OMC
ORGANIZACIÓN MÉDICA COLEGIAL DE ESPAÑA | CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

# Requisitos de procedimiento de certificación de sistemas de receta médica privada electrónica

CGCOM
Septiembre de 2017

# Índice

## 1. Generalidades

El apartado 7.1 de la norma ISO/IEC 17065:2012 impone las siguientes obligaciones generales al organismo de certificación:

a) Operar uno o más esquemas de certificación que cubran sus actividades de certificación;
b) Emplear los requisitos que se encuentran en las normas y en otros documentos normativos especificados[1] para evaluar el sistema de receta médica privada electrónica.
c) Si se requieren explicaciones sobre la aplicación de los documentos del punto anterior para un esquema de certificación específico, estás deben ser formuladas por personas o comités pertinentes e imparciales que cuenten con la competencia técnica necesaria, y el organismo de certificación debe ponerlas a disposición según solicitud.
d) Tener en cuenta las especificidades del sistema de receta médica privada electrónica que se va a evaluar;
e) Asegurar que se cubren ampliamente todos los aspectos relacionados con la actividad de la entidad evaluada; y,
f) Basarse en estándares, especificaciones a disposición del público y/o requisitos regulatorios.

## 2. Solicitud de certificación[2]

El apartado 7.2 de la norma ISO/IEC 17065:2012 impone al organismo de certificación la obligación de obtener toda la información necesaria para completar el proceso de solicitud de certificación de acuerdo con el esquema de certificación pertinente[3]. Como parte de dicha información, el organismo obtiene:

a) El sistema de receta médica privada electrónica que va a certificar;

[1] ISO/IEC 17007 proporciona una orientación para desarrollar documentos normativos adecuados para este propósito.

[2] La solicitud de certificación incluye el supuesto de solicitud para la ampliación del alcance de la certificación, que podría incluir servicios similares, ubicaciones diferentes, etc.

[3] Se puede utilizar una variedad de medios y mecanismos para recopilar esta información en diversos momentos, incluyendo un formulario de solicitud. Esta recopilación de información puede ser de forma conjunta o por separado al completar el acuerdo legalmente vinculante (acuerdo de certificación).

b) Las normas y/ otros documentos normativos para los cuales la entidad evaluada busca la certificación;
c) Las características generales de la entidad evaluada, incluyendo su nombre y dirección de las ubicaciones físicas, los aspectos significativos de sus procesos y operaciones (si así lo exige el esquema de certificación correspondiente) y cualquier obligación legal pertinente;
d) La información general relativa a la entidad evaluada, pertinente para el campo de actividad de certificación para el que se presenta la solicitud, tales como sus actividades, recursos técnicos y humanos, instalaciones de laboratorios y/o inspección, y sus funciones y relaciones en una organización más grande, si se diera el caso;
e) La información relacionada con todos los procesos subcontratados que la entidad evaluada utiliza y que afectarán a la conformidad con los requisitos; si la entidad evaluada ha identificado una o varias entidades legales para prestar sus servicios certificados, el organismo de certificación puede establecer los controles contractuales adecuados sobre las entidades legales en cuestión, si es necesario para una supervisión eficaz; si dichos controles contractuales son necesarios, se pueden establecer antes de proporcionar documentación formal de certificación (ver apartado 2.7 del presente documento);
f) Toda otra información necesaria, de acuerdo con los requisitos de certificación correspondientes, tal como la información para las actividades de certificación inicial y vigilancia, por ejemplo, los lugares donde se prestan los servicios certificados y el personal de contacto en estas ubicaciones.

## 3. Revisión de la solicitud de certificación

El apartado 7.3 de la norma ISO/IEC 17065:2012 impone al organismo de certificación las siguientes obligaciones:

a) Realizar una revisión de la información obtenida (ver apartado anterior) con el fin de asegurarse de que:

    1) La información acerca de la entidad evaluada y del sistema de receta médica privada electrónica es suficiente para realizar el proceso de certificación;

2) Se resuelve cualquier diferencia de entendimiento conocida entre el organismo de certificación y la entidad evaluada, incluyendo el acuerdo con respecto a las normas u otros documentos normativos;
3) Se define el alcance de la certificación[4] solicitada;
4) Se dispone de los medios para realizar todas las actividades de certificación;
5) El organismo de certificación tiene la competencia y la capacidad para llevar a cabo la actividad de certificación.

b) Si el organismo de certificación se basa en las certificaciones que ya ha otorgado a la entidad evaluada, o que ya ha otorgado a otros clientes, para omitir algunas actividades, entonces debe hacer referencia a las certificaciones existentes en sus registros. Si la entidad evaluada lo solicita, el organismo de certificación debe proporcionar la justificación para la omisión de las actividades.

c) No acepten ninguna solicitud para la cual no sea competentes o si no puede realizar un proceso de auditoría. En dicho supuesto, el organismo deberá revisar el contrato con la entidad evaluada, a partir de los resultados del análisis de competencias. En concreto, deberá tener la capacidad de demostrar que es capaz de:

1) Conocer las áreas de actividad de la entidad evaluada y los riesgos de negocio asociados;
2) Definir las competencias necesarias del organismo para que certifique, en relación con el sistema de receta médica privada electrónica, y los riesgos relevantes para la seguridad, las vulnerabilidades y los impactos sobre el sistema evaluado; y
3) Confirmar la disponibilidad de las competencias exigidas.

