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

Requerimientos para la auditoría de certificación de los Sistemas de Prescripción y Repositorios de Prescripciones del Sistema de Receta Electrónica privada

Versión 1.2 (Diciembre 2024)

Índice

1 Introducción

En este documento se presentan los requerimientos relacionados con el proceso de auditoría de certificación de los Sistemas de Prescripción y Repositorios de Prescripciones que deseen operar en el Sistema de Receta Electrónica privada.

El documento contiene los objetivos de control que deben cumplir los Sistemas de Prescripción y Repositorios de Prescripciones candidatos a la certificación por el organismo de certificación, y los criterios para la auditoría.

Los objetivos de control se han agrupado en las siguientes categorías:

- Controles funcionales y técnicos.
- Controles de formalización documental.
- Controles de interoperabilidad.
- Controles de protección de datos de carácter personal.
- Controles de seguridad y confidencialidad.

Por su parte, los criterios desarrollan los anteriores objetivos de control, indicando:

- Una descripción detallada del control, incluyendo, en su caso, descripción de mejores prácticas para el cumplimiento del control.
- La documentación acreditativa a presentar en la justificación del cumplimiento.
- El contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles.

Definiciones

Para facilitar la comprensión del presente documento, a continuación, se define el significado de determinadas palabras a los efectos de lo dispuesto en el mismo:

CGCOF: Consejo General de Colegios Oficiales de Farmacéuticos.

CGCOM: Consejo General de Colegios Oficiales de Médicos.

CGCOE: Consejo General de Colegios Oficiales de Odontólogos y Estomatólogos.

CGCOP: Consejo General de Colegios Oficiales de Podólogos de España

CGCOM, CGCOP y CGCOE, serán denominados conjuntamente como, los "**Consejos Generales de Prescriptores**".

CGCOM, CGCOP, CGCOE y CGCOF, serán denominados conjuntamente como, los "**Consejos Generales**".

Sistema de Receta Electrónica Privada/SREP: conjunto organizado de agentes, y de plataformas operadas por los mismos o terceros autorizados que, en el ámbito de la sanidad privada, se relacionan en una solución interoperable en base a unos estándares mínimos exigidos por los Consejos Generales, con el fin de facilitar la prescripción a los pacientes, en un soporte electrónico, por los profesionales legalmente facultados para ello, de medicamentos y productos sanitarios para que puedan ser posteriormente dispensados por un farmacéutico o bajo su supervisión, en cualquier oficina de farmacia del territorio nacional, de manera que queden garantizas las condiciones de interoperabilidad, seguridad en el acceso y transmisión de la información y protección de la confidencialidad de los datos personales, así como el cumplimiento de los requisitos obligatorios para las recetas médicas establecidos en el RD 1718/2010 y el resto de normativa de aplicación.

Sistemas de Prescripción: entidades que voluntariamente decidan participar como prestadoras de serviciosen el SREP, en las condiciones establecidas en el mismo, y dotadas de una Plataforma de Prescripción certificada de acuerdo con el presente documento para integrarse con los estándares mínimos del modelo del SREP, quepermitan, únicamente a los profesionales facultados para ello, la prescripción de recetas electrónicas válidamente emitidas conforme a los estándares mínimos establecidos en el SREP y lo dispuesto en el RD 1718/2010 y el resto de normativa de aplicación.

Repositorios de Prescripciones (o Repositorio): entidades que voluntariamente decidan participar como prestadoras de serviciosen el SREP, dotadas de un repositorio que deberá estar certificado de acuerdo con el presente documento para integrarse con los estándares mínimos del modelo del SREP, donde se almacenen las recetas electrónicas privadas válidamente emitidas en el SREP desde uno o varios Sistemas de Prescripción certificados con la finalidad de posibilitar el acceso a las mismas a todas las oficinas de farmacia del territorio nacional, en las condiciones establecidas por los Consejos Generales para salvaguardar el correcto

funcionamiento del SREP, para su dispensación y resto de funcionalidades previstas en la legislación cuando les sean presentadas por los pacientes en las condiciones legal y reglamentariamente establecidas.

Nodofarma: sistema de nodos de servicios farmacéuticos de titularidad del CGCOFdesde el que se dará servicio al SREP para garantizar la interoperabilidad de los diferentes Repositorios de Prescripciones certificados según el presente documento, para operar en el SREP con todas las oficinas de farmacia del territorio nacional, garantizando con ello el derecho de los pacientes a obtener su tratamiento válidamente prescrito, en todo momento y en todas las oficinas de farmacia, de acuerdo con lo establecido en la legislación, así como garantizar que la dispensación se produce de acuerdo con los procedimientos de homologación establecidos por Consejos Generales para la dispensación, garantizando que se realiza por un farmacéutico habilitado y desde una oficina de farmacia autorizada, y garantizando asimismo la trazabilidad de las actuaciones profesionales en el SREP, a disposición de las autoridades competentes.

2 Objetivos de control de los Sistemas de Prescripción y Repositorios de Prescripciones del Sistema de Receta Electrónica Privada

2.1 Controles funcionales y técnicos

Esta sección identifica los controles funcionales y técnicos mínimos aplicables a los Sistemas de Prescripción y, según proceda al Repositorio, del Sistema de Receta Electrónica Privada.

FT01	Posibilidad de prescribir, en cada receta electrónica, uno o varios medicamentos y productos sanitarios.
FT02	Generación de la relación de medicamentos y productos sanitarios prescritos al paciente.
FT03	Posibilidad de establecer un plan terapéutico en soporte de la prescripción, en base a intervalos de tratamiento definidos no superiores a un año.
FT04	Control de la periodicidad de la dispensación, en prescripción en base a plan terapéutico a intervalos definidos.
FT05	Medidas de control en relación con la prescripción de medicamentos estupefacientes y psicotrópicos.
FT06	Comprobación de la habilitación del colegiado.
FT07	Verificación, cuando resulte procedente, del aseguramiento privado del paciente, y registro de dicha información, para su posterior uso en el acceso a la historia.
FT08	Seguimiento de las dispensaciones del tratamiento prescrito, con posibilidad de su modificación o anulación, atendiendo a cualquier evento o circunstancia sobrevenida en la situación clínica del paciente, así como a criterios de cumplimiento terapéutico, que deberán ser registradas.
FT09	Mecanismos de protección en la dispensación de los tratamientos de especial confidencialidad.
FT10	Impresión de la hoja de información al paciente.
FT11	Remisión telemática de la hoja de información al paciente.
FT12	Comprobación de que la información facilitada es completa y suficiente para los procesos de dispensación.

FT13	Comprobación de la actividad comunicada sobre los casos de uso de dispensación es registrada correctamente en el Repositorio.

2.2 Controles de formalización documental

Esta sección identifica los controles mínimos de formalización documental aplicables a los Sistemas de Prescripción y, según proceda, Repositorios de Prescripciones.

FD01	Contenidos mínimos de la receta electrónica.
FD02	Firma electrónica de la receta electrónica.

2.3 Controles de seguridad y confidencialidad

Esta sección identifica los controles mínimos referidos a la seguridad y confidencialidad de los Sistemas de Prescripción del Sistema de Receta Electrónica Privada, adicionales a las medidas de seguridad de datos de carácter personal.

SC01	Acceso del médico al sistema de receta electrónica.
SC01 bis	Inscripción de los profesionales prescriptores
SC01 ter	Relación de los profesionales prescriptores con el Sistema de Prescripción
SC02	Medidas de seguridad para la receta electrónica.
SC03	Acceso del paciente al Sistema de Receta Electrónica Privada.
SC03 bis	Registro identidad del paciente con anterioridad al acceso al sistema de receta electrónica
SC04	Seguridad del equipo de acceso al sistema de receta electrónica.
SC05	Controles de custodia y conservación segura.
SC06	Controles de disponibilidad 24x7x365 del Sistema de Receta Electrónica Privada.
SC07	Servicio de almacenamiento facilitado por el Repositorio de Prescripciones y los Sistemas de Prescripción

SC08	Seguridad en el acceso facilitado por el Repositorio a NodoFarma.
SC09	Acceso del sistema de farmacia al Repositorio de Prescripciones.

2.4 Controles de interoperabilidad.

Esta sección identifica los controles mínimos en relación con la interoperabilidad de los Repositorios del Sistema de Receta Eelectrónica Privada.

IN01	Aplicación por el Repositorio de las normas de interoperabilidad con NodoFarma.
IN02	Consumo de servicios de autenticación delegada, en caso de sistemas basados en federación de identidad médica.
IN03	Verificación interoperable de certificados.

2.5 Controles de protección de datos de carácter personal

Esta sección identifica los controles mínimos a aplicar en relación con los datos de carácter personal gestionados por los Sistemas de Prescripción y Repositorios de Prescripciones del Sistema de Receta Electrónica Privada.

PD01	Existencia de cláusula de información de protección de datos personales en la hoja de información al paciente.
PD02	Medidas de seguridad derivadas de la confidencialidad de la información almacenada en el Repositorio.

