipificación, traten y resuelvan las causas de las desviaciones halladas.

El plazo para la presentación del plan de acciones correctivas es de 1 mes, salvo casos debidamente justificados y autorizados. Cámara Certifica se reserva el derecho de aceptar las acciones y evidencias planteadas por la organización.

Respecto del Plan de Acciones Correctivas, es necesario verificar que todas las No Conformidades se han corregido. No obstante, en caso de que la entidad auditada precise de un tiempo para la implantación de unas acciones correctivas que ataquen a la causa del problema, deberá demostrar que se han establecido acciones de remedio para el problema detectado y que el Plan de Acciones Correctivas contiene una planificación concreta de acciones precisas que, en el tiempo adecuado y razonable en función de las no conformidades detectadas y su tipificación, traten y resuelvan las causas de las desviaciones halladas.

Si la organización disiente de las desviaciones descritas, podrá presentar las alegaciones que estime oportunas, justificando los motivos por los que disiente del juicio del equipo auditor.

No podrá expedirse una Certificación de Conformidad con el ENS si existe una No Conformidad y no se ha presentado un Plan de Acciones Correctivas que trate adecuadamente tal desviación.

6.9. Proceso de toma de decisiones

A la vista del informe de la auditoría, de las acciones correctivas o alegaciones presentadas por la organización y de la confirmación de la información proporcionada para la revisión de la solicitud, el Comité de Certificación decidirá sobre la concesión de la certificación.

Cámara Certifica emitirá la Certificación de Conformidad con el ENS únicamente si el dictamen fuera “FAVORABLE” o, si habiendo sido “FAVORABLE CON NO CONFORMIDADES”, el Plan de Acciones Correctivas presentado por la entidad titular del sistema de información, trata y resuelve y corrige las desviaciones evidenciadas, a criterio de Cámara Certifica.

Ante un dictamen “DESFAVORABLE” del sistema de información auditado, la organización deberá someterse a una Auditoría Extraordinaria, exclusivamente sobre las desviaciones evidenciadas que, de resultar satisfactorio, permitirá la expedición del correspondiente Certificado de Conformidad con el ENS. Esta auditoría no podrá realizarse en un plazo superior

a seis meses desde la fecha de emisión del Informe de Auditoría, en caso contrario deberá iniciarse un proceso completo de auditoría.

7. CONCESIÓN DE LA CERTIFICACIÓN

No podrá expedirse una Certificación de conformidad con el ENS si existieran No Conformidades (Mayores o Menores) y no se hubiere presentado y evaluado satisfactoriamente el correspondiente Plan de Acciones Correctivas, que trate adecuadamente las desviaciones halladas.

En la Certificación de Conformidad expedida, es obligatorio identificar y publicar con precisión el alcance de la misma (sistema o sistemas de información afectados) y, con el mayor detalle posible, los servicios comprendidos en la Certificación. Cualquier servicio que no se encuentre explícitamente reseñado en la correspondiente Certificación de Conformidad se entenderá que no está amparado por ella.

Cuando el alcance de la Certificación de Conformidad con el ENS comprenda sistemas de información utilizados para la prestación de servicios comercializados bajo signos distintivos (marcas y nombres comerciales), la denominación de tales signos deberá figurar, explícitamente, en el Certificado de conformidad.

Con el objetivo de ofrecer la debida transparencia en el cumplimiento del ENS y del resto de regulaciones concordantes, la Certificación de Conformidad con el ENS de aquellos sistemas de información que ofrezcan Servicios en la Nube, expresarán, dentro de la mención a los servicios comprendidos en el alcance, la ubicación (ciudad, región y país) de los CPD en los que se soportan dichos servicios, junto con una mención sobre los que hayan sido objeto de evaluación directa por parte de Cámara Certifica.

Tras la decisión de certificación favorable, y previo pago de los costes correspondientes, Cámara Certifica emitirá documentos oficiales que justifiquen la concesión de la certificación ENS, que tendrá una vigencia de 2 años.

Los tipos de certificados emitidos podrán ser los siguientes:

- Certificación de Conformidad de categoría básica.
- Certificación de Conformidad de categoría media.
- Certificación de Conformidad de categoría alta.