## 4. Certificación/auditoría

El apartado 7.4 de la norma ISO/IEC 17065:2012 impone las siguientes obligaciones generales al organismo de certificación en materia de auditoría de servicios confiables:

[4] Identificación del servicio para el que se otorga certificación, del esquema de certificación y de las normas y otros documentos normativos, incluida su fecha de publicación, con respecto a los cuales se considera que el servicio es conforme.

a) Disponer de un plan para las actividades de auditoría que permita gestionar las disposiciones necesarias.
b) Asignar personal para realizar cada tarea de auditoría que lleve a cabo con sus recursos internos (consultar el apartado 4.2.1 del documento "Requisitos para organismos de certificación de sistemas de receta médica privada electrónica").
c) Asegurarse de que toda la información y/o documentación necesaria está disponible para llevar a cabo las tareas de auditoría.
d) Ejecutar las actividades de auditoría que lleva a cabo con sus recursos internos y gestionar los recursos subcontratados (consultar los apartados 4.2.1 y 4.2.2 del documento "Requisitos para organismos de certificación de sistemas de receta médica privada electrónica", respectivamente) según el plan de auditoría. El servicio se debe auditar frente a los requisitos cubiertos por el alcance de la certificación y otros requisitos especificados en el esquema de certificación.
e) El organismo de certificación únicamente debe basarse en los resultados de una certificación terminada antes de la solicitud de certificación cuando asume la responsabilidad de los resultados y tiene el convencimiento de que el organismo que realizó la auditoría cumple con los requisitos en materia de personal subcontratado y con aquellos especificados por el esquema de certificación.
f) Informar a la entidad evaluada sobre todas las no conformidades.
g) Si se han detectado una o más no conformidades, y si la entidad evaluada expresa interés en continuar el proceso de certificación, el organismo de certificación debe proporcionar información con respecto a las labores de certificación adicionales necesarias para verificar que las no conformidades se han corregido.
h) Si la entidad evaluada está de acuerdo en completar las labores de certificación adicionales, el proceso que se especifica en el presente apartado 2 se debe repetir para completar las tareas de auditoría adicionales.
i) Los resultados de todas las actividades de certificación deben documentarse antes de la revisión.

## 4.1. Alcance de la auditoría

### 4.1.1. Aspectos generales

La documentación del organismo de certificación deberá incluir las políticas y procedimientos para la implementación de un proceso de auditoría, incluyendo los "listas de comprobación" empleados en la auditoría, y los procedimientos para evaluar la conformidad del sistema de receta médica privada electrónica, con los criterios con los que se lleva a cabo dicha auditoría.

El organismo de certificación deberá asegurar que el alcance y los límites del sistema están claramente definidos en términos de modelo de negocio, organización, instalaciones, activos y tecnología.

El organismo de certificación deberá asegurar que la certificación de los riesgos para la seguridad de la información y el tratamiento del riesgo de la entidad evaluada refleja adecuadamente sus actividades y los límites de sus servicios de receta electrónica.

### 4.1.2. Mandato del equipo auditor

El organismo de certificación deberá definir y comunicar explícitamente a la entidad evaluada el mandato proporcionado al equipo auditor, que deberá requerir que el equipo examine las estructuras, políticas, procedimientos, prácticas, gestión y operativa de la entidad evaluada, y confirme que este cumple con todos los requisitos relevantes en el alcance de la certificación y que se implementan los procedimientos, de manera que se proporcione confianza en el sistema de receta médica privada electrónica.

El organismo de certificación dispondrá de un procedimiento para:

a) Seleccionar auditores y expertos técnicos a partir de sus competencias, formación, calificaciones y experiencia; y,
b) Supervisar el rendimiento de los auditores durante los procesos de auditoría.

### 4.1.3. Metodología de la auditoría

La planificación de la auditoría, y su fecha de realización, deberán ser acordadas con la entidad evaluada. El organismo de certificación puede adoptar

procedimientos de notificación que se adapten a sus necesidades, pero, como mínimo, deberán asegurar que:

a) Se celebra una reunión entre el equipo auditor y la Dirección de la entidad evaluada, en la que el equipo proporciona:

    1) Una indicación escrita u oral relativa a la conformidad del sistema de receta médica privada electrónica, a partir de los criterios con los que se ha realizado la auditoría; y,
    2) La oportunidad de preguntar acerca de las conclusiones y sus fundamentos.

b) El líder del equipo auditor proporciona al organismo de certificación un informe de conclusiones de la conformidad del sistema de receta médica privada electrónica que presta, a partir de los criterios con los que se ha realizado la auditoría.

