Instituto de Certificación S.L.
www.icdq.es

# Procedimiento de prestación del servicio de certificación en el ENS

© 2024 ICDQ S.L. – Material reservado, está prohibido cualquier uso o duplicación en cualquier formato o medio sin autorización escrita previa por parte de Instituto de Certificación S.L.

**DIFUSIÓN LIMITADA**

# Indice

## CONTROL DE FIRMAS

| ROL | FECHA | FIRMA |
|---|---|---|
| ELABORADO POR<br>Responsable técnico, supervisor de expedientes | 04/06/2024 | Luis Diez García, |
| APROBADO POR<br>Director de certificación | 06/06/24 | Luis Tatay |

## CONTROL DE VERSIONES

| VERSIÓN | FECHA | AUTOR | CAMBIOS |
|---|---|---|---|
| 1.0 | 06/06/2024 | Luis Tatay | Versión inicial del documento |
| | | | |
| | | | |
| | | | |

# 1. Ámbito de aplicación

Este documento tiene por objeto establecer y describir el desarrollo del proceso de certificación según los requisitos establecidos en el Esquema Nacional de Seguridad (en adelante ENS), desde la elaboración de la oferta hasta la toma de decisión y emisión de certificados. Estas actividades comprenden los siguientes procesos:

- Elaboración de ofertas. Revisión de solicitud
- Designación del equipo auditor.
- Planificación de auditorías
- Realización de auditorías. Desarrollo y Ejecución. Elaboración de Informe
- Valoración del Plan de Acciones Correctivas
- Toma de decisión. Emisión del Certificado

El presente documento, dirigido a clientes de la certificación, es de aplicación para todas las actividades desarrolladas durante el proceso de certificación ENS por todas las partes implicadas en la evaluación y certificación de los mismos, entendiendo como partes implicadas todos los participantes en el proceso de evaluación (auditores, responsables técnicos de área y personal interno de ICDQ).

# 2. Documentación de referencia

- UNE-EN-ISO/IEC 17065 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Guía CCN-STIC 809, "Declaración y certificación de conformidad con el ENS y distintivos de cumplimiento"
- Guía CCN-CERT IC-01/19, "Criterios generales de auditoría y certificación"

# 3. Términos y definiciones

- Auditoría de sistemas de información: 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: auditoría requerida para dar cumplimiento a lo establecido en el artículo 34 y en el Anexo III del RD 311/2022, y por lo tanto, verificar el cumplimiento de los requisitos establecidos en los capítulos II y III y anexos I y II del ENS. 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 obtencion de la certificación y las renovaciones para su mantenimiento.
- Auditoría 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.
- Personal efectivo: consiste en todo el personal involucrado en el alcance de la certificación.
- Información documentada: Información que una organización tiene que controlar y mantener y el medio en el que está contenido.

- No conformidad menor: existe algún requisito del Real Decreto 311/2022 por el que se regula el ENS, que no se está cumplimiento total o parcialmente, pero que no representa un riesgo grave para el desempeño del SGSI-ENS.
- No Conformidad Mayor: "No Conformidades Menores" en relación con cualquiera de los preceptos contenidos en el Real Decreto 311/2022, en el Marco organizativo de su anexo II, o en varios controles a la vez que integran alguno de los dominios del Marco operacional o el de Medidas de Protección, de forma que evaluados en su conjunto, puedan implicar el incumplimiento del objetivo del dominio considerado.
- Observación: incumplimiento potencial de un requisito, a juicio del auditor, y caso de no ponerse remedio en un corto plazo de tiempo podría derivar en una no conformidad.

# 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) 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).
b) Las actividades desarrolladas en cada uno de sus centros de trabajo y que están cubiertas por el sistema que soporta el ENS.
c) 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 parte de ICDQ 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 ICDQ, 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.

ICDQ 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.

Los requisitos para obtener la certificación en el esquema ENS no son otros que haber superado el 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 (RD 311/2022)

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 ICDQ 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 ICDQ.

## 6. Imparcialidad & Confidencialidad

Las actividades de certificación desarrolladas por ICDQ 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.
La Declaración de Imparcialidad está a disposición de las organizaciones certificadas en la página web de ICDQ y ha sido aprobada por el Director General y ratificada por el Comité de Partes de ICDQ.
Para asegurar dicha imparcialidad, ICDQ ha realizado un análisis para identificar conflictos de intereses y gestionarlos de manera adecuada. Dicho análisis ha sido aprobado por la Dirección General y ratificado por el Comité de Partes de ICDQ, cuya composición de sus miembros está a disposición de cualquier empresa u organismo interesado.
La información recibida por ICDQ 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 ICDQ como confidencial.

Cuando ICDQ, fuera obligada por la ley o autorizada por acuerdos contractuales (como aquellos celebrados entre ICDQ 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.

# 7. Actuaciones previas al inicio de la auditoria

## 7.1. Recogida de datos y elaboración de ofertas

La organización interesada en recibir una oferta de certificación deberá facilitar al departamento comercial de ICDQ 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, ver apartado 8.2.1 del presente documento, se enviará 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.