El Certificado emitido por Cámara Certifica se expresará en un documento electrónico, en formato no editable, firmado electrónicamente y seguirá las directrices definidas en el Anexo III de la Resolución de 13 de octubre de 2016 e incluye como mínimo la siguiente información:

a) Nombre, dirección y marca de certificación de la entidad de certificación y símbolo de acreditación, cuando aplique.

b) La categoría máxima aplicable al sistema de información auditado.

c) Los datos de la organización certificada, incluida la ubicación geográfica y su condición de pública o privada.

d) Declaración de Conformidad contra el RD 3/2010, de 8 de enero o RD 311/2022, de 3 de mayo.

e) Los sistemas de información y los servicios objeto de la certificación (para más información ver apartado 4 de este documento).

f) Fecha de certificación de conformidad inicial.

g) Fecha de renovación de la certificación de conformidad. (debe entenderse como "Fecha de expiración de la certificación de conformidad").

h) Número de certificado.

i) Distintivo de Declaración de Conformidad con el Esquema Nacional de Seguridad, acorde con la categoría del sistema certificado, según Anexo IV de la Resolución de 13 de octubre de 2016 para RD 3/2010 y Anexo B de la CCN-STIC-909 para el RD 311/2022.

Con la entrada en vigor del RD 311/2022, cualquier certificado emitido contra el RD 3/2010 tendrá como fecha máxima de validez el 5 de mayo de 2024. Vencida esta fecha, el certificado dejará de tener validez.

Este certificado es propiedad de Cámara Certifica y está bajo su control. Por tanto, no podrá ser modificado si no es por la propia Cámara Certifica.

8. USO DE REFERENCIAS A LA CERTIFICACIÓN POR LAS ORGANIZACIONES

Las organizaciones certificadas podrán hacer uso de las marcas y certificados en las condiciones y con las restricciones establecidas en el Procedimiento General de utilización de marcas de conformidad (PG-CC-02) que será remitido junto a la documentación relacionada en el apartado anterior.

La Certificación de Conformidad con el ENS podrá representarse mediante un Distintivo de Certificación de Conformidad y cuyo uso por parte de la entidad pública o privada titular o usuaria del sistema de información en cuestión estará condicionado a la posesión de la antedicha Certificación de Conformidad.

El citado Distintivo de Certificación de Conformidad será un documento electrónico, en formato no editable, firmado por Cámara Certifica, que incluirá un enlace que conduzca a la Certificación de Conformidad anterior, que también permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada, respectivamente, de que se trate.

El incumplimiento detectado en una auditoría de certificación del deber de adecuada exhibición de los Distintivos de Conformidad correspondientes será objeto de una No Conformidad Mayor, por cuanto supone el incumplimiento de uno de los preceptos obligatorios del ENS (art. 41 del RD 3/2010 o art. 38.2. del RD 311/2022).

Cámara Certifica supervisará, al menos semestralmente, el uso que las organizaciones certificadas hagan de las marcas de certificación y certificado. En caso de detectarse

incumplimiento, se establece el plazo de un (1) mes para que el cliente lo resuelva. El uso indebido podrá iniciar los mecanismos de sanción dispuestos en el apartado 12 de este documento. En este supuesto, Cámara Certifica se reserva el derecho de establecer las acciones legales que estime oportunas.

Cuando el incumplimiento en la adecuada exhibición del Distintivo de Conformidad fuera imputable a un proveedor de la entidad auditada, Cámara Certifica instará a su cliente a poner remedio a esta anómala situación que, de no resolverse satisfactoriamente, obligará a Cámara Certifica a poner este extremo en conocimiento del Centro Criptológico Nacional, que procederá en consecuencia, conforme a derecho.

9. RECERTIFICACIÓN

Con una antelación aproximada de cuatro meses, el departamento comercial se pondrá en contacto con la organización y se le comunicará la proximidad de la finalización del período de vigencia de dos años del certificado procediendo a la actualización de los datos de la organización.

La organización que desee recertificar su(s) sistema(s) deberá cumplimentar una nueva solicitud formal, la cual seguirá los mismos trámites y procesos descritos en el apartado 6.1 del presente procedimiento.

Las auditorías de recertificación deberán realizarse con una antelación aproximada de dos meses respecto a la vigencia del certificado y serán realizadas en una sola etapa.