El organismo de certificación deberá disponer de procedimientos que sean capaces de verificar si la entidad evaluada ya ha establecido, con anterioridad a la auditoría para la certificación de la conformidad, un programa de auditoría o si ha superado otras auditorías externas o certificaciones para diferentes ubicaciones, proporcionando suficientes evidencias del cumplimiento de todos los requisitos relevantes de la ubicación, especificados en los criterios con los que se realizado la auditoría.

Los procedimientos de auditoría del organismo de certificación:

a) No deberán presuponer una forma concreta de implementación de un sistema de receta médica privada electrónica o un formato concreto para la documentación y los registros.
b) Deberán focalizarse en establecer que la entidad evaluada, y el sistema de receta médica privada electrónica que presta, cumplen con los requisitos especificados en los criterios con los que se ha realizado la auditoría.

Si se prevé el uso de técnicas de auditoría asistidas por red[5], la entidad evaluada deberá ser consciente de las posibles implicaciones para la seguridad y la planificación de la auditoría deberá identificarlas cuando se considere apropiado.

[5] Por ejemplo, teleconferencias, reuniones web, comunicaciones interactivas basadas en sitios web y acceso electrónico a distancia a la documentación y/o a los procesos del servicio de confianza.

### 4.2. Tiempo para la realización de la auditoría

El organismo de certificación deberá permitir que los auditores dispongan de suficiente tiempo para implementar todas las actividades relacionadas con la auditoría inicial, la de vigilancia y la de recertificación. La distribución de tiempo deberá tener en cuenta los siguientes factores:

a) El tamaño del alcance del sistema de receta médica privada electrónica (p.ej. el número de sistemas de información empleados, el número de trabajadores, el número de certificados expedidos);
b) La complejidad del sistema de receta médica privada electrónica;
c) El tipo(s) de negocio desarrollado dentro del ámbito del sistema de receta médica privada electrónica;
d) El alcance y la diversidad de la tecnología utilizada en la implementación de los varios componentes del sistema de receta médica privada electrónica;
e) El número de ubicaciones;
f) El rendimiento previamente demostrado del sistema de receta médica privada electrónica;
g) El alcance en la externalización de trabajos y en los acuerdos con terceras partes empleados en el ámbito del sistema de receta médica privada electrónica;
h) Los estándares, especificaciones a disposición del público y requisitos regulatorios aplicables a la certificación; y,
i) Las certificaciones existentes.

El organismo de certificación deberá documentar una justificación sobre la cantidad de tiempo empleado en cualquier auditoría inicial, de vigilancia y de recertificación.

### 4.3. Informe de auditoría

#### 4.3.1. Contenido del informe

El informe de auditoría proporcionado a la entidad evaluada, o a cualquier otra parte que tenga una motivación legal para acceder al mismo, deberá contener la siguiente información:

a) Una explicación de la auditoría, incluyendo un resumen de la revisión del documento y de los estándares, de las especificaciones a disposición del público y/o de los requisitos regulatorios a partir de los cuales se ha desarrollado la auditoría;
b) Una explicación de la auditoría que dé cuenta de análisis del riesgo para la seguridad de la información de la entidad evaluada;
c) El tiempo total empleado para la auditoría y una especificación detallada del tiempo utilizado para la revisión documental, la certificación del análisis del riesgo, la auditoria in situ, y la realización del informe de auditoría; y,
d) Las solicitudes que se han seguido en la auditoría, las razones para su selección, y la metodología empleada, incluyendo una metodología de muestreo y procedimientos de prueba.

### 4.3.2. Detalles del contenido del informe a proporcionar

El informe de auditoría de la entidad evaluada o las conclusiones proporcionadas por el líder del equipo auditor al organismo de certificación deberá contener suficientes detalles para facilitar y suportar una decisión de certificación y deberá contener:

a) Las áreas cubiertas por la auditoría, incluyendo requisitos de certificación e instalaciones auditadas, pistas de auditoría significativas que se han seguido y metodologías de auditoría empleadas;
b) Las observaciones realizadas, tanto positivas como negativas.
c) Los detalles de cualquier no conformidad identificada, suportada por evidencias objetivas y una referencia de estas no conformidades a los criterios con los que se ha realizado la auditoría; y,
d) Comentarios sobre la conformidad de la entidad evaluada, y del sistema de receta médica privada electrónica, a partir de los criterios con los que se realizado la auditoría, juntamente con una declaración clara de no conformidad, y, cuando sea aplicable, cualquier comparativa útil con los resultados de auditorías previas de dicho PSC y del sistema de receta médica privada electrónica que presta.