## 7.2. 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 (Ficha de solicitud de información inicial)

### 7.3. Designación del equipo auditor

El Responsable Técnico designará, de entre los auditores cualificados, 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, ICDQ 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.

ICDQ 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.

Los auditores cualificados podrán ser tanto del personal de la plantilla de ICDQ como contratados externamente.
ICDQ 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

## 8. Desarrollo de la auditoria

Este capítulo detalla la preparación y realización de la actividad de auditoría. La figura que sigue proporciona una visión general de las actividades del proceso de auditoría en consideración la norma UNE-EN ISO 19011:2018


**Ilustración 1. Actividades de auditoría (ISO 19011:2018)**

## 8.1. Preparación de actividades

### 8.1.1. Revisión de la documentación

Se revisará la documentación pertinente relacionada con el Sistema de Información que se certifica y su sistema de gestión asociado, de existir. El objetivo es:

- Reunir información para preparar las actividades de auditoría y los documentos de trabajo aplicables, por ejemplo, sobre servicios, funciones, etc.
- Establecer una visión general del grado de completitud de la documentación del Sistema para detectar posibles carencias.

**La documentación requerida incluirá, al menos, los siguientes documentos:**

- Política de seguridad
- Organigrama/identificación responsables de la información, servicios, seguridad, sistema
- Descripción detallada del sistema de información bajo el alcance (Sw, Hw, comunicaciones, etc)
- Política de firma electrónica y certificados
- Normativa de seguridad
- Informes con el análisis y tratamiento de la apreciación del riesgo
- Declaración de aplicabilidad
- Registros de actividad relativos a las medidas de seguridad implantadas o en estado de implantación
- Informes de auditorías previas de seguridad y de e seguimiento de los resultados de auditorías
- Lista de proveedores externos (que afecten al alcance) y evidencias del control realizado sobre los servicios
- Sistemas de métricas con referencias a las guías CCN-STIC-815, CCN-STIC-824

### 8.1.2. Plan de auditoria

El Auditor Jefe preparará un plan de auditoría basado en los requisitos establecidos en el Esquema de Certificación, basada en las medidas de seguridad del Anexo II del RD 311/2022 que apliquen, según la categoría del sistema de información que se certifique, y en su articulado relevante.

El plan de auditoría cubrirá o hará referencia a lo siguiente:

- El alcance, criterios y objetivo de la auditoría.
- Modalidad de auditoría, que podrá ser en remoto y/o presencial
- Las ubicaciones, las fechas, el horario y la duración previstos de las actividades de auditoría, con indicación, en su caso, del rol del auditado más adecuado para su participación.
- las funciones y responsabilidades de los miembros del equipo auditor para cada actividad de auditoría, así como los observadores, en su caso.

## 8.2. Realización de actividades

Habitualmente las actividades de auditoría se realizarán en una secuencia definida como se muestra en la ilustración anterior. Esta secuencia puede variar para adaptarse a las circunstancias específicas de determinada auditoría (Inicial, de renovación o extraordinaria).

### 8.2.1. Reunión de apertura

El propósito de la reunión de apertura es:

- Confirmar el acuerdo de todas las partes sobre el plan de auditoría y adaptarlo de forma consensuada, si es el caso.
- Presentar al equipo auditor.
- Asegurarse de que se pueden realizar todas las actividades de auditoría planificadas.
- Resolver cuántas cuestiones pueda plantear el cliente al Auditor Jefe o éste considere relevante informar previamente.

Es deseable que en la reunión de apertura esté presente algún miembro de la Dirección del auditado y, cuando sea apropiado, aquellos responsables de las áreas o unidades que se van a auditar. Durante la reunión de apertura se proporcionará la oportunidad de realizar preguntas.

### 8.2.2. Recopilación y verificación de la información

Durante la auditoría se recopilará y verificará, mediante un muestreo apropiado, la información pertinente a los objetivos, el alcance y los criterios de la misma, incluyendo la información relativa a las interrelaciones entre funciones, actividades y procesos.
Los métodos para recopilar la información incluyen lo siguiente:

- entrevistas
- observaciones
- revisión de información documentada.

Durante la auditoría, el Auditor Jefe comunicará periódicamente los progresos de la auditoría y cualquier inquietud al auditado. Las evidencias recopiladas durante la auditoría que sugieren un riesgo inmediato y significativo para el sistema de información evaluado se comunicarán sin demora al auditado.
Cuando los hallazgos de auditoría basados en evidencias indiquen que los objetivos de la misma no son alcanzables, el líder del equipo auditor informará de las razones al cliente de la auditoría y al auditado para determinar conjuntamente las acciones apropiadas. Estas acciones pueden incluir, entre otras, la modificación del plan de auditoría, cambios en el alcance de la auditoría, o el aplazamiento de la misma.