3 Criterios de auditoría

3.1 Controles funcionales y técnicos

3.1.1 [FT01] Posibilidad de prescribir, en cada receta electrónica, uno o varios medicamentos y productos sanitarios

Descripción detallada del control:

En este control se revisa el cumplimiento de esta posibilidad prevista en el artículo 14.1 del RD 1718/2010, en virtud del cual "en la receta médica privada electrónica se podrá prescribir uno o varios medicamentos y productos sanitarios [...]".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos-tipo de recetas electrónicas.
- Ejemplos de las recetas generadas donde bajo un mismo tratamiento al paciente se han prescrito múltiples medicamentos y productos sanitarios.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la expedición de recetas electrónicas donde dentro de un mismo tratamiento al paciente se permite prescribir múltiples medicamentos o productos sanitarios.
- Revisión técnica: se prescriben múltiples medicamentos y productos sanitarios dentro de un mismo tratamiento al paciente y se verifica la documentación resultante.

3.1.2 [FT02] Generación de la relación de medicamentos y productos sanitarios prescritos al paciente

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[1] contenida en el artículo 8.2 del RD 1718/2010, en virtud de la cual "el sistema de receta médica

[1] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

electrónica generará la relación de medicamentos y productos sanitarios prescritos al paciente y deberá incluir, además de los datos de consignación obligatoria que se especifican en el artículo 3, los siguientes:
a) Código o número de identificación de la prescripción de cada medicamento y producto sanitario, que será asignado por el sistema electrónico con carácter único e irrepetible.
b) Información de la relación activa de medicamentos correspondiente a los tratamientos en curso".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Ejemplos tratamientos al paciente con su correspondiente relación de medicamentos y productos sanitarios.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos donde dentro de un mismo tratamiento al paciente se permite prescribir múltiples medicamentos o productos sanitarios.
- Revisión técnica: se prescriben múltiples medicamentos y productos sanitarios dentro de un mismo tratamiento al paciente, y se verifica la documentación resultante.

3.1.3 [FT03] Plan terapéutico en soporte de la prescripción

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[2] contenida en el artículo 8.3 del RD 1718/2010, en virtud de la cual "los medicamentos y productos sanitarios serán prescritos según el plan terapéutico establecido [...]".

[2] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Ejemplos de planes terapéuticos.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para el establecimiento de planes terapéuticos y sus limitaciones.
- Revisión documental: el modelo de datos permite el establecimiento de controles para implementar las limitaciones establecidas reglamentariamente en relación con el plan terapéutico, en especial en relación con prescripción de medicamentos estupefacientes.
- Revisión documental: existen ejemplos de planes terapéuticos con sus correspondientes limitaciones en cuanto a los medicamentos y productos sanitarios prescritos.
- Revisión técnica: se crea un plan terapéutico de prueba al auditor, con múltiples medicamentos o productos sanitarios, y sus correspondientes limitaciones, y se verifica la documentación resultante en el sistema.

3.1.4 [FT04] Control de la periodicidad de la dispensación, en prescripción en base a plan terapéutico a intervalos definidos

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[3] contenida en el artículo 8.3 del RD 1718/2010, en virtud de la cual "los medicamentos y productos sanitarios serán prescritos según el plan terapéutico establecido, en base a intervalos de tratamiento definidos que no podrán ser superiores a un año […].
No obstante, cada dispensación no podrá superar un mes de duración máxima de tratamiento, salvo que el formato del medicamento o producto sanitario que deba ser dispensado conforme a la

[3] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

prescripción corresponda a un periodo de tratamiento superior según su ficha técnica".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Descripción del interfaz y casos de uso de la dispensación
- Modelos de datos correspondientes a la aplicación de prescripción.
- Ejemplos de planes terapéuticos.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para el establecimiento de planes terapéuticos y sus intervalos.
- El interfaz y casos de uso de la dispensación permite dispensar sólo las prescripciones "dispensables" en un momento dado.
- Revisión documental: el modelo de datos permite el establecimiento de controles para hacer cumplir los intervalos establecidos en el plan terapéutico.
- Revisión documental: existen ejemplos de planes terapéuticos con sus correspondientes intervalos en cuanto a los medicamentos y productos sanitarios prescritos.
- Revisión técnica: se crea un plan terapéutico de prueba al auditor, con múltiples medicamentos o productos sanitarios, y sus correspondientes intervalos, y se verifica la documentación resultante en el sistema. Se verifica que desde el sistema de dispensación sólo pueden dispensarse las recetas "dispensables" para un periodo dado.

3.1.5 [FT05] Medidas de control en relación con la prescripción de medicamentos estupefacientes y psicotrópicos

En relación con los medicamentos **estupefacientes**, el artículo 8 del RD 1675/2012, en sus apartados 1, 2 y 4, señala que "En cada receta de estupefacientes **se podrá prescribir un solo medicamento**"; "La prescripción formulada en una receta oficial de estupefacientes podrá amparar como máximo la medicación precisa para tres meses de

tratamiento y sin superar un total de cuatro envases" y "El prescriptor entregará al paciente la receta junto a la hoja de información…".

En relación con las sustancias y preparados medicinales **psicotrópicos**, este control revisa el cumplimiento de la obligación contenida en el artículo 17.Dos del RD 2829/1977, sobre que "Los preparados (especialidades farmacéuticas o fórmulas magistrales) que contengan sustancias en las Listas II, III y IV, […] habrán de cumplir en su prescripción y para su dispensación los siguientes requisitos en la receta médica: a) […] Si se tratara de especialidades farmacéuticas, **sólo podrá dispensarse un ejemplar por receta**, y b) No deberán prescribirse en una misma receta médica otros preparados junto con los que contengan sustancias de dichas Listas."

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Ejemplos de planes terapéuticos con medicamentos estupefacientes y psicotrópicos.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para el establecimiento de planes terapéuticos y sus limitaciones referidas a estupefacientes.
- Revisión documental: el modelo de datos permite el establecimiento de controles para implementar las limitaciones establecidas reglamentariamente en relación con el plan terapéutico, en especial en relación con prescripción de medicamentos estupefacientes.
- Revisión documental: existen ejemplos de planes terapéuticos con sus correspondientes limitaciones en cuanto a los estupefacientes.
- Revisión técnica: se crea un plan terapéutico de prueba al auditor, con medicamentos estupefacientes, y se verifica la documentación resultante en el sistema.
- Revisión técnica: El auditor verifica la imposibilidad de materializar recetas médicas por parte del Sistema de Prescripción que contengan:

  - Más de 4 envases de un medicamento estupefaciente.
  - Un tratamiento superior a 3 meses de un medicamento estupefaciente.
  - Más de 1 medicamento psicotrópico
  - La prescripción de un medicamento psicotrópico o estupefaciente junto a otros medicamentos.
- NOTA: Aclarar que esta revisión hace referencia a la imposibilidad de realizar esos condicionantes en una misma receta. No obstante en una misma visita el prescriptor puede crear más de una receta para el mismo paciente.

3.1.6 [FT06] Comprobación de la habilitación del colegiado

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación contenida en el artículo 8.1 del RD 1718/2010, en virtud de la cual "El prescriptor ha de acreditar su identidad".

Previamente a permitir la prescripción electrónica, debe comprobarse la habilitación del colegiado utilizando para ello el servicio de cada Consejo General de Prescriptores (Médicos, Dentistas o Podólogos), que permite validar a un colegiado.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión técnica: se muestra al auditor el funcionamiento del servicio de habilitación de colegiados con los diferentes Consejos Generales de Prescriptores (Médicos, Podólogos y Dentistas), según corresponda en función de si se quiere certificar el Sistema de Prescripción para ser ofrecido a uno o varios de los tipos de profesionales prescriptores anteriormente indicados, en la URL habilitada para ello.
- Revisión técnica:
  a) para el cumplimiento con el Registro de profesionales del CGCOM el auditor revisará la inclusión en el log o elemento técnico de la plataforma, que son registrados los datos suficientes para identificar la

transacción, incluyendo además el hash devuelto por dicho Registro de CGCOM, que será verificable por la herramienta aportada

b) Deberá verificar que no existen transacciones cuya fuente no sea el Registro de CGCOM (transacciones vacías, hash no válido o sin hash)

3.1.7 [FT07] Verificación del aseguramiento privado del paciente, y registro de información del aseguramiento privado del paciente, para su posterior uso en el acceso a la historia

Descripción detallada del control:

En este control, que es optativo, se revisa el cumplimiento de la posibilidad de verificar, cuando resulte procedente, el aseguramiento privado del paciente, y registro de dicha información para su posterior uso en el acceso a la historia clínica electrónica. El registro de esta información es voluntario por parte del paciente.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Ejemplos de prescripciones expedidas a asegurados privados.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la verificación y registro del aseguramiento privado del paciente.
- Revisión documental: existen ejemplos de receta electrónica vinculados a un registro de aseguramiento privado.
- Revisión técnica: se crean recetas asociadas a aseguramiento privado y se recuperan a partir de una búsqueda por número de asegurado o similar.