Durante la auditoría de recertificación, se auditarán todos los requisitos del esquema ENS al igual que en la auditoría inicial. En especial se revisarán los cambios sufridos desde la auditoría anterior. Así mismo, se verificará:

La eficacia del sistema en relación con el logro de los objetivos,

- El progreso de las actividades planificadas dirigidas a la mejora continua,
- La eficacia del cierre de las no conformidades de la auditoría anterior y el correcto uso de las marcas.

Tras una decisión favorable, del Comité de Certificación, y previo pago de los costes correspondientes, Cámara Certifica emitirá un nuevo certificado de conformidad que atestigüe la renovación de la certificación del ENS, que tendrá el mismo contenido que el descrito en el apartado 7 del presente procedimiento, detallándose la fecha de entrada en vigor de la certificación, la fecha de renovación y la fecha de expiración.

El proceso de toma de decisiones deberá realizarse antes de la expiración de la certificación.

En el caso de que se detecten No Conformidades Mayores en el proceso de evaluación de un sistema ya certificado, éste quedará en suspenso durante el período de resolución de las referidas No Conformidades. En caso de no cerrarlas en un plazo de seis meses, el Certificado de Conformidad quedaría revocado y la organización auditada deberá eliminar el Distintivo de Conformidad de su sede electrónica o página web hasta su próxima recertificación.

La organización que no desee recertificar su(s) sistema(s) deberá comunicar dicha circunstancia a Cámara Certifica. Una vez recibida dicha comunicación y cumplido el plazo de vigencia de la certificación, se procederá a anular el expediente y a su archivo. En el caso de no recibir comunicación y cumplido el plazo de vigencia de la certificación, Cámara Certifica comunicará por escrito la finalización de su condición de organización certificada.

10. AUDITORÍAS EXTRAORDINARIAS

En el proceso de toma de decisiones se podrá considerar la realización de auditorías extraordinarias en los siguientes casos:

- Ante un dictamen "DESFAVORABLE" del sistema de información auditado
- Que la organización o el organismo del que ésta dependa soliciten esta auditoría al detectar fallos del sistema.
- Ante cambios sustanciales en la organización o en su sistema ENS
- Ante reclamaciones o quejas.
- Ante aumentos de alcance entre categorías (de BÁSICA a MEDIA o de MEDIA a ALTA) para la evaluación exclusiva sobre las medidas no evaluadas y siempre y cuando esta extraordinaria se realice antes de cumplidos los seis (6) meses desde que el sistema en cuestión obtuvo la certificación anterior. Transcurridos dichos seis (6) meses, la auditoría será completa.

Los expedientes resultantes de estas auditorías deberán siempre presentarse al Comité de Certificación que emitirá un juicio sobre la concesión, el mantenimiento o no de la certificación (retirada o suspensión), o el levantamiento de la suspensión de la misma, aumento o reducción de alcance.

10.1 tránsito de una Certificación de Conformidad de una categoría a otra superior

El tránsito de una Certificación de Conformidad de categoría BÁSICA a una de categoría MEDIA, o de categoría MEDIA a una de categoría ALTA, con la exclusiva evaluación de aquellas medidas que no hayan sido evaluadas en la auditoría anterior, podrá ser posible si concurren las siguientes circunstancias:

- El proceso de realización de la nueva auditoría para la categoría superior, incluyendo la evaluación del Plan de Acciones Correctivas, debe realizarse, íntegramente, dentro del período de validez de los dos (2) años de la Declaración o Certificación de Conformidad vigente.
- El alcance del sistema de información que pretende elevarse de categoría debe ser exactamente el mismo que el que fue evaluado para la categoría inferior.
- Es imperativo que no se hayan producido cambios en el sistema de información concernido, y, en todo caso, solo podrá realizarse si no han transcurrido más de seis meses desde la evaluación previa.

- Se deberá mantener la fecha de la Declaración o Certificación de Conformidad con la que se expidió el certificado precedente, lo que supone que el período de validez de la nueva Certificación será coincidente con el expresado en la Declaración o Certificación anterior.
- En relación con el aumento del alcance aplicable exclusivamente a sistemas previamente certificados contra el RD 3/2010, se seguirá el siguiente protocolo:

  o Es condición "sine qua non" que la auditoría extraordinaria a la que haya lugar debe realizarse antes de cumplidos los seis (6) meses desde que el sistema en cuestión obtuvo la certificación anterior, lo que posibilita que la evaluación solo necesite hacerse sobre las medidas no evaluadas. Transcurridos dichos seis (6) meses, la auditoría será completa.

  o No es posible acometer lo descrito en el punto anterior si lo pretendido es un aumento de alcance que persiga la certificación contra el RD 311/2022. En estos casos, la auditoría será completa.