### 8.2.3. Hallazgos en la auditoría

Los Hallazgos serán clasificados conforme a la siguiente taxonomía:

- Conformidad.
- Oportunidades de Mejora, de haberlas
- Observaciones
- Desviaciones:
  - No Conformidades, graduadas a su vez en:
    - No Conformidad Menor.
    - No Conformidad Mayor.

En el informe se registrarán las No Conformidades, observaciones y las evidencias de auditoría que las apoyan que serán revisadas con el auditado para reconocer que la evidencia de la auditoría es exacta y que las no conformidades se han comprendido.

### 8.2.4. Realización de la reunión de cierre

La reunión de cierre, dirigida por el Auditor Jefe, se realizará para presentar los hallazgos y las conclusiones de la auditoría.

Las conclusiones de la auditoría pueden tratar aspectos tales como los siguientes:

- El grado de conformidad y el reconocimiento de la fortaleza del sistema de información con los criterios de auditoría, incluyendo la eficacia del sistema para cumplir los resultados previstos.
- La eficacia de la implementación, el mantenimiento y las acciones de mejora continua, del sistema de información y su sistema de gestión asociado, de existir.
- El logro de los objetivos de la auditoría, cobertura del alcance de la auditoría y completitud en la verificación de los criterios de la auditoría.
- Hallazgos repetitivos o similares encontrados en distintas áreas que se auditaron, con el propósito de identificar tendencias.

Entre los participantes en la reunión de cierre se recomienda estén los representantes de la dirección del auditado y, cuando sea apropiado, aquellos responsables de las áreas o unidades que han sido auditadas.

Se comunicará durante la reunión el periodo de tiempo para presentar un Plan de Acciones Correctivas (PAC) que trate las desviaciones (No Conformidades Mayores y/o menores) surgidas de la auditoría.

Cualquier opinión divergente relativa a los hallazgos de la auditoría o las conclusiones entre el equipo auditor y el auditado deben discutirse y, si es posible, resolverse. Si no se resuelve, deberán registrarse todas las opiniones.

Se indicará que caso de constar en el Informe de Auditoría, Observaciones u Oportunidades de Mejora, ésas no son obligatorias de resolver inmediatamente, ni requieren plan de acciones correctivas.

## 8.3. Informe de auditoría

El Auditor Jefe enviará el informe de la auditoría al auditado en los 15 días siguientes a la finalización de la auditoría.

El informe de auditoría proporcionará un registro completo, preciso, conciso y claro de la auditoría, y hará referencia a lo siguiente:

- los objetivos de la auditoría;
- el alcance de la auditoría, particularmente la identificación de los sistemas de información auditados y sus servicios soportados;
- la identificación de la organización responsable el sistema de información auditado;
- la identificación del equipo auditor y de los participantes del auditado en la auditoría;
- las fechas y ubicaciones donde se realizaron las actividades de auditoría;
- los criterios de auditoría (en este caso, como mínimo, el RD 311/2022);
- los hallazgos de la auditoría y las evidencias relacionadas;
- las conclusiones de la auditoría;
- el resultado de la auditoría: FAVORABLE, FAVORABLE CON NO CONFORMIDADES o DESFAVORABLE;
- una declaración del grado en el que se han cumplido los criterios de la auditoría;
- cualquier opinión divergente sin resolver entre el equipo auditor y el auditado;
- que las auditorías, por naturaleza, son un ejercicio de muestreo; como tales, hay un riesgo de que las evidencias de auditoría examinadas no sean representativas.

El informe de la auditoría también puede incluir o hacer referencia a lo siguiente, cuando sea apropiado:

- cualquier aspecto dentro del alcance de la auditoría, que no ha podido ser cubierto;
- un resumen incluyendo las conclusiones de la auditoría y los principales hallazgos de la auditoría que las apoyan;
- las oportunidades para la mejora, de haberlas;
- las buenas prácticas identificadas (puntos fuertes);
- una declaración sobre la naturaleza confidencial de los contenidos;

El informe de auditoría se emitirá en el periodo de tiempo acordado.

## 8.4. Acciones correctivas/alegaciones

Tras la recepción del informe de auditoría, la organización solicitante deberá presentar a ICDQ 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.

Se deberán adjuntar las evidencias solicitas por el auditor jefe.

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

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.

## 8.5. 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.

ICDQ 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.

Ante un dictamen "DESFAVORABLE", 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.

Asimismo, se pondrá en conocimiento del solicitante la posibilidad de recurrir las decisiones adoptadas en materia de certificación.

# 9. Concesión de la certificación

Tras la decisión de certificación favorable, y previo pago de los costes correspondientes, ICDQ emitirá documentos oficiales que justifiquen la concesión de la certificación ENS en la categoría que corresponda (básica, media, alta) y tendrá una vigencia de 2 años.