3.1.8 [FT08] Seguimiento de las dispensaciones del tratamiento prescrito

Descripción detallada del control:

En este control, de aplicación únicamente a los Sistemas de Prescripción, se revisa el cumplimiento de la obligación[4] contenida en el artículo 8.4 del RD 1718/2010, en virtud de la cual "el sistema posibilitará al prescriptor el seguimiento de las dispensaciones del tratamiento prescrito y permitirá en el transcurso del tratamiento, informando al paciente, su modificación o anulación, atendiendo a cualquier evento o circunstancia sobrevenida en la situación clínica del paciente, así como a criterios de cumplimiento terapéutico".

Asimismo, se revisa el cumplimiento de la obligación[5] contenida en el artículo 9.5 del RD 1718/2010, en virtud de la cual "cuando el farmacéutico sustituya un medicamento prescrito de conformidad con los criterios legales vigentes, introducirá en el sistema la causa de dicha sustitución, quedando registrado el código del medicamento dispensado. Esta sustitución quedará registrada en el sistema electrónico para posibilitar su consulta por el prescriptor. De la misma forma se actuará en supuestos de sustitución de productos sanitarios".

Finalmente, se revisa el cumplimiento de la obligación[6] contenida en el artículo 9.6 del RD 1718/2010, en virtud de la cual "el sistema electrónico permitirá que el farmacéutico bloquee cautelarmente la dispensación de un medicamento prescrito cuando se aprecie la existencia de error manifiesto en la prescripción, inadecuación de ésta a la medicación concomitante, alerta de seguridad reciente o cualquier otro motivo que pueda suponer un riesgo grave y evidente para la salud del paciente. Esta circunstancia se comunicará de forma telemática al

[4] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

[5] El artículo 8.4 del RD 1718/2010, que resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010, exige a los prescriptores el seguimiento de las dispensaciones, para lo que se aplicarán aquellas disposiciones establecidas en el artículo 9 del RD 1718/2010, que, por no estar relacionadas con aspectos relativos a la financiación pública de los medicamentos y productos sanitarios, sean extrapolables al ámbito de la receta médica privada electrónica

[6] El artículo 8.4 del RD 1718/2010, que resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010, exige a los prescriptores el seguimiento de las dispensaciones, para lo que se aplicarán aquellas disposiciones establecidas en el artículo 9 del RD 1718/2010, que, por no estar relacionadas con aspectos relativos a la financiación pública de los medicamentos y productos sanitarios, sean extrapolables al ámbito de la receta médica privada electrónica.

prescriptor. El farmacéutico informará sobre dicho bloqueo al paciente.

El prescriptor deberá revisar la prescripción bloqueada cautelarmente procediendo a su anulación o reactivación según considere".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Descripción del interfaz establecido con el sistema de dispensación.
- Ejemplos de informaciones de dispensación recibidas y, en su caso, modificaciones o anulaciones del tratamiento, también para dispensación o anulación parcial.
- Ejemplos de informaciones de sustituciones y bloqueos realizados desde los sistemas de dispensación.
- Ejemplos de información al paciente, para la verificación de la composición, contenido y formato codificado del código DataMatrix.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la recepción de información para el seguimiento de la dispensación, así como para la realización de modificaciones en el tratamiento, o su anulación.
- Revisión documental: el funcional de la aplicación considera elementos de interfaz y casos de uso para la recepción de información que permita el seguimiento de la dispensación por parte del sistema prescriptor.
- Revisión documental: el funcional de la aplicación considera elementos de interfaz y casos de uso para la consulta de información sobre sustituciones realizadas por los sistemas de dispensación, indicando el medicamento de sustitución.
- Revisión documental: el funcional de la aplicación considera elementos de interfaz y casos de uso para la recepción de información sobre bloqueos realizados por los sistemas de dispensación, quedando a disposición del sistema prescriptor información y observaciones sobre el bloqueo

- Revisión técnica: se expide una receta electrónica de prueba al auditor, se dispensa y se verifica la recepción de la información sobre la dispensación en el Sistema/Repositorio de prescripciones.
- Revisión técnica: se modifica un tratamiento.
- Revisión técnica: se anula un tratamiento.
  Revisión técnica: se expide una receta electrónica de prueba al auditor, se bloquea desde el sistema de dispensación y se observa la información que dispone el prescriptor sobre el bloqueo realizado (incluyendo observaciones sobre el bloqueo).

3.1.9 [FT09] Mecanismos de protección en la dispensación de los tratamientos de especial confidencialidad

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[7] contenida en el artículo 8.5 del RD 1718/2010, en virtud de la cual "el paciente podrá solicitar en el momento de la prescripción, protección y confidencialidad en la dispensación de algún tratamiento. En estos casos el tratamiento se diferenciará para la dispensación, pudiéndose realizar a través de receta en soporte papel o a través de los procedimientos que se determinen por las Administraciones sanitarias".

En este control se revisa el cumplimiento del uso de un código PIN para consultar las prescripciones en las que paciente ha solicitado una confidencialidad especial del tratamiento.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Descripción del interfaz establecido con el sistema de dispensación.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Ejemplos de prescripciones con protección y confidencialidad en la dispensación.

[7] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la protección y confidencialidad en la dispensación de un medicamento, todo ello con información al paciente.
- El interfaz establecido con el sistema de dispensación incorpora un mecanismo electrónico que permite ocultar a la farmacia, y a voluntad del paciente, una determinada receta (mediante un pin elegido o informado al paciente).
- Revisión técnica: se muestra al auditor el funcionamiento del sistema de prescripciones en caso de tratamientos farmacológicos que desea que permanezcan en la confidencialidad.

3.1.10 [FT10] Impresión de la hoja de información al paciente

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación contenida en el artículo 3.1 del RD 1718/2010, en virtud de la cual "las recetas médicas, públicas o privadas […] deberán ser complementadas con una hoja de información al paciente, de entrega obligada al mismo, en la que se recogerá la información del tratamiento necesaria para facilitar el uso adecuado de los medicamentos o productos sanitarios prescritos", así como de la obligación[8] contenida en el artículo 8.6 del RD 1718/2010, en virtud de la cual "al efectuar la prescripción mediante el sistema de receta electrónica, se imprimirá y deberá ser entregado al paciente un documento de información del tratamiento prescrito"; obligaciones que vienen moduladas además por lo establecido en el artículo 14.3 del RD 1718/2010, en virtud del cual "el prescriptor podrá realizar la impresión de la hoja de medicación activa, en función de las características del sistema implantado".

Adicionalmente se hace necesario asegurar que la Hoja de Información al paciente contenga, al menos la siguiente información, al objeto de facilitar los procesos de dispensación en farmacia:

[8] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

- Los datamatrix de las prescripciones o recetas activas.
- Los identificativos de Repositorio y acceso legibles, para el caso de que el datamatrix no lo sea.
- Los identificativos de Prescripción o receta legibles, por la misma razón.
- El código del producto prescrito, o la composición en el caso de fórmulas magistrales o vacunas sin código nacional.
- Código de barras conteniendo una Primary Key y el código identificativo del Sistema de Prescripción desde el cual se ha emitido la Hoja de Información al paciente con el siguiente formato:

  IDXXXX/idEntidadSanitaria

  Siendo:

  - ID: Literal fijo
  - XXXX: Primary Key (Clave principal) Nº secuencial del sistema de prescripción definido por la BBDD del CGCOM
  - iDEntidadSanitaria: Cadena de caracteres única de tamaño 64 caracteres definida por el CGCOM

Este código sirve para que desde Nodofarma se valide la certificación del Sistema de Prescripción.

- Código (ID_HIP) que identifique unívocamente las hojas de información al paciente con el siguiente el formato:

  YYYYYYIDXXXX

  Siendo:

  - YYYYYY. Código alfanumérico de 6 posiciones
  - IDXXXX. Código definido en el punto anterior

Este código permite utilizar la HIP como sistema en el que se basa la dispensación en contingencia, cuando la oficina de farmacia no tiene conectividad.

Finalmente, la HIP debe contener la siguiente leyenda: "Esta hoja de información ha sido generada empleando el Sistema y/o Repositorio de Prescripción de [.....][9]"
Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos-tipo de documento de información al paciente y, en su caso, de hoja de medicación activa.
- Ejemplos de documentos de información al paciente y, en su caso, de hojas de medicación activa.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la expedición de documentos de información al paciente y, en su caso, de hojas de medicación activa.
- Revisión documental: existen ejemplos de documentos de información al paciente y, en su caso, de hojas de medicación activa.
- Revisión técnica: se expide una receta electrónica de prueba al auditor, y se verifica la producción y entrega del documento de información al paciente y, en su caso, de la hoja de medicación activa.
- Revisión documental: La HIP deberá identificar (logo o denominación) del titular de la certificación del Sistema de Prescripción y/o Repositorios de Prescripciones en el SREP emitida por el CGCOM, de acuerdo con la Prohibición del uso de los Sistemas de Prescripción y/o Repositorios de Prescripciones certificados sin identificación de la entidad titular de la certificación, de acuerdo con el apartado 15 d) del documento de *Requisitos de procedimiento de certificación de los Sistemas de Prescripción y Repositorios de Prescripciones del Sistema de Receta Electrónica Privada*.

3.1.11 [FT11] Remisión telemática de la hoja de información al paciente

Descripción detallada del control:

[9] NOTA: Este sistema tiene que ser uno de los homologados por los CGCOM.