Los cuestionarios, listas de comprobación, observaciones, registros o notas completas del auditor pueden formar una parte integral del informe de auditoría. Si se emplean estos métodos, los documentos deberán ser enviados por el líder del equipo auditor al organismo de certificación como evidencia que suporte la

decisión de certificación. La información acerca de las muestras evaluadas durante la auditoría debería ser incluida en el informe de auditoría o en otra documentación para la certificación. El informe deberá tener en cuenta la adecuación de la organización interna y los procedimientos adoptados por la entidad evaluada para proporcionar seguridad en los servicios de confianza.

Con el objetivo de proporcionar una base para tomar la decisión que confirma que la entidad evaluada, y el sistema de receta médica privada electrónica auditado cumple con los criterios definidos, los auditores deberán producir informes claros que proporcionen suficiente información para tomar dicha decisión.

## 4.4. Proceso de auditoría

### 4.4.1. Preparación general para la auditoría inicial

El organismo de certificación deberá requerir que la entidad evaluada establezca todos los acuerdos para la realización de la auditoría, incluyendo disposiciones para examinar la documentación y el acceso a todas las áreas, incluyendo las de los subcontratistas, los registros (incluyendo informes internos de auditoría e informes de revisiones independientes de la seguridad de la información) y del personal con el objetivo de auditar, reevaluar la auditoría y resolver quejas.

Con anterioridad a la auditoría in situ, el organismo de la certificación deberá requerir a la entidad evaluada solicitante que proporcione, al menos, la siguiente información:

a) Información general relativa al sistema de receta médica privada electrónica y las actividades que cubre;
b) Información sobre las localizaciones, tamaños y funciones de la entidad evaluada, y de las instalaciones del subcontratista, que proporciona o contribuye a suministrar el sistema de receta médica privada electrónica;
c) Una copia de la documentación de las políticas y prácticas que rigen la provisión y la operativa del sistema de receta médica privada electrónica, y, cuando sea necesario, la documentación asociada como la planificación de la infraestructura de red de TI con todos los sistemas relevantes, manuales e instrucciones para la operativa del sistema de receta médica privada electrónica.

### 4.4.2. Proceso de auditoría

El objetivo de la auditoría es confirmar y certificar que la entidad evaluada, y los servicios de confianza que presta, cumple con los criterios de certificación aplicables.

Con anterioridad a la realización de la auditoría, los auditores deberán revisar qué registros son considerados confidenciales o sensibles para la entidad evaluada de manera que el equipo auditor no pueda examinarlos durante el transcurso de la auditoría. Los auditores deberán juzgar si los registros que pueden ser examinados demuestran que la auditoria es efectiva. Si los auditores concluyen que no se garantiza dicha efectividad, el organismo de certificación deberá informar a la entidad evaluada que la auditoría únicamente se podrá llevar a cabo cuando acepte acuerdos apropiados de acceso a la información confidencial o sensible.

Esta auditoría deberá incluir visitas a las instalaciones de la entidad evaluada. El organismo de certificación deberá estar de acuerdo sobre cuándo y cómo se realiza el proceso de auditoría. Los auditores deberán realizar su auditoría en, como mínimo, dos fases.

#### *4.4.2.1 Fase 1 de la auditoría*

Para preparar la auditoría, los auditores deberán obtener y revisar la documentación de la entidad evaluada y de sus servicios auditados. Además, deberán poner en conocimiento de la entidad evaluada cualquier otro tipo de información y registro que pudiera ser requerido adicionalmente para la verificación realizada durante esta fase de la auditoría, en la que el organismo de certificación también deberá obtener documentación sobre el diseño del sistema de receta médica privada electrónica.

El objetivo de la fase 1 de la auditoría es proporcionar información para planificar la fase 2 a través de la obtención de la comprensión de la estructura y extensión de los servicios auditados de la entidad evaluada. La fase 1 de la auditoría deberá incluir, pero no restringirse a, una revisión documental. Otros elementos que pueden ser incluidos en esta fase 1 son: verificación de los registros relativos a las personas jurídicas; acuerdos que cubran la responsabilidad; relaciones contractuales entre la entidad evaluada y los posibles contratistas que operan o que suministran servicios de subcomponentes; auditorías o certificaciones

internas/externas, revisión de la gestión, y más investigaciones relativas a la auditoría preliminar de los cumplimientos parciales y no cumplimientos auto-declarados.

Los auditores deberán acordar con la entidad evaluada cuándo y dónde se realiza la fase 1 de la auditoría.