El Certificado emitido por ICDQ, seguirá las directrices definidas en la guía **CCN-STIC-809**

**Este certificado es propiedad de ICDQ y está bajo su control. Por tanto, no podrá ser modificado si no es por el propio ICDQ.**

# 10. Uso de referencias a la certificación

Las organizaciones certificadas podrán hacer uso de las marcas y certificados que serán remitidos junto a la documentación relacionada en el apartado anterior, en las condiciones y con las restricciones establecidas en el Anexo II del presente documento.

La marca permanecerá accesible a través de la sede electrónica o página web de la entidad certificada, e incluirá un enlace que conduzca a visualizar la Certificación de Conformidad.

ICDQ supervisará el uso que las organizaciones certificadas hagan de las marcas de certificación y certificado. El uso indebido podrá iniciar los mecanismos de sanción dispuestos en el apartado 13 de este documento. En este supuesto, ICDQ se reserva el derecho de establecer las acciones legales que estime oportunas.

# 11. Renovación de la certificación

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 renovar la certificación deberá cumplimentar una nueva solicitud, la cual seguirá los mismos trámites y procesos descritos en el apartado 7 del presente procedimiento.

Las auditorías de renovación 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 renovación, 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, y previo pago de los costes correspondientes, ICDQ emitirá un nuevo certificado de conformidad que atestigüe la renovación de la certificación del ENS, 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 caso de un sistema certificado sobre el que se detecten No Conformidades Mayores, durante su período de resolución, el Certificado de Conformidad quedará en suspenso. En caso de no cerrar las No Conformidades Mayores 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.
La organización que no desee renovar su certificación deberá comunicar dicha circunstancia a ICDQ. 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, ICDQ comunicará por escrito la finalización de su condición de organización certificada.

## 12. 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.

En estos casos la auditoría los tiempos de auditoría se ajustarán a las deficiencias detectadas y nunca será inferior a 0,5 jornadas.

Los expedientes resultantes de estas auditorías deberán seguir el proceso descrito en este procedimiento y será el Comité de Certificación quien emitirá un juicio sobre la concesión o no de la certificación o el levantamiento de la suspensión.

# 13. Apercibimiento, suspensión, retirada...

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 ICDQ, 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.

El Responsable de Área Técnica, 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 Director de Certificación podrá 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:

a) **Apercibimiento**

Comunicación por escrito por parte de ICDQ 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.

b) **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 in situ a la organización con resultado satisfactorio.

c) **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 ICDQ, 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.

# 14. Apelaciones, quejas o reclamaciones

## 14.1. 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:

- Decisiones del equipo auditor sobre el levantamiento de no conformidades contra requisitos o criterios de certificación.
- Decisiones denegatorias de la concesión de la certificación en procesos iniciales.
- 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.
- Decisiones de apercibimiento o sancionadoras (incremento de la frecuencia o del tiempo de auditoría, realización de auditorías especiales) 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 ICDQ, aportando razones objetivas y adecuadamente justificadas, que tras la comprobación por parte del responsable de calidad, notificará al apelante por escrito el acuse de recibo correspondiente y se le solicitará, en su caso, aclaraciones y toda la documentación necesaria.

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 Responsable del 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 solicitará al equipo auditor y/o Responsable del Área Técnica, las aclaraciones oportunas para solventar la alegación recibida.

El Responsable del Área Técnica o el Director de Certificación, 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 Responsable del Área Técnica quien analice dicha documentación y tome una opinión al respecto que podrá ser trasladada al Comité de Certificación.

Tras el análisis descrito 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.

ICDQ 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 Comité de Certificación.

## 14.2. 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 ICDQ.

A partir de la recepción de una queja o reclamación, el responsable de calidad de ICDQ 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 ICDQ.

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, ICDQ deberá indicar al reclamante que con anterioridad al tratamiento por ICDQ 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 ICDQ 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 ICDQ**

ICDQ 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 ICDQ 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, ICDQ 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, ICDQ se pronunciará sobre la eficacia del sistema y su conformidad con el RD 311/2022 y sus decisiones, tomadas en el Comité de Certificación, quedarán limitadas a la suspensión, retirada, reducción o mantenimiento de la certificación.

ICDQ 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.

# 15. ANEXOS

- Anexo I. Uso de marcas de certificación
- Anexo II. Derechos y obligaciones

# ANEXO I. USO DE MARCAS DE CERTIFICACIÓN

Este anexo se refiere a las marcas de certificación del ENS, en base a sellos oficiales, cuyo modelo base es propiedad del Centro Criptológico Nacional (CCN), así como certificados de conformidad expedidos por ICDQ siguiendo contenidos mínimos y directrices del CCN.

Los certificados expedidos por ICDQ a la organización, área o unidad que certifica alguno de sus sistemas de información para los fines de este documento, estará alineada con la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad y con cualquier resolución posterior que la reemplace o modifique.

Asimismo, se concretará en base a anexos de la Guía CCN-CERT IC-01/19 sobre criterios generales de auditoría y certificación del ENS, y en la guía CCN-STIC-809 sobre declaración, certificación y aprobación de conformidad con el ENS y distintivos de cumplimiento.