En este control se revisa el cumplimiento de la posibilidad[10] contenida en el artículo 8.6 del RD 1718/2010, en virtud de la cual "en el caso de personas que acrediten situación de discapacidad que impida o dificulte el acceso al contenido de los documentos referidos en el apartado anterior, las autoridades sanitarias competentes, en función de las características del sistema de receta electrónica implantado, promoverán la incorporación de las herramientas que permitan a estos pacientes recibir la información en formato digital accesible, por medio de envío a la dirección de correo electrónico que indiquen u otra vía o canal idóneo a este propósito".

Adicionalmente se hace necesario asegurar que la Hoja de Información al paciente contiene al menos la siguiente información de cara a facilitar los procesos de dispensación en farmacia:

- Los datamatrix de las prescripciones o recetas activas.
- Los identificativos de Repositorio y acceso legibles, para el caso de que el datamatrix no lo sea.
- Los identificativos de Prescripción o receta legibles, por la misma razón.
- El código del producto prescrito, o la composición en el caso de fórmulas magistrales o vacunas sin código nacional.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos-tipo de documento de información al paciente y, en su caso, de hoja de medicación activa, en formato digital adaptado.
- Ejemplos de documentos de información al paciente y, en su caso, de hojas de medicación activa, en formato digital adaptado.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la expedición de documentos de información al

[10] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

paciente y, en su caso, de hojas de medicación activa, en formato digital adaptado.
- Revisión documental: existen ejemplos de documentos de información al paciente y, en su caso, de hojas de medicación activa, en formato digital adaptado.
- Revisión técnica: se expide una receta electrónica de prueba al auditor, y se verifica la producción y entrega del documento de información al paciente y, en su caso, de la hoja de medicación activa, en formato digital adaptado.

3.1.12 [FT12] Comprobación de que la información facilitada es completa y suficiente para los procesos de dispensación

Descripción detallada del control:

El Repositorio de Prescripciones facilita la información completa para orientar al paciente sobre prescripciones y dispensaciones, para en caso necesario resolver sus dudas sobre plazos y proceso en relación con su medicación.

Superar este requisito supone superar un proceso de prueba conjunto con Nodofarma (ver a continuación "documentación acreditativa").

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Descripción del interfaz y casos de uso de la dispensación.
- Informe positivo emitido por Nodofarma de haber superado las pruebas de los casos de uso de la dispensación.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera el interfaz y casos de uso de la dispensación, y en concreto la respuesta estipulada en consultas de prescripciones y dispensaciones.
- Revisión técnica: se obtiene un informe positivo por parte de Nodofarma de haber superado al menos las siguientes pruebas:

- Se realizan consultas de prescripciones desde el sistema de dispensación, y se devuelven las prescripciones en los estados acordados en el interfaz de dispensación:
  - 0 - Dispensable a futuro (para los Sistemas de Prescripción de prescripción que contemplen esta posibilidad)
  - 1- Dispensable
  - 2 - Bloqueada cautelarmente
  - 5 - Caducada
  - 8 - Dispensada parcialmente
  - 9 - Fórmula Magistral en elaboración (sólo si el ID-Farmacia coincide con el ID-Farmacia que solicitó la acción de "Fórmula Magistral en elaboración".
- Se realizan consultas de dispensaciones desde el sistema de dispensación, y se devuelven las prescripciones dispensadas en los estados acordados en el interfaz de dispensación:
  - 3 - Dispensada
  - 4 - Dispensada con sustitución
  - 8 - Dispensada parcialmente
  - 10 – Dispensada parcialmente con sustitución

3.1.13 [FT13] Comprobación de que la actividad sobre los casos de uso de la dispensación es registrada correctamente en el Repositorio

Descripción detallada del control:

La actividad de las pruebas de dispensación realizadas (ver control anterior en relación con el sistema de prescripciones) se registra correctamente en el Repositorio para su posterior uso y control. Por tanto, este control es dependiente de la ejecución del anterior.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Descripción del interfaz y casos de uso de la dispensación.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera el interfaz y casos de uso de la dispensación, y en concreto registra en base de datos los estados e informaciones que provienen de las acciones realizadas sobre las recetas.
- Revisión técnica: se realizan consultas de prescripciones y dispensaciones, y se comprueba que se son procesadas las acciones del Sistema de Dispensación en su comunicación con el sistema de prescripciones, y en concreto:
    1. Una receta en estado dispensable se puede dispensar. En caso de disponer de varios envases prescritos se permite dispensar un número de envases menor que el total ("dispensación parcial").
    2. Una receta dispensable se puede sustituir.
    3. Una receta dispensable se puede bloquear cautelarmente.
    4. Una receta dispensable, que consiste en una fórmula magistral, se puede informar desde una farmacia que ha sido solicitada en la misma para su elaboración.
    5. Una receta dispensada se puede anular, siempre que la acción se realice desde la misma farmacia que la dispensó y no haya trascurrido más de diez días desde la dispensación.
    6. Una receta que ha sido informada que está en elaboración por una farmacia, se puede anular.
    7. En caso de haber habido una contingencia, se pueden recibir acciones de dispensación en contingencia desde las farmacias.

- Revisión técnica: se realizan consultas de prescripciones y se comprueba que se han almacenado correctamente la información correspondiente a las acciones de la farmacia:
    - En cualquier caso, se almacena el identificador de la acción, el de la Versión SW del Nodo y del Repositorio que han intervenido
    - En la dispensación:
        - Si el número de envases dispensados coincide con el total, el estado de la receta cambia a 3 – Dispensada.
        - Se almacena el número de envases dispensados, que tiene que ser igual o menor que el número de envases prescritos.
        - Si el número de envases dispensados es menor que el de prescritos, el estado de la prescripción pasa a 8 - "dispensado parcialmente", llevando la prescripción correctamente la contabilización del número de envases pendientes para

dispensar (y este número es correcto aun cuando se realicen múltiples dispensaciones parciales y/o anulaciones sucesivas de las mismas).

- En una sustitución:
  - Si se sustituye el total de envases prescritos el estado de la receta cambia a 4 "Dispensada con Sustitución",
  - Si se sustituyen menos envases de los totales prescritos el estado de la receta cambia a 10 – Dispensado Parcialmente con sustitución.
- En una anulación, el estado de la receta retorna a 1 – "Dispensable" (o a 5 – "Caducada" si ha trascurrido el plazo de 10 días),
- En un bloqueo cautelar el estado cambia a 2 "Bloqueada cautelarmente".
- En el caso de que desde una farmacia se informe que se inicia la elaboración de una fórmula magistral, el estado de la receta pasa a 9 "Fórmula Magistral en Elaboración". Y si se solicita la anulación de este estado, la receta retorna a 1 – "Dispensable" (o a 5 – "Caducada" si ha trascurrido el plazo de 10 días).
- En caso de que se reciba una dispensación en contingencia, además de adherirse a las especificaciones técnicas que hayan sido acordadas en el momento de la certificación:
  - Si las validaciones oportunas dan un resultado correcto, la receta queda en el mismo estado que si la dispensación se hubiera producido con normalidad (ver arriba el punto referido a la dispensación).
  - Si el resultado es incorrecto, queda registrado en el sistema de prescripción los datos de la dispensación en contingencia y el motivo del error.

3.2 Controles de formalización documental

3.2.1 [FD01] Contenidos mínimos de la receta electrónica

Descripción detallada del control:

En este control se revisan el cumplimiento de las obligaciones de emisión de la receta en soporte electrónico, previstas en los artículos 3.2 y 8.2 del RD

1718/2010, con los datos básicos obligatorios, relativos a paciente, medicamento, prescriptor y fecha de prescripción, así como de la inclusión del código o número de identificación de la prescripción de cada medicamento y producto sanitario, asignado por el sistema electrónico con carácter único e irrepetible; y de la información de la relación activa de medicamentos correspondiente a los tratamientos en curso.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos de datos correspondientes a la aplicación de prescripción.
- Modelos-tipo de recetas electrónicas.
- Ejemplos de recetas electrónicas.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la expedición de recetas electrónicas con los datos e informaciones exigidas.
- Revisión documental: el modelo-tipo de receta electrónica incluye los datos e informaciones exigidas.
- Revisión documental: existen ejemplos de receta electrónica con los datos e informaciones exigidas.
- Revisión técnica: se expide una receta electrónica de prueba al auditor, con los datos e informaciones exigidas, y se verifica la documentación resultante.
- Revisión técnica: Se verifica que el dato relativo a la identificación del paciente contiene un dato con un formato válido (DNI o NIE y para ciudadanos extranjeros el número de pasaporte.)