11. DERECHOS Y OBLIGACIONES DE LAS EMPRESAS CERTIFICADAS

En la oferta/contrato se incluyen las "Condiciones generales de certificación", que describen los derechos y obligaciones de las organizaciones certificadas. Así mismo, se describen las obligaciones de Cámara Certifica para con las organizaciones.

Adicionalmente:
a) la organización auditada deberá contar con procedimientos que permitan detectar las modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas, tal y como dispone el artículo 31 y el Anexo III del ENS y comunicar esta circunstancia a la Entidad de Certificación (EC), o al Órgano de Auditoría Técnica del Sector Público (OAT), de que se trate.

12. APERCIBIMIENTO, SUSPENSIÓN, RETIRADA, RECHAZO DE LA CERTIFICACIÓN O REDUCCIÓN DE ALCANCE

Se podrá apercibir, suspender, retirar o reducir la certificación a una organización si se demostrara que no ha cumplido los requisitos y compromisos incluidos en el presente procedimiento y en el correspondiente contrato de certificación y, en particular, se hubiera puesto de manifiesto alguno, entre otros, de los hechos descritos a continuación:

a) No mantener adecuadamente implantado el sistema ENS certificado
b) Hacer un uso inadecuado de las marcas de certificación.
c) Hacer una inadecuada publicidad de su condición de organización certificada.
d) No prestar la adecuada colaboración a los equipos auditores de Cámara Certifica, ENAC u Organismos Reguladores en el desempeño de sus labores de evaluación.

e) No cumplir con las obligaciones económicas derivadas de la condición de organización certificada.

f) No cumplir los plazos establecidos en cada una de las fases del proceso de certificación.

g) No cumplir con sus obligaciones legales, en base a sus actividades y al referente auditado.

h) No comunicar a Cámara Certifica, o al Órgano de Auditoría Técnica del Sector Público (OAT), de que se trate las modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La ausencia de tal comunicación, cuando fuere necesaria, podrá suponer la retirada de la Certificación de Conformidad concedida.

El jefe Técnico de Área, solicitará a la organización afectada aclaración sobre los hechos de que se trate, fijando un plazo para presentar las evidencias, alegaciones que entendiese oportunas. Una vez valorada la información remitida por la organización, lo elevará al Comité de Certificación quien tomará la decisión oportuna (apercibimiento, suspensión temporal, retirada o rechazo de la certificación, reducción de alcance u otro tipo de decisiones adecuadas al incumplimiento detectado).

Cuando se trate de incumplimientos relativos al punto d) y e), el responsable de Calidad, Jefe Técnico de Área o el Director Gerente podrán iniciar los trámites necesarios y elevarlo al Comité de Certificación de acuerdo con lo establecido anteriormente.

Dependiendo de la gravedad de los incumplimientos detectados y de si son de carácter repetitivo o no, se aplicará uno de los tres tipos de decisión siguientes:

12.1) Apercibimiento

Comunicación por escrito por parte de Cámara Certifica de que la repetición de los hechos constatados podrá ser motivo de la suspensión o retirada de la certificación, indicando la obligación por parte de la empresa de adoptar las acciones necesarias en un plazo determinado.

12.2) Suspensión temporal

Implica la prohibición inmediata de utilizar por parte de la empresa las marcas de conformidad y certificados, así como de toda publicidad que, de cualquier forma, contenga alguna referencia a la certificación, hasta que no se subsanen los incumplimientos detectados.

De producirse esta situación y previo a poder finalizar la suspensión temporal, que no podrá ser superior a 6 meses, será necesario realizar una auditoría extraordinaria a la organización con resultado satisfactorio.

12.3) Retirada de la certificación

Implica la prohibición inmediata de utilizar por parte de la organización las marcas de conformidad y certificados, así como de toda publicidad que, de cualquier forma, contenga alguna referencia a la certificación y la devolución del correspondiente certificado a Cámara Certifica, así como la retirada de la organización del registro de organizaciones certificadas.