El uso de la Marca de Certificación únicamente está autorizado en las condiciones fijadas en el presente documento, comprometiéndose a respetarlo las organizaciones, áreas o unidades con algún sistema de información certificado de conformidad con las disposiciones del ENS. Lleva aparejado la licencia de uso de la marca, en los términos previstos, en calidad de organización que ha obtenido la certificación para alguno de sus sistemas de información. El uso de dicha marca (certificado o sello de certificación) por un período renovable, habitualmente de dos años, se limita estrictamente a la organización, área o unidad cuyo(s) sistema(s) de información ha(n) sido certificado(s) satisfactoriamente respecto a las disposiciones del ENS por ICDQ en calidad de organismo de certificación.

La Marca de Certificación mostrada en el anexo I es un ejemplo de los tres sellos de certificación disponibles en función de la categoría del sistema: BÁSICA, MEDIA o ALTA. Además, el organismo de certificación expenderá a la organización cliente cuyo sistema de información ha sido certificado, un certificado de conformidad con las disposiciones del ENS para la categoría y alcance acordados. ICDQ se reserva el derecho de reemplazar el sello de certificación mostrada en el anexo I, o el Certificado de Conformidad con el ENS, por otro en cualquier momento, de común acuerdo con el CCN, aunque siempre se advertirá a las organizaciones, áreas o unidades titulares del certificado de dicha circunstancia, igual que de cualquier otro cambio que se produzca en el Esquema de certificación, siempre alineado con las ITS o guías correspondientes editadas por el CCN.

La autorización del derecho de uso de la marca de certificación (sello y certificado de conformidad) se obtiene con la consecución y posteriores renovaciones de la Certificación de Conformidad con las disposiciones del ENS. No sustituirá en ningún caso a la garantía ni a la responsabilidad sobre los

servicios soportados por el sistema de información certificado que, de acuerdo con la ley, corresponde al licenciatario de la marca de certificación.

## I.1 Condiciones de aplicación

El uso de la Marca de Certificación debe cumplir las siguientes condiciones:

1) El Certificado de Conformidad deberá aparecer siempre completo, a tenor literal, no siendo posible suprimir conceptos, logotipos, o recortar partes del mismo. Debe quedar clara la organización que obtiene la certificación de su sistema de información, expedido por ICDQ, así como especialmente su vigencia, su alcance, su categoría, su fecha de emisión y su validez.

2) Si la organización, área o unidad cuyo sistema de información está certificado, debe entregar a un tercero una copia del Certificado de Conformidad, éste deberá ser una copia fidedigna del mismo que lo reproduzca en su totalidad, no pudiendo enmendarse o suprimirse parte del contenido a proporcionar.

3) No estará autorizada la utilización de marcas de conformidad por parte de organizaciones sin sistemas de información certificados, con independencia de que exista cierta relación o dependencia con alguna otra organización que sí disponga de ellos.

4) Si se produce, o se requiere, un cambio que afecte parcial o totalmente a la identidad legal que ha obtenido la certificación, se debe exponer el caso al Comité de Certificación de ICDQ que lo estudiará y decidirá la forma de abordarlo. En determinados casos puede requerirse elevar una consulta al CCN con el resultado de transferir directamente el certificado a la nueva entidad legal, o bien iniciar un nuevo proceso de certificación.

5) Las organizaciones, áreas o unidades con su sistema de información en proceso de certificación no podrán incluir en sus comunicaciones la marca de certificación con el ENS hasta la finalización del proceso y les haya sido facilitado por ICDQ el correspondiente Certificado de Conformidad con el ENS, que quedará registrado con su referencia identificativa exclusiva.

6) El sello que se muestre corresponderá claramente a la categoría de los sistemas certificados (BÁSICA, MEDIA o ALTA) en función del tipo de auditoría realizado en el proceso de certificación, viniendo ésta asimismo reflejada en el Certificado de Conformidad con el ENS expedido por ICDQ.

7) En material de papelería únicamente se podrá usar la marca de certificación si está claramente asociada a la organización (tal y como aparece en su certificado) y al sistema de información certificado, no pudiendo llegar a interpretarse que podría abarcar a otros sistemas de información que no lo están.

8) En material promocional de cualquier índole (anuncios de prensa, TV, Internet, etc., únicamente se podrá usar la marca de certificación si está claramente asociada a la organización certificada (tal y como aparece en su certificado) y al sistema de información certificado, no pudiendo llegar a interpretarse que podría abarcar a otros sistemas de información que no lo están.

9) El uso conjunto de otras marcas de certificación junto a la de certificación de la conformidad con el ENS, deberá ser analizado caso a caso. Para ello la organización solicitante comunicará por escrito a ICDQ su intención de hacer esta utilización conjunta de marcas. El Comité de Certificación si estima que no entra en contradicción con las normas aquí descritas, informará en su caso al CCN, trasladando la decisión de éste a la unidad u organización certificada.