Los informes de la fase 1 deberán ser enviados por el líder del equipo auditor al organismo de certificación. Juntamente con la información retenida en el archivo, estos informes deberán contener, como mínimo, la siguiente información:

a) Una descripción de la estructura organizativa de la entidad evaluada, incluyendo el uso realizado y la estructura organizativa de terceros (subcontratistas) que suministran partes de los servicios de confianza que están siendo auditados;
b) Un breve resumen de la revisión documental;
c) Un informe relativo a la auditoría del análisis del riesgo de la seguridad de la información de la entidad evaluada y de sus servicios de confianza que están siendo objeto de auditoría;
d) Una breve certificación del auditor indicando la probabilidad de que se produzca la fase 2 y si, para esta, son necesarios recursos adicionales.
e) El tiempo de auditoría invertido en la revisión documental;
f) Cualquier aspecto preocupante referente a si la entidad evaluada, y el sistema de receta médica privada electrónica objeto de auditoría, cumple los requisitos del criterio de auditoría aplicable; y,
g) La metodología de auditoría empleada en la fase 1.

En todo caso, la revisión documental deberá ser completada antes de iniciar la fase 2 de la auditoría.

Los resultados de la fase 1 de la auditoría deberán ser documentados en un informe escrito que incluya todas las recomendaciones relativas a la planificación para llevar a cabo la fase 2. Las conclusiones de la fase 1, incluyendo la identificación de cualquier aspecto preocupante que pudiera ser clasificado como una no conformidad durante la fase 2 de la auditoría, deberán ser comunicadas a la entidad evaluada.

Para determinar el intervalo temporal entre la fase 1 y 2 de la auditoría, deberán proporcionarse consideraciones a las necesidades de la entidad evaluada para la

resolución de los aspectos identificados durante la fase 1. El cuerpo de certificación también podría necesitar revisar sus acuerdos para la fase 2.

El organismo de certificación deberá poner en conocimiento de la entidad evaluada la planificación de la fase 2 de la certificación de la auditoría y de los otros tipos de información y registros que pudieran ser requeridos para una verificación detallada durante esta segunda fase.

#### *4.4.2.2 Fase 2 de la auditoría*

Esta fase consiste en una auditoría in situ que persigue validar las conclusiones del informe de la auditoría preliminar y completar la auditoría de los servicios auditados de la entidad evaluada contra los criterios de certificación.

Deberá ser llevada a cabo siempre en las instalaciones de la entidad evaluada. A partir de las observaciones documentadas en la fase 1 de la auditoría, los auditores deberán esbozar un plan de auditoría para llevar a cabo la fase 2, cuyos objetivos sean:

a) Confirmar que la entidad evaluada cumple sus propias políticas, objetivos y procedimientos; y,
b) Confirmar que los servicios de confianza implementados se adecuan a los requisitos de los criterios de auditoría aplicables y que son seguidos por las políticas, objetivos y procedimientos.

Para ello, la auditoría deberá centrarse en la recopilación de evidencias de los servicios de confianza que tengan relación con:

a) La implementación de los criterios de auditoría del sistema de receta médica privada electrónica;
b) Los procesos y procedimientos organizativos del sistema de receta médica privada electrónica;
c) Los procesos y procedimientos técnicos del sistema de receta médica privada electrónica;
d) Las medidas implementadas para la seguridad de la información del sistema de receta médica privada electrónica;
e) La seguridad física de las instalaciones relevantes de la entidad evaluada.

### 4.5. Frecuencia de la auditoría

En un periodo de tiempo no superior a dos (2) años se debe realizar una recertificación completa de la auditoría, excepto en el caso que sea requerido por la legislación aplicable o por el esquema comercial aplicados en el presente documento[6].

## 5. Revisión de la información y de los resultados de la certificación

El apartado 7.5 de la norma ISO/IEC 17065:2012 impone al organismo de certificación las siguientes obligaciones en referencia al proceso de revisión de la información y los resultados de la certificación. En concreto:

a) Debe asignar por lo menos a una persona para que revise dicha información y resultados. La revisión se debe realizar por personas que no hayan estado involucradas en el proceso de certificación.
b) Las recomendaciones para una decisión sobre la certificación con base en la revisión se deben documentar, a menos que la revisión y la decisión sobre la certificación se realicen simultáneamente por la misma persona.

## 6. Decisión de certificación

El apartado 7.6 de la norma ISO/IEC 17065:2012 impone al organismo de certificación las siguientes obligaciones en referencia al proceso de decisión de certificación. En concreto:

a) Debe ser responsable de sus decisiones en relación con la certificación y debe conservar la autoridad en tales decisiones;
b) Debe asignar por lo menos a una persona para que tome la decisión de certificación basada en toda la información relacionada con la certificación, su revisión y toda otra información pertinente. La decisión de certificación se debe llevar a cabo por una persona o un grupo de personas (p.ej. un comité) que no hayan estado involucradas en el proceso de certificación/auditoría[7].