Aquellas organizaciones a las que se les haya retirado la certificación deberán reiniciar todo el proceso de certificación, incluyendo una nueva solicitud.

12.4) Rechazo

Implica la no concesión de la certificación a la organización en la fase de certificación inicial.

12.5) Comunicación de la resolución

La decisión sancionadora o el levantamiento de la sanción, incluyendo sus motivos, adoptada por el Comité de Certificación será comunicada por escrito a la organización y partes interesadas con carácter inmediato.

13. TRATAMIENTO DE APELACIONES, QUEJAS O RECLAMACIONES

13.1) Tramitación de apelaciones

Se consideran apelaciones aquellas comunicaciones en contra de decisiones en materia de certificación presentadas por empresas solicitantes de la certificación, a saber:

a) Decisiones del equipo auditor sobre el levantamiento de no conformidades contra requisitos o criterios de certificación.
b) Decisiones denegatorias de la concesión de la certificación en procesos iniciales.
c) Decisiones sobre suspensión temporal o retirada definitiva de certificados tras las actividades de evaluaciones periódicas a organizaciones certificadas o incumplimiento de las obligaciones de organización certificada.
d) Decisiones de apercibimiento o sancionadoras (incremento de la frecuencia o del tiempo de auditoría, realización de auditorías extraordinarias) por incumplimiento por parte de las organizaciones certificadas de las obligaciones derivadas de su condición de certificadas.

Las apelaciones deberán ser presentadas por escrito dirigiéndolas a Cámara Certifica, aportando razones objetivas y adecuadamente justificadas, que tras la comprobación por parte del responsable de calidad que la apelación se relaciona con actividades de certificación realizadas por Cámara Certifica, notificará al apelante por escrito el acuse de recibo correspondiente y se le solicitará, en su caso, aclaraciones y toda la documentación necesaria para alcanzar una decisión sobre la apelación.

El escrito de apelaciones, junto a toda la documentación relacionada con la decisión contra la que se alega, será trasladado con la mayor brevedad posible al Jefe de Área Técnica, cuando la alegación se refiera a las generadas en la realización de la auditoría o al Responsable de Calidad cuando se refieran a decisiones de la certificación.

El Responsable de Calidad y/o Jefe Técnico de Área solicitará al equipo auditor y/o Responsable Técnico de Área, las aclaraciones oportunas para solventar la alegación recibida.

El Responsable Calidad o el Jefe Técnico de Área, en su caso, contactarán con la organización ofreciendo la posibilidad de presentar cuanta documentación crea necesaria, y si lo considera necesario, dará audiencia personal al interesado.

En el caso de alegaciones contra las no conformidades o actuaciones del equipo auditor, será el Jefe Técnico de Área quien revise y analice dicha documentación o en su defecto otro Responsable de área técnica que no haya estado involucrado en la decisión apelada, quien tomará una opinión al respecto que podrá ser trasladada al Comité de Certificación.

En el caso de alegaciones contra la decisión del Comité de Certificación, será igualmente un Responsable Técnico de Área no involucrado en la decisión apelada quien revisará y analizará la documentación recopilada junto con la apelación y tomará una decisión al respecto, que se trasladará al Comité de Certificación.

Tras el análisis descrito por el Jefe Técnico de Área o por el Comité de Certificación se adoptará una resolución que será comunicada por escrito al apelante, donde se justificará la decisión de manera motivada y objetiva y que tendrá carácter definitivo.

Cámara Certifica informará al apelante cuando haya finalizado el proceso para el tratamiento de la apelación y se realizará a través de la comunicación de la decisión de certificación adoptada por el Jefe Técnico de Área o el Comité de Certificación.

13.2) Tramitación de quejas o reclamaciones

Se consideran quejas, expresiones de insatisfacción, diferentes de las apelaciones, aquellas presentadas por una persona u organización en relación a actividades relacionadas por una organización solicitante de la certificación, organización certificada o Cámara Certifica.

Las reclamaciones deberán ser presentadas por escrito dirigiéndolas a Cámara Certifica.