3.2.2 [FD02] Firma electrónica

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación del prescriptor prevista en el artículo 3.2.c.6º) del RD 1718/2010, en virtud de la cual "la firma será estampada personalmente una vez cumplimentados los datos de

consignación obligatoria y la prescripción objeto de la receta. En las recetas electrónicas se requerirá la firma electrónica, que deberá producirse conforme con los criterios establecidos por la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos", así como artículo 8.1 del RD 1718/2010, que dispone que "el prescriptor […] firmará electrónicamente la prescripción". La referencia a la Ley 11/2007 debe entenderse realizada hoy, a la Ley 39/2015, de 1 de octubre, de procedimiento administrativo común de las Administraciones Públicas (LPAC), que se encuentra alineada con el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

En marzo del 2021 se publicó un documento para clarificar y ampliar los aspectos de este control. El denominado "*Informe relativo a controles de autenticación y firma electrónica de sistema de receta médica privada electrónica*" apuntaba en referencia al control [FD02] sobre el uso de firma electrónica, además de las referencias al Reglamento eIDAS, aquellas a tener en cuenta de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Así, se indicaba que "En ambas leyes se apuesta por la posibilidad de utilizar **diversos sistemas de firma electrónica**, incluyendo sistemas de **firma electrónica ordinaria o no criptográfica**, sistemas de **firma electrónica avanzada** (con certificado cualificado) y sistemas **de firma electrónica cualificada"**. Además se incluía que "La decisión sobre el sistema de firma electrónica a utilizar no es libre, sino que se debe adoptar conforme a lo establecido de forma obligatoria por el ENS [Esquema Nacional de Seguridad].

Así mismo, se exigía que "cuando se haga uso de un sistema diferente de la firma electrónica" [con certificado], el sistema utilizado "deberá apoyarse necesariamente en **una previa identificación electrónica de nivel medio** por parte del profesional […] y aportar garantías adiciones para la integridad y el no-repudio de la receta expedida".

Finalmente se indicaba que "Podrán firmarse diversas recetas durante una única sesión de autenticación, siempre que la misma tenga una duración máxima que impida la efectiva suplantación de identidad del firmante. Dicha duración máxima no debe superar los 60 minutos sin justificación adecuada mediante el correspondiente análisis de riesgos".

De acuerdo con lo anterior,este control permite únicamente el uso para la firma electrónica de las recetas mediante alguna de las opciones:

- **Firma electrónica cualificada**, que es aquella firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica[11].
- **Firma electrónica avanzada,** siempre que se base en el uso de un certificado cualificado de firma electrónica, conforme al Reglamento eIDAS y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- **Firma electrónica no criptográfica**, que es aquella firma electrónica que no usa un certificado electrónico, se apoya en una previa identificación electrónica de nivel medio del usuario, aporta garantías adicionales para la integridad y el no-repudio de sus actuaciones, y podrá[12] usarse cuando el sistema de información asociado al procedimiento haya sido categorizado, según el Esquema Nacional de Seguridad, de categoría básica y aquellos de categoría media en los que no sea necesario utilizar otro tipo de firma electrónica.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Modelos-tipo de recetas electrónicas.
- Ejemplos de firmas electrónicas del prescriptor en las recetas electrónicas.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la firma electrónica de los actos del prescriptor.
- Revisión técnica: Empleo de firma electrónica de la receta electrónica, por ejemplo, empleando el carné oficial del Colegio de Médicos correspondiente,

[11] Según definición en el artículo 3.12, del Reglamento EIDAS.

[12] Según indicación del apartado III del Anexo de la Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital.

u otro sistema basado en certificado cualificado, y de acuerdo con las reglas de la política de firma electrónica que resulte aplicable.

- Revisión técnica: Empleo de formatos de firma electrónica, como, por ejemplo, cuando se emplee firma electrónica avanzada, XAdES, CAdES o PAdES.
- Revisión técnica: Cuando se use firma electrónica cualificada o avanzada, revisar que el profesional prescriptor haya firmado electrónicamente la receta con su certificado electrónico de persona física, verificando que los datos (nombre y apellidos) del profesional prescriptor en la receta coincidan con los datos de la persona física identificada en el certificado electrónico cualificado.
- Revisión técnica: Cuando se use firma electrónica ordinaria o no criptográfica, revisar que:
    - Se pueda establecer una relación entre los datos personales (nombre y apellidos) del profesional prescriptor que constan en la receta con la identificación del registro en el acceso a la plataforma electrónica de recetas.
    - La relación entre los datos personales indicada sea íntegra y no pueda ser alterada.
    - Conste como parte del documento de trazabilidad o puedan verificarse los datos del acceso del profesional prescriptor, qué usuario ha accedido a la plataforma y en qué momento.
    - Conste como parte del documento de trazabilidad o pueda verificarse el uso por parte del profesional prescriptor de un segundo factor de autenticación (2FA) para corrobar el acceso inicial a la plataforma.
    - Conste como parte del documento de trazabilidad o pueda verificarse en qué momento se ha realizado la firma de la receta, es decir el momento en que el profesional prescriptor ha dado su consentimiento a firmar la receta. Si este momento supera los 60 minutos desde la última petición de 2FA deberá existir un nuevo 2FA que deberá también constar en el log.

3.3 Controles específicos de seguridad y confidencialidad

3.3.1 [SC01] Acceso del médico al sistema de receta electrónica

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[13] establecida en el artículo 8.1 del RD 1718/2010, en virtud de la cual "el prescriptor ha de acreditar su identidad". Asimismo, se revisa el cumplimiento de la obligación establecida en el artículo 14.2 del RD 1718/2010, en virtud de la cual "el acceso al sistema de receta médica privada electrónica se efectuará […] a través del […], además del certificado electrónico del prescriptor".

Asimismo, de acuerdo con lo establecido en el artículo 18.1 del RD 1718/2010, "el prescriptor se responsabilizará […] del acceso […] para la prescripción electrónica. Las instituciones en las que los prescriptores presten sus servicios pondrán los medios necesarios para que puedan cumplirse estas obligaciones".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Diseño técnico del sistema de autenticación de la aplicación de prescripción.
- Modelos de datos de autenticación intercambiables correspondientes a la aplicación de prescripción.
- Ejemplos de autenticación.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la autenticación del prescriptor.
- Revisión técnica: Se verifica el funcionamiento correcto del sistema de autenticación, mediante un juego de pruebas de certificados, vigentes y revocados, – por ejemplo, correspondientes al carné oficial del Colegio de Médicos correspondiente –, y de acuerdo con las reglas de la política de autenticación electrónica.
- Revisión técnica: Constatación en el log del sistema de la verificación del profesional prescriptor contra el Registro de profesionales del Consejo

[13] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

General correspondiente, incluyendo el momento en que se realiza la verificación y la contestación recibida.

- Revisión técnica:
  a) para el cumplimiento con el Registro de profesionales del CGCOM el auditor revisará la inclusión en el log o elemento técnico de la plataforma, que son registrados los datos suficientes para identificar la transacción, incluyendo además el hash devuelto por dicho Registro de CGCOM, que será verificable por la herramienta aportada;
  b) Deberá verificar que no existen transacciones cuya fuente no sea el Registro de CGCOM (transacciones vacías, hash no válido o sin hash);
  c) Verificación de la validez y utilización de la consulta contra el registro CGCOM dentro del periodo máximo de 24 horas de vigencia de dicha consulta, es decir, que pasadas las 24 horas no puede realizarse ninguna transacción asociada al mismo colegiado consultado sin una nueva validación contra el registro de CGCOM. Para ello, el auditor dispondrá del valor until que debe quedar registrado para cada transacción en el log o elemento técnico de la plataforma.

3.3.2 [SC01bis] Inscripción de los profesionales prescriptores

Descripción detallada del control:

En este control se revisa cómo se realiza la inscripción[14] del profesional prescriptor ante el correspondiente Sistema de Prescripción para disponer del servicio de emisión de recetas en el SREP.

En caso de que el cliente del Sistema de Prescripción sea el usuario final (un **prescriptor individual) de una consulta privada** que contrata directamente el software para la prescripción de recetas electrónicas privadas, el titular del Sistema y/o Repostorio de prescripción deberá **requerir que el registro de dichos profesionales se realice o bien:**

- **Presencialmente**, en las oficinas de la empresa titular del Sistema y/o Repositorio

[14] De acuerdo con el REGLAMENTO DE EJECUCIÓN (UE) 2015/1502 DE LA COMISIÓN de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica

- **con certificado cualificado** de cualquiera de los prestadores de servicios de confianza incluidos en la lista de confianza española[15]; o,
- **con video-identificación** conforme a los requerimientos de SEPBLAC. Este método debe ser auditado para ser aceptado como válido.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Se debe incluir por parte del auditor en el informe qué tipos de registro realiza el Sistema de Prescripción, ya sea uno solo, varios o todos. Y describir y verificar cada uno de ellos.
- Revisión documental de los contratos o términos y condiciones modelo que aplican a los clientes que son profesionales prescriptores individuales de consultas privadas.
- Revisión documental: informe de auditoría técnica que certifique el cumplimiento de las obligaciones que marca SEPBLAC. En particular, aquellos requerimientos técnicos que permitan verificar la autenticidad, vigencia e integridad de los documentos de identificación utilizados y la correspondencia del titular del documento con el cliente objeto de vídeo-identificación.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión técnica de la realización de la opción "**Registro presencial**" ante una oficina de la entidad titular del Sistema de Prescripción.
- Revisión técnica de la realización de la opción "**Registro presencial**" ante una oficina del centro sanitario donde ejerce el usuario (profesional prescriptor) del Sistema de Receta Electrónica.
- Revisión técnica de la realización de la opción "**Registro a distancia mediante un certificado digital cualificado**".
- Revisión técnica de la realización de la opción "**Registro a distancia mediante video-identificación",** siempre que el sistema utilizado esté auditado de acuerdo con la normativa del SEPBLAC, justificando los siguientes aspectos:
    - Indicar el proveedor con quien se realiza.