[6] En cualquier momento, un tercero designado o un organismo de certificación de la conformidad puede demandar una auditoría de vigilancia.
[7] La revisión y la decisión de certificación se pueden realizar simultáneamente por la misma persona o grupo de personas.

c) La persona o personas, excluyendo los miembros de los comités, asignadas por el organismo de certificación para tomar la decisión sobre la certificación deben ser empleadas o estar bajo contrato con uno de los siguientes:

    1) El organismo de certificación (consultar el apartado 4.1 "Personal del organismo de certificación" del documento "Requisitos para organismos de certificación de sistemas de receta médica privada electrónica");
    2) Una entidad bajo el control organizacional del organismo de certificación (ver el apartado 2.6 d), a continuación)).

d) El control organizativo de un organismo de certificación debe corresponder a uno de los siguientes:

    1) Propiedad total o mayoritaria de otra entidad por parte del organismo de certificación;
    2) Participación mayoritaria por parte del organismo de certificación en la junta de directiva de otra entidad;
    3) Autoridad documentada del organismo de certificación sobre otra entidad en una red de entidades legales (a la cual pertenece el organismo de certificación), vinculada por propiedad o por el control de la junta directiva.

e) Las personas empleadas por, o con contratos con, entidades bajo control de la organización deben cumplir los mismos requisitos que las personas empleadas por, o con contrato con, el organismo de certificación.
f) Deber de notificar a la entidad evaluada la decisión de no otorgar la certificación, debiendo identificar las razones que motivan tal decisión.

Por otra parte, podrá existir tres posibilidades relativas la decisión de certificación:

a) **Certificado:** el sistema de receta médica privada electrónica auditado cumple los criterios y queda certificado como conforme.
b) **Condicionado:** cuando la entidad evaluada supera la auditoría con no conformidades pendientes de ser solucionadas, siempre que estas no impactes en su capacidad de cumplir el servicio previsto. En este sentido, la certificación queda condicionada hasta que se implementen las medidas

correctivas dentro de los tres (3) meses siguientes a la finalización de la auditoría (dependiendo del tipo y criticidad de dichas medidas).

c) **No certificado:** el sistema de receta médica privada electrónica auditado no queda certificado como conforme.

## 7. Documentación de la certificación

El apartado 7.7 de la norma ISO/IEC 17065:2012 impone al organismo de certificación las siguientes obligaciones en materia de documentación de la certificación. En concreto:

a) Debe proporcionar a la entidad evaluada la documentación formal de la certificación que indique claramente o permita la identificación de los siguientes aspectos:

   1) El nombre y la dirección del organismo de certificación;
   2) La fecha en que se otorga la certificación (esta fecha no debe ser anterior a la fecha en la cual se tomó la decisión sobre la certificación);
   3) El nombre y la dirección de la entidad evaluada;
   4) El alcance de la certificación;
   5) El plazo de vigencia o la fecha de expiración de la certificación, si esta expira después de un periodo establecido; y,
   6) Cualquier otra información requerida por el esquema de certificación.

b) La documentación formal de la certificación debe incluir la firma u otra autorización definida de las personas del organismo de certificación a quienes se ha asignado tal responsabilidad.

c) La documentación formal de certificación únicamente se debe emitir después o simultáneamente con las siguientes actividades:

   1) Cuando se ha tomado la decisión de otorgar o ampliar el alcance de la certificación;
   2) Se ha cumplido con los requisitos de la certificación; y,
   3) Se ha completado/firmado el acuerdo de certificación (consultar el apartado 2.1.2 “Acuerdo de certificación” del documento “Requisitos para organismos de certificación de sistemas de receta médica privada electrónica”).

## 8. Repositorio de sistemas certificados

El apartado 7.8 de la norma ISO/IEC 17065:2012 impone al organismo de certificación la obligación de mantener información sobre los servicios certificados que contendrá, por lo menos, los siguientes datos:

a) Identificación del servicio;
b) Normas y otros documentos normativos con los cuales se ha certificado la conformidad; e,
c) Identificación de la entidad evaluada.

Las partes de esta información que es necesario publicar o poner a disposición según solicitud en un repositorio (a través de publicaciones, medios electrónicos u otros medios) están estipuladas en el esquema correspondiente. Como mínimo, el organismo de certificación debe suministrar información, según solicitud, acerca de la validez de una certificación determinada.

## 9. Supervisión

El apartado 7.9 de la norma ISO/IEC 17065:2012 impone al organismo de certificación las siguientes obligaciones en materia de supervisión y monitorización. En concreto:

a) Si el esquema de certificación requiere supervisión, o según se especifica en los apartados c) y d) (a continuación), el organismo de certificación debe iniciar la supervisión del servicio cubierto por la decisión de la certificación de acuerdo con el esquema de certificación.
b) Cuando la supervisión emplea certificación o auditoría, revisión o una decisión de certificación, se deben satisfacer los requisitos indicados en el documento “Requisitos para la auditoría del sistema de receta médica privada electrónica”, y en los apartados 2.5 y 2.6 del presente documento, respectivamente.
c) Cuando se autoriza el uso continuo de una marca de certificación para un servicio, se debe establecer la supervisión, y se deben incluir actividades periódicas de monitoreo para asegurar la continuidad de la validez de la demostración del cumplimiento de los requisitos que afectan a dicho servicio.
d) Se deberá definir un programa periódico de supervisión y recertificación que incluya auditorías in situ para verificar que la entidad evaluada, y el

sistema de receta médica privada electrónica que presta, mantiene su cumplimiento con los requisitos. Se recomienda que, como mínimo, se realice una auditoría de supervisión anual entre medio de las auditorías completas de recertificación.