A partir de la recepción de una queja o reclamación, el Responsable de Calidad de Cámara Certifica la analizará y confirmará si la queja/reclamación se refiere a un cliente certificado o si concierne a las actividades de certificación de las que es responsable Cámara Certifica.

Con respecto a las reclamaciones relativas a organizaciones, en el análisis efectuado para comprobar la viabilidad de la gestión de este tipo de reclamaciones se deberá tener en cuenta:

- Que la organización contra la que se recibe la queja dispone de un certificado en vigor.
- Que la actividad que ha originado la queja está cubierta por el sistema de gestión y el alcance certificado.
- Que el reclamante se ha dirigido en primera instancia a la organización certificada. En caso negativo, Cámara Certifica deberá indicar al reclamante que con anterioridad al tratamiento por Cámara Certifica será necesario que reclame a la organización certificada.

Previamente al registro de la reclamación, el Responsable de Calidad la analizará para comprobar si es posible validar la queja. En caso positivo se dará entrada en el registro de documentación y se notificará al reclamante por escrito el acuse de recibo correspondiente.

Una vez admitida la queja, el Responsable de Calidad recopilará la información necesaria e investigará específicamente los hechos y el comportamiento de Cámara Certifica o de la organización certificada en relación con las actividades de certificación o la conformidad con los requisitos de la norma de referencia en el caso de reclamaciones contra organizaciones certificadas.

a) Actuaciones de CÁMARA CERTIFICA

Cámara Certifica ha implantado un procedimiento para el tratamiento de reclamaciones de índole administrativa, técnica y humana (por la actuación de sus auditores), por incumplimiento de los requisitos de confidencialidad establecidos, o de cualquier otro derivado de sus relaciones contractuales, el cual se encuentra a disposición de las organizaciones que lo soliciten.

A la vista del análisis realizado se tomarán las acciones inmediatas necesarias para la resolución de la reclamación recibida.

Si el resultado de la investigación pone de manifiesto que la actividad desarrollada por Cámara Certifica no es conforme y es la causa de la queja recibida, el Responsable de calidad actuará de acuerdo al procedimiento interno de gestión de reclamaciones.

El resultado de la investigación y su resolución deberá ser puesto en conocimiento del reclamante.

b) Actuaciones de organizaciones certificadas

En este caso concreto, además de otra documentación, el Responsable de Calidad recabará información relativa:

- Acciones reparadoras tomadas por la organización certificada hacia el reclamante.
- Acciones correctivas tomadas, en su caso, para evitar la recurrencia y su eficacia.

Si el resultado de la investigación pone de manifiesto que la organización ha actuado sin respetar su sistema certificado, que éste no es conforme con los requisitos del esquema ENS o que es ineficaz para lograr los objetivos previstos, Cámara Certifica tomará las medidas adecuadas que podrán consistir en:

- Apercibimiento a la organización sobre los hechos detectados y sus eventuales consecuencias.
- Realización de auditorías extraordinarias.
- Aplicación de los procedimientos de sanciones de la entidad (suspensión, retirada o reducción del alcance certificado).

El análisis de la queja puede requerir entre otras actividades, la visita a la organización.

Como resultado de sus investigaciones, Cámara Certifica se pronunciará sobre la eficacia del sistema de información y su conformidad con el RD 3/2010 o RD 311/2022 y sus decisiones, tomadas en el Comité de Certificación, quedarán limitadas a la suspensión, retirada, reducción o mantenimiento de la certificación.

Cámara Certifica no se pronunciará sobre cumplimientos o incumplimientos contractuales o legales. Por ello, el hecho de que la queja esté siendo investigada en otras instancias (tribunales, autoridades de consumo, etc.) no será en general motivo suficiente para que se paralice o retrase su tratamiento.

Toda la información generada en el tratamiento de la reclamación será puesta en conocimiento del auditor responsable del expediente, en su caso, para que durante la siguiente visita se investigue específicamente el estado del cierre de las no conformidades, internas y externas, que se hubieran derivado de la investigación de la queja así como la eficacia continuada de las acciones tomadas al respecto.

El resultado de la investigación y resolución se trasladará a la organización certificada y al reclamante.

14. CONFIDENCIALIDAD

La información recibida por Cámara Certifica o por las personas involucradas en el proceso de certificación, incluyendo el organismo de acreditación y organismos competentes en el esquema, será considerada privada y tratada a todos los efectos como confidencial. Salvo la información que el cliente pone a disposición pública o la relativa a la validez de la certificación.