10) Los sellos de conformidad con el ENS deben reproducirse literalmente, completos, eligiendo el modelo asociado a la categoría del sistema, no estando permitido emplear únicamente el logo genérico del ENS que consta en su interior para denotar que la organización está certificada, ya que se interpreta como un uso incompleto e ilícito.

11) Cuando los sellos de conformidad se ubiquen en una página Web, portal o Sede Electrónica, si se pincha sobre el mismo debe visualizar el Certificado de Conformidad completo.

12) Según se determina en el artículo 38.2 del RD 311/2022, los sujetos responsables de los sistemas de información certificados de conformidad con el ENS darán publicidad en los correspondientes portales de internet o sedes electrónicas a las certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la ITS de Conformidad y en la guía CCN-CERT IC-01/19.

13) Cuando excepcionalmente en un mismo documento se incluyan servicios, tanto amparados como no amparadas por la certificación, se señalarán las actividades no amparadas mediante un asterisco o similar, incluyendo con el mismo tipo de letra que el usado en el cuerpo del documento, en un lugar visible y cercano a la marca, de forma que se perciban en un único golpe de vista, la siguiente leyenda "*los [servicios, productos o sistemas según proceda] marcados no están amparados por la Certificación de conformidad con el Esquema Nacional de Seguridad*". En estos casos, la organización, área o unidad certificada someterá a la consideración de ICDQ los documentos donde piensa colocar la marca, indicando el lugar de su ubicación y los servicios que serán relacionados.

14) La organización certificada no podrá hacer uso de la marca una vez finalizado el periodo de validez del certificado sin su renovación, o después de la entrada en vigor de una suspensión temporal, retirada o renuncia del derecho de uso.

## I.2 Compromisos de la organización

La organización, área o unidad con licencia de uso de la marca de certificación, en calidad de organización certificada, adquiere los compromisos siguientes:

a) Cumplir con todos los requisitos que pueda estipular el esquema de certificación del ENS con relación al uso de las marcas de conformidad y a la información relacionada con los servicios soportados por el sistema de información certificado.
b) Mantener los sistemas de información en el ámbito de la certificación de conformidad con el ENS, para los cuales se ha concedido el derecho de uso de la marca de certificación, conforme a las disposiciones del ENS.
c) Aceptar las decisiones tomadas respecto a la aplicación del presente Esquema de certificación, según las condiciones establecidas en cada caso.
d) Facilitar al equipo auditor todos los medios necesarios para realizar las verificaciones que implica la aplicación del presente esquema de certificación.
e) Utilizar la marca de certificación únicamente en la forma establecida en el presente documento y exclusivamente en relación con su alcance de certificación.
f) Proceder a realizar la solicitud de una auditoría complementaria ante cualquier modificación que se desee hacer al alcance y categoría de los sistemas respecto a los cuales se le haya concedido el derecho de uso de la marca de certificación.
g) Abstenerse de hacer uso de la marca de certificación cuando haya riesgo de confusión con actividades, productos, procesos, servicios, sistemas de información o partes de la organización que no disfruten del derecho de uso de dicha marca de certificación.
h) Informar a ICDQ de cambios en la organización que puedan afectar a los sistemas de información en el ámbito del Esquema Nacional de Seguridad, al alcance, o a la categoría de la certificación.

## I.3 Vigilancia del uso de marcas de certificación por ICDQ

Durante todo el período de validez de la marca de certificación, que para el ENS se establece inicialmente en dos años, ICDQ debe realizar todas las verificaciones consideradas necesarias respecto a su buen uso, o encargar su realización a un tercero, siendo habitual que éstas se lleven a cabo cada 6 meses.

En caso de uso indebido de la marca de certificación, el organismo de certificación a través de su Comité de Certificación puede apercibir inicialmente, pudiendo llegar a suspender o retirar inmediatamente la certificación y el derecho a utilizar la marca de certificación, conforme establece el apartado 13 del presente documento.

La Organización, área o unidad certificada puede apelar la decisión conforme establece el apartado 14.1 del presente documento.

I.4 Renuncia voluntaria al uso de la marca de certificación

La organización, área o unidad certificada puede renunciar a o suspender por un período de tiempo el uso de la marca de certificación, notificándolo por escrito a ICDQ. Ante dichas circunstancias, se le informará respecto a los términos y condiciones para la terminación temporal o definitiva del uso de la marca de certificación.

## I.5 Reproducción de sellos oficiales de certificación

El diseño de los sellos de certificados estará a lo dispuesto por la última versión publicada de la guía técnica CCN-STIC-809, junto a sus anexos, y la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad, y modificaciones posteriores.