e) Las siguientes actividades deberán formar parte de la auditoría de supervisión:

   1) Revisión de las acciones emprendidas sobre las no conformidades identificadas durante la auditoría previa;
   2) Revisión de la estrategia de muestreo de diferentes ubicaciones, si en la auditoría previa se aplicó el muestreo;
   3) Revisión de cualquier cambio en la documentación y en la operativa de la entidad evaluada;
   4) Revisión de auditorías internas y revisión por parte de la Dirección;
   5) Tratamiento de quejas;
   6) Uso de marcas/logotipos y/o cualquier otra referencia a la certificación de la conformidad; y,
   7) Revisión de toda declaración pública de la entidad evaluada relacionada con sus operaciones (p.ej. material promocional, sitio web).

f) Las auditorías de vigilancia no necesitan ser, necesariamente, auditorías completas del sistema. Deberán ser planificadas conjuntamente con otras actividades de supervisión y tener en consideración la aplicación previa de una estrategia de muestreo de diferentes ubicaciones.

g) Adicionalmente, el auditor deberá examinar una muestra de los registros relacionados con las operaciones de la entidad evaluada transcurridas durante el periodo temporal comprendido desde la auditoría anterior a la actual;

h) Los informes de supervisión deberán contener información auditada sobre la eliminación de las no conformidades reveladas con anterioridad.

## 10. Cambios que afectan a la certificación

El apartado 7.10 de la norma ISO/IEC 17065:2012 obliga al organismo de certificación a:

a) Comunicar a todos sus clientes cualquier cambio introducido en el esquema de certificación que les afecte. Deberá existir un procedimiento por parte del organismo de certificación para negociar los cambios que afecten a la certificación con cada cliente. Además, también deja bien claro que los procesos de notificación y decisión sobre la certificación serán anteriores a la implementación de las medidas o cambios;
b) Verificar la implementación de los cambios por parte de la entidad evaluada y emprender las acciones requeridas por el esquema.
c) Considerar otros cambios que afectan a la certificación, incluyendo los cambios iniciados por la entidad evaluada, y decidir sobre la acción más adecuada.
d) Las acciones para implementar los cambios que afectan a la certificación deben incluir, según sea necesario, las siguientes actividades:
    1) Certificación/auditoría (consultar el documento "Requisitos para organismos de certificación de sistemas de receta médica privada electrónica");
    2) Revisión (ver el apartado 2.5 del presente documento);
    3) Decisión (ver el apartado 2.6 del presente documento);
    4) Emisión de documentación formal de certificación revisada (ver el apartado 2.7 del presente documento) para ampliar o reducir el alcance de la certificación;
    5) Emisión de documentación de certificación de las actividades de supervisión revisadas (si la monitorización forma parte del esquema de certificación).

e) Los registros (ver el apartado 2.12 a continuación) deben incluir la justificación para excluir cualquiera de las actividades mencionadas.

Los siguientes cambios serán considerados relevantes:

a) Cambios considerables en la documentación de la entidad evaluada;
b) Cambios en las políticas, objetivos o procedimientos de la entidad evaluada que afectan al sistema de receta médica privada electrónica;
c) Cambios relevantes en la seguridad;
d) Inclusión en el alcance un nuevo sistema de receta médica privada electrónica; o
e) Cambios considerables en los sistemas de TI o en los procesos de negocio empleados por la entidad evaluada, incluyendo el traslado de la mayor parte de los sistemas a otra ubicación física.

## 11. Actuación en caso de no conformidades confirmadas

El apartado 7.11 de la norma ISO/IEC 17065:2012 impone al organismo de certificación la consideración y decisión sobre la acción adecuada a emprender en caso de confirmación de una no conformidad con los requisitos de la certificación. En concreto, dicha acción incluirá una de las siguientes posibilidades[8]:

a) Mantener la certificación bajo condiciones especificadas por el organismo de certificación (por ejemplo, incrementar la supervisión);
b) Reducir del alcance de la certificación para eliminar las variantes del servicio no conforme. En este caso, el organismo de certificación debe tomar las acciones especificadas por el esquema de certificación y debe hacer todas las modificaciones necesarias en los documentos formales de la certificación, la información pública, las autorizaciones para el uso de marcas de conformidad, etc., con el fin de asegurarse de que el alcance reducido de la certificación se comunica claramente a la entidad evaluada y se especifica con claridad en la documentación de la certificación y en la información pública;
c) Suspender temporalmente la certificación a la espera de la implementación de acciones remediadoras por parte de la entidad evaluada. En cuyo caso, el organismo de certificación debe asignar a una o más personas para que establezcan y comuniquen a la entidad evaluada:
    1) Las acciones necesarias para finalizar la suspensión y restablecer la certificación de los servicios de acuerdo con el esquema de certificación;
    2) Cualquier otra acción requerida por el esquema de certificación. Estas personas deben ser competentes con respeto a su conocimiento y comprensión de todos los aspectos del tratamiento de las certificaciones suspendidas.

d) Retirar la certificación.