[15] https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/ES

- Describir el procedimiento, siguiendo los reglamentos de videoidentificación de la entidad SEPBLAC, ya sea asistido o desasistido.
- El auditor justificará cada uno de los puntos del reglamento, incluyendo las oportunas pruebas para ser verificadas por el CGCOM:
    - El **análisis de riesgo** al que se refiere el artículo 32.2 del Reglamento de la Ley 10/2010
    - Los **resultados** de la prueba de eficacia del procedimiento de video-identificación.
    - Los **resultados** de los procedimientos implantados que aseguren i) que el proceso se realiza por el cliente desde un único dispositivo, (ii) que las imágenes y el sonido son inmediatamente transmitidos al sujeto obligado en formato digital, sin alteración y en directo ("streaming") y (iii) que el sujeto obligado procede a la grabación inmediata del proceso de modo que permita su posterior reproducción en secuencia.
    - La **constatación fehaciente de la fecha y hora** de la grabación del proceso de vídeo-identificación, con la aportación del fichero de grabación.
    - **Los requerimientos técnicos para la verificación de la autenticidad, vigencia e integridad de los documentos** de identificación utilizados.
    - La **formación** específica recibida por los operadores congruente con las funciones desempeñadas, y acreditada de conformidad con lo dispuesto en el artículo 39 del Reglamento de la Ley 10/2010.
    - La descripción de la **revisión** de cada grabación para verificar el cumplimiento de las especificaciones establecidas por el documento de autorización de SEPBLAC.
    - La realización de una **fotografía** del documento de identificación no siendo válida una captura de fotogramas del proceso de vídeoidentificación.

3.3.3 [SC01ter] Relación jurídica de los profesionales prescriptores con el Sistema de Prescripción

La prescripción en receta médica, en virtud del art. 79 del Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios y de lo dispuesto en el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación, constituye una actuación sanitaria reservada a unos profesionales sanitarios concretos (médicos, odontólogos y podólogos) y que debe tener lugar de acuerdo con las exigencias y requisitos contenidos en la normativa sanitaria.

La Ley 14/1986 de 25 de abril, General de Sanidad dispone en su art. 24 que las actividades que incidan sobre la salud deberán ser sometidas a limitaciones de carácter administrativo, señalándose que los centros que las presten precisarán autorización administrativa previa" (art. 29). Por su parte, el Real Decreto 1277/2003, de 10 de octubre, por el que se establecen las bases generales sobre autorización de centros, servicios y establecimientos sanitarios, define actividad sanitaria ("conjunto de acciones de promoción, prevención, diagnóstico, tratamiento o rehabilitación, dirigidas a fomentar, restaurar o mejorar la salud de las personas realizadas por profesionales sanitarios") indicando que la autorización sanitaria se orienta a garantizar que el centro o establecimiento reúne los medios técnicos, instalaciones y profesionales necesarios para llevar a cabo la actividad sanitaria (art. 4.2).

Como consecuencia de ello, la prescripción de una receta médica solo puede ser realizada por un **profesional médico en su consulta privada** o por un **profesional médico que mantenga una relación laboral o mercantil con un centro o establecimiento sanitario que cuente con una autorización administrativa** para poder operar, siendo incluido en el Registro General de Centros, Servicios y Establecimientos Sanitarios (REGCESS) del Ministerio de Sanidad del gobierno de España.

Por otra parte, el apartado 3.1. vi) de los "*Términos y condiciones para la prestación de servicios de sistemas y repositorios de prescripción certificados en el sistema de receta electrónica privada" e*stablece que, vi) para poder operar en el SREP el Titular de un Sistema de Prescripción deberá *"Garantizar que los profesionales prescriptores, como Usuarios Finales del SREP, han sido informados para las acciones que se van a realizar como consecuencia de su prescripción de Recetas en*

el mismo, así como los requerimientos establecidos por la normativa vigente en materia de privacidad y protección de datos personales".

Descripción detallada del control:

En este control se revisa qué tipo de relación jurídica se establece entre el profesional prescriptor y el Sistema de Prescripción, una vez superado la identificación y registro y antes de su acceso al Sistema de Prescripción.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Debe constar en el informe del auditor qué tipos posibles de relación jurídica pueden existir entre los profesionales prescriptores y el Sistema y/o Repositorio de Prescripción.
- Contrato modelo que emplea el Sistema y/o Repositorio de Prescripción y que establece cuál es la relación jurídica con el cliente, diferenciando las siguientes situaciones:
    - Cuando el cliente es un profesional prescriptor individual que ejerce su actividad de forma privada contratando directamente para ello, el Sistema y/o Repositorio de Prescripción; y,
    - Cuando el cliente es uno o varios centros sanitarios registrados en el REGCESS que contrata el el Sistema y/o Repositorio de Prescripción para su empleo por la plantilla conformada por distintos profesionales prescriptores que ejercen en el referido centro o centros sanitarios de su titularidad.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión del documento que relaciona al profesional prescriptor con el Sistema de Prescripción, como **usuario final del mismo,** para la emisión de prescripciones a sus pacientes. El documento que establece la relación existente entre el profesional prescriptor y el Sistema de Prescripción son los **términos y condiciones** de uso (o documento de adhesión similar) que debe aceptar el usuario al acceder al Sistema.
    - Se debe aportar como evidencia el documento de Términos y Condiciones de uso (o similar) que debe suscribir el profesional prescriptor como usuario del Sistema de Prescripciones.

- Revisión del documento que relaciona al profesional prescriptor con el Sistema de Prescripción, cuando su titular es un centro sanitario y la **relación con el usuario es laboral o, en su caso, mercantil, para prestación de servicios profesionales como profesional sanitario facultativo prescriptor**. Dicha entidad titular debe ser un centro sanitario autorizado y estar inscrita en el REGCESS (Registro General de centros, servicios y establecimientos sanitarios). El documento a revisar es un contrato laboral o mercantil para los servicios como profesional sanitario.
    - Se debe aportar como evidencia el código de inscripción del centro sanitario en el REGCESS así como una plantilla tipo del contrato laboral o mercantil para los servicios como profesional sanitario.

- Revisión del documento que relaciona al profesional prescriptor con el Sistema de Prescripción, cuando la **relación a través de** una entidad cliente del titular del Sistema de Prescripción. Dicha entidad cliente del titular del Sistema de Prescripción debe ser un centro sanitario autorizado y encontrarse inscrito en el REGCESS (Registro General de centros, servicios y establecimientos sanitarios). El documento a revisar es un contrato laboral para prestación de servicios profesionales como profesional prescriptor con la entidad titular del centro sanitario cliente del titular del Sistema y/o Repositorio de prescripciones. Debe existir, además, un contrato o convenio entre la entidad titular del centro sanitario cliente con el titular del Sistema de Prescripción para la regulación de la prestación del servicio. El profesional prescriptor debe aceptar los términos y condiciones de uso del Sistema de prescripción.
    - El auditor debe verificar que todos los centros sanitarios clientes del titular del Sistema y/o Repositorio de Prescripciones son centros registrados en REGCESS. En caso de que el titular del sistema disponga de muchos centros sanitarios clientes, deberá verificarse un mínimo de 10 centros sanitarios clientes, elegidos al azar.
    - Se deberá aportar el código de inscripción de dicho centro sanitario cliente en el REGCESS, así como una plantilla tipo del contrato laboral o mercantil para prestación de servicios profesionales como profesional prescriptor.

3.3.4 [SC02] Garantía de seguridad de la información de la receta electrónica

Descripción detallada del control:

En este control se revisa la existencia de medidas de seguridad de la información de la receta electrónica, además de la garantía de correcta conservación y confidencialidad de la misma.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Planes y Medidas de seguridad de los Sistemas de Prescripción y Repositorios de Prescripciones.
- Medidas de conservación y de mantenimiento de la confidencialidad de la información.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental de los planes de seguridad de la información de los Sistemas de Prescripción y Repositorios de Prescripciones prescriptores.
- Revisión documental de los planes de conservación y de mantenimiento de la confidencialidad de la información.

3.3.5 [SC03] Acceso del paciente al sistema de receta electrónica

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación establecida en el artículo 14.2 del RD 1718/2010, en virtud de la cual "el acceso al sistema de receta médica privada electrónica se efectuará a través del certificado del DNI electrónico del paciente y en caso de imposibilidad se accederá a través del Documento Nacional de Identidad o en su caso del padre o tutor, además del certificado electrónico del prescriptor".

Esta indicación solo se permite cuando la relación entre el profesional prescriptor y el paciente se realice presencialmente.

Mientras no se produzca la extensión generalizada del DNI-e, este control podrá ser sustituido por medidas compensatorias, debidamente justificadas.