Se reproducen a continuación los sellos proporcionados por el CCN, que asimismo pueden descargarse del portal del ENS:


Certificación. Categoría Básica (RD 311/2022)


Certificación. Categoría Media (RD 311/2022)


Certificación. Categoría Alta (RD 311/2022)

| Colores directos | CMYK | RGB | HEXADECIMAL |
|---|---|---|---|
| **Pantone 653C** | C: 82 | R: 55 | 336699 |
| | M: 47 | G: 99 | |
| | Y: 11 | B: 150 | |
| | K: 0 | | |

# ANEXO II. DERECHOS & OBLIGACIONES

Las organizaciones, o sus áreas o unidades, que estén en proceso de certificación de la conformidad de alguno de sus sistemas de información respecto a las disposiciones del Esquema Nacional de Seguridad (en adelante, ENS), o ya dispongan de un certificado en vigor, disfrutarán de una serie de derechos, a la vez que estarán sujetas a una serie de obligaciones, que se detallan en este anexo.

## II.1 Derechos del auditado

1) Una vez obtenida la certificación, hacer uso del sello oficial, o del Certificado de Conformidad con el ENS, o referencia a la condición de organización certificada del ENS, tal y como estipula el anexo "**Uso de Marcas de Certificación**", pudiendo hacer constar dicha condición en los actos derivados de sus competencias y potestades administrativas.

2) Que toda la información que proporcione ICDQ sea tratada como confidencial, sin menoscabo de requerimientos legales o de verificaciones realizadas a ICDQ por parte del Centro Criptológico Nacional (CCN). Se recuerda que puede consultarse información sobre los sistemas certificados del ENS, junto a su categoría, alcance y vigencia, en el portal del ENS del Centro Criptológico Nacional.

3) Conocer los informes que se generen con motivo de las auditorías, incluidas las extraordinarias, como consecuencia del proceso de certificación inicial, de certificaciones sucesivas, o de vigilancia del correcto uso de los certificados obtenidos.

4) Ser informado puntualmente por ICDQ de los cambios que se produzcan tanto en los requisitos y criterios de certificación, como en los procedimientos de evaluación, como de cualquier modificación sustancial del ENS.

5) Solicitar a ICDQ la suspensión temporal voluntaria o retirada de la certificación, en las condiciones que se especifican en el presente documento.

6) Reclamar, si procede, el servicio prestado por IDCQ, como podrían ser las actuaciones parciales o inadecuadas del equipo auditor, mediante la presentación de una queja o reclamación según se indica en el apartado 14.2 del presente documento.

7) Recurrir a las decisiones adoptadas por el Comité de Certificación de ICDQ, o quién adopte la decisión de certificación, presentando una apelación, como también se indica apartado 14.1 del presente documento. Las apelaciones las resuelve o bien el Comité de Imparcialidad, en el caso de haberse constituido, o bien miembros externos que no hayan participado en el proceso; en cualquier momento, la organización puede solicitar a ICDQ la composición actual del Comité de Imparcialidad.

# II.2 Obligaciones del auditado

## en proceso de certificación de conformidad en el ENS

Las unidades u organizaciones en proceso de certificación de alguno de sus sistemas de información deberán cumplir en todo momento las obligaciones previas a la obtención de su certificación de conformidad con el ENS, las cuales son:

1) Cumplir puntualmente las condiciones impuestas por el Comité de Certificación en sus acuerdos.

2) Comunicar a ICDQ los cambios significativos que se proponga llevar a cabo mientras dura el proceso de certificación que pudieran alterar las condiciones de éste.

3) No hacer declaraciones engañosas relacionadas con el proceso de certificación. Tampoco hacer ver que ya se está certificado sin haber finalizado el proceso con una decisión favorable de certificación y la emisión del correspondiente certificado.

4) Enviar en tiempo y forma tanto la documentación, como los acuerdos suscritos, que vaya solicitando ICDQ, necesarios para el avance del proceso de certificación.

5) Cooperar con ICDQ para la correcta realización de las actividades de evaluación en las fechas establecidas, permitiendo el acceso a sus instalaciones y a la información, documentos y registros que avalan el cumplimiento de los requisitos de certificación dispuestos por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y modificaciones posteriores, a las personas debidamente autorizadas y anunciadas por ICDQ. En el supuesto caso de existir alguna información a la que el equipo auditor no pueda acceder si no cuenta con, por ejemplo, una Habilitación Personal de Seguridad (HPS) para determinado grado, debe indicarse, justificando el motivo.

6) Aceptar que se lleven a cabo, si es el caso, las visitas de acompañamiento, determinadas por el Centro Criptológico Nacional (CCN), que se establezcan durante las auditorías, como puede ser para que otras entidades de certificación en proceso de reconocimiento, puedan realizar las prácticas reales necesarias.

7) Aceptar que se incorpore al equipo auditor, bajo la responsabilidad del Auditor Jefe, algún auditor en formación o en prácticas, facilitando así la adquisición de experiencia para una futura cualificación de los mismos.