Si la certificación se finaliza (a solicitud de la entidad evaluada), se suspende o se retira, el organismo de certificación debe implementar las acciones especificadas en el esquema de certificación y debe hacer todas las modificaciones necesarias en los documentos formales de la certificación, la información pública, las

[8] Siempre que la acción implementada incluya la certificación, revisión o decisión de certificación, se deben cumplir los requisitos de los apartados 2.4, 2.5 o 2.6, respectivamente.

autorizaciones para el uso de logotipos de conformidad, etc. con el fin de asegurarse de que estos no suministran indicación alguna de que el servicio sigue estando certificado.

Toda certificación, revisión o decisión necesaria para resolver la suspensión, o que se requiera por el esquema de certificación, se debe llevar a cabo de acuerdo con las partes aplicables de los apartados 2.4, 2.5, 2.6, 2.7 c), 2.9 y en el párrafo anterior.

Si se restablece la certificación después de la suspensión, el organismo de certificación debe hacer todas las modificaciones necesarias en los documentos formales de la certificación, la información pública, las autorizaciones para el uso de las marcas de conformidad, etc., con el fin de asegurarse de que existen todas las indicaciones correspondientes de que el servicio sigue estando certificado.

Si se decide reducir el alcance de la certificación como condición para su restablecimiento, similarmente, el organismo de certificación debe hacer todas las modificaciones necesarias en los documentos mencionados en el anterior parágrafo, con el fin de asegurarse de que se comunica claramente la reducción del alcance de la certificación a la entidad evaluada y que esto se especifica con claridad en la documentación de la certificación y la información pública.

## 12. Registros

El apartado 7.12 de la norma ISO/IEC 17065:2012 impone al organismo de certificación las siguientes obligaciones en materia gestión de registros:

a) Conservar los registros que demuestren que se han cumplido eficazmente todos los requisitos del proceso de certificación (los de esta Norma Internacional y los del esquema de certificación) (consultar el apartado 5.3 “Control de registros” del documento “Requisitos para organismos de certificación de sistemas de receta médica privada electrónica”);
b) Preservar la confidencialidad de los registros. Los registros se deben transportar, transmitir y transferir de manera que se asegure la conservación de la confidencialidad (consultar el apartado 2.5 “Confidencialidad” del documento “Requisitos para organismos de certificación de sistemas de receta médica privada electrónica”);
c) Si el esquema de certificación implica la re-certificación completa de los servicios dentro de un ciclo determinado, se deben conservar, como

mínimo, registros del ciclo actual y del anterior. O bien, se deben conservar los registros durante un periodo definido por el organismo de certificación.

## 13. Quejas y apelaciones

El apartado 7.13 de la norma ISO/IEC 17065:2012 impone al organismo de certificación las siguientes obligaciones en materia gestión de quejas y apelaciones:

a) Disponer de un proceso documentado para recibir, evaluar y tomar decisiones acerca de las quejas y las apelaciones. Además, deberá registrar y realizar el seguimiento de la resolución, así como las acciones que se han implementado;
b) Tras la recepción de una queja o apelación, el organismo debe confirmar si tiene relación con las actividades de certificación de las cuales es responsable y, si es así, tratarlas.
c) Realizar el acuse de recibo de una queja o apelación formal.
d) Responsabilizarse de reunir y verificar toda la información necesaria (en la medida de lo posible) para alcanzar una decisión sobre la queja o la apelación.
e) La decisión que resuelve la queja o la apelación debe ser tomada, revisada y aprobada por parte de personas que no estén involucradas en las actividades de certificación relacionadas con dicha queja o apelación.
f) Para asegurarse de que no existe conflicto de intereses, el personal (incluyendo aquel que actúa a nivel directivo) que ha proporcionado consultoría a un cliente, o ha sido empleado de un cliente, no debe ser empleado por el organismo de certificación para revisar ni aprobar la resolución de una queja o una apelación para ese cliente durante los dos años siguientes a la terminación de la consultoría o el empleo.
g) Siempre que sea posible, el organismo debe proporcionar al reclamante una notificación formal sobre el resultado y la finalización del proceso de reclamación.
h) Proporcionar al apelante una notificación formal del resultado y la finalización del proceso de apelación.
i) Emprender las acciones posteriores necesarias para resolver la queja o la apelación.