La información relativa al cliente obtenida de fuentes distintas al mismo (quejas, reclamaciones, o de autoridades reglamentarias, etc.) será tratada por Cámara Certifica como confidencial.

Cuando Cámara Certifica, fuera obligada por la ley o autorizada por acuerdos contractuales (como aquellos celebrados entre Cámara Certifica y la Entidad Nacional de Acreditación – ENAC-) a divulgar información confidencial, el cliente o la persona involucrada debe ser notificada sobre la información proporcionada, salvo que esté prohibido por ley.

Si bien, en el caso de auditorías de vigilancia para el mantenimiento de la acreditación de Cámara Certifica en el esquema ENS, Cámara Certifica podrá divulgar a ENAC y/o CCN la información confidencial recopilada en el transcurso de las auditorias de sus clientes, sin necesidad de ser éstos notificados explícitamente.

En concreto se considerará como información y documentos sometidos a confidencialidad los siguientes:

- Informes de Auditoria,
- Documentación aportada por el cliente o generada en el transcurso de la auditoría como: planes de acciones correctivas, etc…

Cámara Certifica podrá hacer entrega de una copia del informe de auditoría al CCN a requerimiento de éste, en los términos previstos en los artículos nº 37 (RD 3/2010) o nº 34 (RD 311/2022) del ENS. El equipo auditor no entregará ni concederá acceso al informe de auditoría a terceros distintos de los indicados anteriormente, salvo por imperativo legal o mandato judicial.

Cámara Certifica, dispone de los medios necesarios para asegurar la confidencialidad, integridad y accesibilidad de la información mencionada anteriormente, mediante:

- Control de acceso físico de personal ajeno a las instalaciones de Cámara Certifica
- Acceso restringido a las salas donde se gestiona y almacena la documentación.
- Se dispone de servidores diferenciados para correos electrónicos y almacenamiento de la información.
- La información almacenada en el servidor de ficheros se accede a ella con usuarios existentes en un Directorio Activo Windows Server 2012R2 con nivel funcional del bosque y del dominio de "Windows Server 2012R2", usuarios con contraseñas de "nivel alto" y acceso a las carpetas mediante grupos de seguridad global.
- El acceso a la información de los expedientes está restringida al personal que participa en la certificación ENS. Dicho acceso se realiza a través de niveles de usuarios definidos.
- Las comunicaciones que se realizan con el cliente, equipo auditor y otros miembros de Cámara Certifica se realizan a través de cuentas de correo corporativas protegidas por usuario y contraseña de alta seguridad.
- En los casos en el que el cliente aporte la documentación mediante sistemas de encriptación o cifrado, Cámara Certifica, mantendrá medios similares de seguridad para la transmisión de dicha información al personal externo implicado en el proceso.

Así mismo, tanto en los contratos con los auditores, como en las ofertas/contrato y en las designaciones del equipo auditor, existen cláusulas de confidencialidad sobre la información a la que se tiene acceso a lo largo del proceso de certificación. Así mismo, todo el personal interno de Cámara Certifica tiene firmados compromisos de confidencialidad.

15. INFORMACIÓN PÚBLICA

Cámara Certifica hará accesible al público, cliente o mercado a través de la Web o proporcionará por otro medio:

- El presente procedimiento en el que se describe el proceso completo de auditoría y certificación; los procesos para otorgar, denegar, mantener, renovar, suspender, restaurar o retirar la certificación o ampliar o reducir el alcance de certificación; los proceso para gestionar solicitudes de información, quejas y apelaciones
- Los esquemas de certificación y áreas geográficas en los que opera.
- El uso del nombre y marca o logo de certificación y la manera de hacer referencia a la certificación otorgada.

Respecto a las certificaciones otorgadas, Cámara Certifica pondrá a disposición del público en general, a través de la web los medios para confirmar la validez de una certificación dada.

Las tarifas de Cámara Certifica para la realización de actividades de certificación estarán a disposición de cualquier persona interesada previa solicitud escrita.

16. ANEXOS

Solicitud de Información (SI SG– datos generales, apartados SGSI y ENS)
Modelo “Oferta/contrato para la certificación” (OF/C_ENS)