Cuando sea necesario la emisión de una receta electrónica y la relación entre el profesional prescriptor y el paciente no se realice presencialmente, el paciente deberá haber accedido al Sistema y/o Repositorio de prescripción empleando uno de estos métodos:

- Por medio de un **certificado electrónico cualificado** emitido por cualquiera de los prestadores de servicios de confianza incluidos en la lista de confianza española.
- Por medio de un **sistema de video-identificación** en el que se hayan implementado las exigencias de las resoluciones del SEPBLAC.
- Por medio de **credenciales que hayan sido otorgadas al paciente tras** un registro presencial, un acceso con certificado electrónico cualificado o un acceso mediante sistema de video-identificación en el que se hayan implementado las exigencias de las resoluciones del SEPBLAC.

Para el caso de sistema de receta electrónica apoyada en un aseguramiento privado, a efectos del servicio opcional de almacenamiento de la prescripción en la historia clínica del paciente, se podría utilizar, de forma complementaria, cualquier sistema de firma electrónica reconocida que contenga el NIF del paciente y, en su caso, la condición de aseguramiento privado del mismo.

Este control se complementa con el control [IN03], sobre verificación interoperable de certificados electrónicos cualificados, incluidos en la lista de confianza española[16].

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Diseño técnico del sistema de autenticación de paciente, con DNI electrónico o, de forma complementaria, otro sistema de firma electrónica.
- Diseño técnico de autenticación mediante mecanismo alternativo al DNI-e.

[16] https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx

- Modelos de datos de autenticación intercambiables correspondientes a la aplicación de prescripción.
- Ejemplos de autenticación.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: El funcional de la aplicación considera casos de uso y procedimientos para la autenticación del prescriptor y del paciente con DNI electrónico o, en su defecto físico.
- Revisión documental: Existen procedimientos solventes para la identificación del padre o tutor, en el caso de acceso a la receta electrónica de menores de edad o mayores de edad sujetos a tutela.
- Revisión técnica: Se verifica el funcionamiento correcto del sistema de autenticación.

3.3.6 [SC03bis] Registro de la identidad del paciente con anterioridad al acceso al sistema de receta electrónica

Descripción detallada del control:

En este control complementa el control [SC03] se revisa el cumplimiento de los requerimientos de control de acceso establecidos por el Esquema Nacional de Seguridad. En concreto, el apartado 4.2.5 – Mecanismo de autenticación (usuarios externos) – de Anexo II del ENS establece los siguientes requerimientos:

"– [op.acc.5.1] Antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.
– [op.acc.5.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.

- [op.acc.5.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
- [op.acc.5.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.
- [op.acc.5.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.
- [op.acc.5.6] Las credenciales serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.
- [op.acc.5.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.
- [op.acc.5.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.
- [op.acc.5.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso".

Además, para sistemas de nivel MEDIO, como el SREP, se debe cumplir con uno de los siguientes refuerzos (R2 o R3 o R4) y con el refuerzo R5:

"- **Refuerzo R2-Contraseña + OTP.**
- [op.acc.5.r2.1] Se requerirá una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario.

Refuerzo R3-Certificados.
- [op.acc.5.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.
- [op.acc.5.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.
- [op.acc.5.r3.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando un certificado electrónico cualificado.

Refuerzo R4-Certificados en dispositivo físico.

- [op.acc.5.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.
- [op.acc.5.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.
- [op.acc.5.r4.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando certificado electrónico cualificado.

Refuerzo R5-Registro.

- [op.acc.5.r5.1] Se registrarán los accesos con éxito y los fallidos.
- [op.acc.5.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

En caso de delegación del registro de la identidad de los pacientes por parte del titular de los Sistemas y/o Repositorios de prescripción a centros sanitarios, plataformas de software, prescriptores de consultas privadas y cualquier otro actor registrado en el REGCESS, ésta deberá incluirse en el contrato de cesión de software o de prestación de servicios. Además, el contrato deberá incluir las metodologías aceptables para el registro de la identidad del paciente, que deberá ser, como mínimo, una de las siguientes:

1. Presencialmente, en unas instalaciones físicas;
2. A distancia, empleando, para ello, un certificado electrónico cualificado; y,
3. A distancia, empleando un método de videoidentificación que sea conforme a SEPBLAC).

Finalmente, las personas encargadas del registro de la identidad de los pacientes, deben estar debidamente formadas para cumplir con los requerimientos del Anexo II del ENS. Dicha formación debe ser proporcionada por el titular de los Sistemas y/o Repositorios de prescripción a los centros sanitarios, plataformas de software y prescriptores de consultas privadas, en caso de que realicen el registro en sus consultas.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Revisión documental de los procedimientos que regulen las condiciones para el registro de la identidad de los pacientes que quieran acceder al SREP, y que cumplan con las exigencias de seguridad del mecanismo de autenticación marcadas por el Anexo II del Esquema Nacional de Seguridad (apartado 4.2.5 [op.acc.5.1]).
- Revisión documental de los planes de formación de los operadores de registro de la identidad de los pacientes.
- Revisión documental de los modelos de contrato para la verificación de los requerimientos de identificación y registro de la identidad del paciente, y las metodologías empleadas para ello.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión técnica del procedimientos de registro seguidos por los operadores de registro habilitados a tal efecto para cada una de las metodologías de registro de la identidad de pacientes empleada (presencial, mediante certificado electrónico cualificado o con videoidentificación conforme a SEPBLAC)
- Revisión técnica de los registros (logs) para comprobar si se registran los accesos exitosos y fallidos de un paciente y
- Revisión técnica para verificar si el sistema informa al usuario de su último acceso.

3.3.7 [SC04] Seguridad del equipo de acceso al sistema de receta electrónica

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación[17] prevista en el artículo 8.1 del RD 1718/2010, en virtud de la cual "el prescriptor accederá al sistema de receta médica electrónica a través de un equipo integrado en el Sistema de receta electrónica que deberá estar autentificado, garantizándose las comunicaciones cifradas", de acuerdo con las correspondientes políticas de seguridad de comunicaciones electrónicas.

En este control se revisan los mecanismos de seguridad relacionados con el acceso al sistema de prescripción, considerando la necesidad de movilidad geográfica de los prescriptores.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Modelo de seguridad de la aplicación de prescripción.
- Mecanismos de autenticación para el control de acceso.
- Mecanismos de cifrado de comunicaciones.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: Existe un modelo de seguridad robusto y fiable de conexión entre el equipo del prescriptor y la aplicación de prescripción, con mecanismos fuertes de autenticación y cifrado de comunicaciones.
- Revisión técnica: Se verifican los registros de actividad y autenticación de la aplicación de prescripción para comprobar los procedimientos de autenticación del equipo.
- Revisión técnica: Se revisan el establecimiento efectivo de un canal cifrado o, alternativamente, un sistema de mensajería cifrada entre una aplicación local del equipo del prescriptor y la aplicación de prescripción o sistema de receta electrónica.

3.3.8 [SC05] Controles de custodia y conservación segura

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación establecida en el artículo 18.1 del RD 1718/2010, en virtud de la cual "el prescriptor se responsabilizará […] del acceso y utilización de datos para la prescripción electrónica. Las instituciones en las que los prescriptores presten sus servicios pondrán los medios necesarios para que puedan cumplirse estas obligaciones".

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Modelo de seguridad de la aplicación de prescripción.
- Descripción de los procedimientos de custodia y conservación de recetas electrónicas, y datos del sistema. En particular, política de evidencia electrónica y preservación digital de las recetas electrónicas.
- Descripción de procedimientos de borrado seguro de datos y recetas, transcurrido el plazo legal de conservación, así como de transferencia a la historia clínica del paciente.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión mixta: Existen procedimientos y mecanismos de custodia y conservación segura de los datos del Sistema (base de datos),
- Revisión mixta: Existen procedimientos documentados y mecanismos de custodia y conservación segura, así como de mantenimiento evidencial y preservación digital, de las recetas electrónicas formalizadas documentalmente (firmadas electrónicamente).

3.3.9 [SC06] Controles de disponibilidad 24x7x365 de los Sistemas de Prescripción y Repositorios de Prescripciones

Descripción detallada del control:

En este control, se revisa la existencia de controles de disponibilidad 24x7x365 del Sistema y/o Repositorio, en soporte de los servicios de urgencias.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Modelo de seguridad de la aplicación de prescripción.
- Plan de continuidad del negocio.
- Plan de recuperación ante el desastre.
- Modelo de servicio y relación 24x7 para atención de incidencias.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: Existen planes y procedimientos formalmente documentados que soportan la operativa 24x7x365, de la aplicación de prescripción y de la gestión de incidencias.
- Revisión documental: Se verifican todos los tiquets de incidencias desde la última auditoría.
- Revisión documental: Existen registros fiables de la prueba ordinaria de los planes de continuidad y recuperación.

3.3.10 [SC07] Seguridad del sistema de prescripción en su acceso a repositorios

Descripción detallada del control:

Este control es opcional y aplica únicamente cuando existan acuerdos que permitan registrar en un único almacén de datos (Repositorio de prescripción) las prescripciones generadas desde múltiples Sistemas de Prescripción.