## con certificado de conformidad en el ENS

Las organizaciones, o sus áreas o unidades, con uno de sus sistemas de información certificados, deberán cumplir en todo momento las obligaciones resultantes de su certificación de conformidad con el ENS, las cuales son:

1) Cumplir en todo momento con los requisitos de certificación que sean aplicables a los sistemas amparados por la certificación, incluyendo la implementación de los cambios adecuados cuando los comunica ICCQ, manteniendo evidencias de su cumplimiento.
2) Cumplir puntualmente las condiciones impuestas por el Comité de Certificación en sus acuerdos.
3) No hacer declaraciones engañosas relacionadas con la certificación.
4) Declarar que está certificado únicamente respecto a los sistemas para los que se le ha concedido la certificación, informando de su categoría y del alcance exacto de su certificación.
5) Abstenerse de cualquier actividad que dañe la credibilidad de ICDQ, o del propio Esquema de Certificación, comunicando cualquier uso indebido de certificados, sellos y marcas de certificación por terceros del que tengan conocimiento, así como de ejercitar cuantas acciones pudieran asistirle en caso de que un tercero use indebidamente o falsifique sus informes, marcas o ~~sellos de certificación y~~ certificados que acreditan la conformidad de sus sistemas respecto al ENS.
6) Mantener en correcto estado de desempeño todos los sistemas de información que determinaron la concesión de la certificación y conservar el equipo suficiente de personas debidamente cualificadas dentro de su alcance.
7) Comunicar con la debida antelación a ICDQ los cambios relevantes que se proponga llevar a cabo en la organización, unidad o área, o en el sistema de información certificado, cuando se prevea o vislumbre que puedan tener implicaciones respecto a la certificación:

- Cambios en la estructura orgánica, situación jurídica, dependencia institucional, etc., como puede ser a raíz de la publicación de nuevos decretos de estructura.
- Cambios en la organización y gestión interna, incluyendo cambios en el personal clave y con responsabilidades en el ámbito de la certificación obtenida, etc.
- Cambios sustanciales en la gestión del sistema de información, como puede ser la sustitución de la mayoría de políticas, normas internas y procedimientos.
- Cambios en los emplazamientos de las diferentes sedes de la organización dentro del alcance de la certificación, especialmente si se modifica la dirección que consta en el certificado otorgado, se traslada algún CPD, o se realiza la migración de éste a la nube.
- Cambios en el sistema de información que soporta los servicios del ENS, si son significativos. Por ejemplo, pasar de máquinas físicas a un entorno virtualizado o empezar a desarrollar software.
- Cambios en los proveedores críticos y la externalización en prestadores de servicios, especialmente si no están certificados conforme al ENS.
- Cualquier otro cambio fundamental que se produjese respecto a las condiciones iniciales en que se realizó la evaluación para conceder la certificación.

Una vez analizados los cambios que se han comunicado, a ICDQ decidirá si conllevan una auditoría extraordinaria limitada al alcance del cambio, o simplemente gestiones administrativas. Un cambio

relevante no notificado por la organización certificada, o su área o unidad, puede representar la suspensión de la certificación en vigor.

8) Informar a ICDQ cuando, por causa de falta de personal, cambio de instalaciones u otro motivo, se presuma que no pueda prestar los servicios soportados por los sistemas de información sujetos a certificación durante determinado periodo, lo que llevaría a incumplir con los requisitos de la certificación, ya sea en parte o en su totalidad, en el alcance certificado.

9) Conservar un registro cronológico de deficiencias en los sistemas de información amparados por la certificación, ya sean detectadas por personal interno o por terceros.

10) Enviar en tiempo y forma cualquier documentación requerida por ICDQ para el mantenimiento de la certificación, incluyendo cualquier información sobre su situación legal, operativa o de otra índole relevante para demostrar su cumplimiento con los requisitos de la misma.

11) Aceptar que se lleven a cabo, si procede, las visitas de acompañamiento por parte del personal evaluador del CCN que se establezca, durante las auditorías de renovación de la certificación, como parte de las posibles actividades necesarias para el mantenimiento del reconocimiento de ICDQ.

12) Aceptar que se incorpore al equipo auditor, bajo la responsabilidad del Auditor Jefe, algún auditor en formación o prácticas, facilitando así la adquisición de experiencia para una futura cualificación de los mismos.

13) Conservar un registro de todas las quejas y reclamaciones conocidas con respecto al cumplimiento de los requisitos de la certificación poniendo tales registros a disposición de ICDQ cuando se le solicite. Tomar y documentar las acciones adecuadas con respecto a tales quejas y reclamaciones, y a las deficiencias que se encuentren en los sistemas que afectan a la conformidad con los requisitos de la certificación. Comunicar inmediatamente a ICDQ las quejas y reclamaciones que se consideren relevantes.

14) A requerimiento de ICDQ, y en relación con quejas y reclamaciones recibidas directamente por éste de ciudadanos o de otras partes relacionadas, que puedan implicar el posible incumplimiento de los requisitos de dicha certificación, adoptar las medidas necesarias, una vez evaluadas, comunicándolas al organismo de certificación. Ignorar dichos requerimientos puede implicar la suspensión o retirada de la certificación.

15) Cumplir en todo momento con todos los requisitos legales y reglamentarios que se hayan establecido, en su caso, para prestar los servicios soportados por los sistemas de información dentro del alcance de la certificación.