Se revisa la seguridad del sistema de prescripción, en especial los controles de seguridad relacionados con las condiciones de acceso y uso de uno o varios Repositorios de Prescripciones para almacenamiento de recetas.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Identificación de los Repositorios accedidos para almacenamiento de recetas.
- Descripción de la tipología de recetas enviada a cada Repositorio.
- Descripción técnica de la arquitectura y mecanismos de interconexión y control de accesos entre el sistema y los Repositorios de prescripciones.
- Certificados utilizados en el establecimiento de las comunicaciones, de los diferentes Sistemas de Prescripción involucrados y del Repositorio de prescripciones.
- Descripción de la arquitectura de comunicaciones entre los diferentes Sistemas de Prescripción involucrados y del Repositorio de Prescripciones.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: La descripción técnica de la arquitectura y mecanismos de comunicación segura entre los múltiples Sistemas de Prescripción y el Repositorio de Prescripciones siguen estándares de comunicación segura: Comunicación cifrada (pe. con TLS/SSL en versiones sin vulnerabilidades conocidas), y reconocimiento mutuo mediante certificados cualificados.
- Revisión documental: Existe una auditoría de seguridad perimetral que incluye en alcance la totalidad de los sistemas implicados: Sistemas de Prescripción y Repositoriosde Prescripciones.

3.3.11 [SC08] Seguridad en el acceso facilitado por el Repositorio a NodoFarma

Descripción detallada del control:

En este control se revisa el cumplimiento por parte del Repositorio de prescripciones de los acuerdos de control de accesos y comunicaciones con el nodo de interoperabilidad del SREP(Nodofarma), garantizando una conexión cifrada y autenticada mediante certificados de entidad.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción técnica de los mecanismos de interconexión y control de accesos entre el sistema o Repositorio de prescripción y NodoFarma.
- Certificados utilizados en el establecimiento de las comunicaciones del Repositorio de prescripciones con NodoFarma.
- Descripción de la arquitectura de comunicaciones entre Repositorio de prescripciones y NodoFarma.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: La descripción técnica de la arquitectura y mecanismos de comunicación del Repositorio con NodoFarma siguen estándares de comunicación segura: Comunicación cifrada (pe. con TLS/SSL en versiones sin vulnerabilidades conocidas), y reconocimiento mutuo mediante certificados cualificados.

- Revisión documental: Existe una auditoría de seguridad perimetral del Repositorio con una antigüedad máxima de un año, y este no identifica vulnerabilidades graves no corregidas.

3.3.12 [SC09] Acceso del sistema de farmacia al Repositorio de Prescripciones

Descripción detallada del control:

En este control se revisa el cumplimiento de los acuerdos de control de accesos entre el sistema farmacéutico y el sistema o repositorio de prescripciones, garantizando una conexión cifrada y autenticada mediante certificados de entidad únicamente a través del nodo de interoperabilidad del SREP (Nodofarma).

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción técnica de los mecanismos de interconexión y control de accesos entre el Sistema de Prescripción o Repositorio de prescripciones y el sistema de conexión con las oficinas de farmacia permitiendo únicamente su acceso a través del canal homologado (vía nodo de interoperabilidad del SREP, NodoFarma).
- Certificados de entidad utilizados en el establecimiento de las comunicaciones: del Sistema de Prescripción o Repositorio de Prescripciones y del nodo de interoperabilidad del SREP (NodoFarma).
- Descripción de la arquitectura de comunicaciones entre el sistema o repositorio de prescripciones y el acceso a las oficinas de farmacia a través del nodo de interoperabilidad del SREP (NodoFarma)
- Informe de la última auditoría de seguridad perimetral (*Pentesting* o *Ethical Hacking*) efectuado en los sistemas.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: La descripción técnica de la arquitectura y mecanismos de comunicación segura entre los Sistemas de Prescripción y las oficinas de farmacia siguen estándares de comunicación segura, únicamente a través del nodo de interoperabilidad del SREP (Nodofarma): Comunicación cifrada (pe. con TLS/SSL en versiones sin vulnerabilidades conocidas), y reconocimiento mutuo mediante certificados cualificados.

- Revisión documental: Existe una auditoría de seguridad perimetral del sistema de prescripciones con una antigüedad máxima de un año, y este no identifica vulnerabilidades graves no corregidas.

3.4 Controles de interoperabilidad

3.4.1 [IN01] Aplicación por el Repositorio de las normas de interoperabilidad con NodoFarma

Descripción detallada del control:

En este control se revisa el cumplimiento de las normas de interconexión del Sistema de Receta Electrónica Privada entre los Repositorios de Prescripciones y el nodo de interoperabilidad del SREP (NodoFarma).

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Diseño técnico de comunicaciones de la aplicación de Repositorio.
- Implementación del interfaz de comunicación con el sistema farmacéutico (NodoFarma)

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: Las comunicaciones necesarias para la interconexión e intercambio de datos entre el Repositorio y NodoFarma, están correctamente documentadas.
- Revisión técnica: El Repositorio de Prescripciones responde en su diseño y funcionamiento a los requisitos establecidos en la documentación sobre el interfaz con NodoFarma.
- Revisión técnica: Se verifica el funcionamiento correcto de los canales establecidos, mediante un juego de pruebas de conexión e integración entre los sistemas, conforme al procedimiento técnico de NodoFarma.

3.4.2 [IN02] Consumo de servicios de autenticación delegada

Descripción detallada del control:

En este control es opcional, sólo aplica cuando el proceso de autenticación se delega a un sistema externo. Se revisa el cumplimiento de la obligación[18] establecida en el artículo 8.1 del RD 1718/2010, en virtud de la cual "el prescriptor ha de acreditar su identidad", mediante el consumo de servicios de autenticación delegada, como el CEF eID.

Este control es complementario, y apoya, al control [SC01], referido al control de acceso por parte del prescriptor.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Diseño técnico del sistema de autenticación de la aplicación de prescripción.
- Modelos de datos de autenticación intercambiables correspondientes a la aplicación de prescripción.
- Ejemplos de autenticación delegada.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la autenticación delegada.
- Revisión documental: Las comunicaciones necesarias para la interconexión e intercambio de datos entre las aplicaciones de prescripción y de autenticación delegada, están correctamente documentadas.
- Revisión técnica: Se verifica el funcionamiento correcto del sistema de autenticación delegada, mediante un juego de pruebas de certificados, vigentes y revocados.

3.4.3 [IN03] Verificación interoperable de certificados electrónicos

Descripción detallada del control:

[18] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

En este control se revisa el cumplimiento de la obligación[19] establecida en el artículo 8.1 del RD 1718/2010, en virtud de la cual "el prescriptor […] firmará electrónicamente la prescripción", cuando se haga uso de firma electrónica basada en certificado cualificado.

La verificación se puede realizar en local, mediante un sistema apropiado de verificación de certificados, o bien en remoto, empleando una plataforma específica de servicio de verificación de certificados.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Descripción del funcional de la aplicación referido a la prescripción.
- Diseño técnico del sistema de verificación de certificados electrónicos de la aplicación de prescripción.
- En la opción de uso de firma electrónica avanzada o cualificada, la verificación del certificado electrónico con el que se va a realizar la firma, contra el servicio de validación (OCSP / CRL) del prestador cualificado que ha emitido el certificado, siempre antes de realizar la firma electrónica.
- En la opción de uso de firma electrónica no criptográfica, la verificación del certificado electrónico del sello electrónico de persona jurídica con el que se va a sellar el conjunto de datos de la receta para dotarla de integridad, contra el servicio de validación (OCSP / CRL) del prestador cualificado que ha emitido el certificado, siempre antes de realizar el sellado de los datos de la receta y la trazabilidad, en su caso.
- La verificación del certificado electrónico del sello de tiempo electrónico con el que se va a dotar de fehacienca en el tiempo a los datos de la receta y trazabilidad, en su caso, contra el servicio de validación (OCSP / CRL) del prestador cualificado que ha emitido el certificado de sello de tiempo electrónico, siempre antes de realizar el sellado.Ejemplos de verificación de los certificados electrónicos cualificados usados según la opción.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

[19] El artículo 8 del RD 1718/2010 resulta aplicable a la prescripción de la receta médica privada electrónica en virtud de lo establecido por el artículo 14.2 del propio RD 1718/2010.

- Revisión documental: el funcional de la aplicación considera casos de uso y procedimientos para la autenticación delegada.
- Revisión documental: Las comunicaciones necesarias para la interconexión e intercambio de datos entre las aplicaciones de prescripción y el sistema de validación de certificados, están correctamente documentadas.
- Revisión técnica: Cumplimiento por las aplicaciones de verificación de firma electrónica reconocida de los requisitos de fiabilidad que se establecen a continuación.
    - Proporcionar servicios de confianza a las aplicaciones usuarias o consumidoras de los servicios de certificación y firma para la receta electrónica.
    - Proporcionar, en un único punto de llamada, como por ejemplo DSS, todos los elementos de confianza y de interoperabilidad organizativa, semántica y técnica necesarios para integrar los distintos certificados reconocidos y firmas del sistema de receta electrónica.
    - Permitir el empleo de formatos, estándares y políticas de firma electrónica y de certificados para las firmas electrónicas entre las aplicaciones usuarias, y de otros elementos de interoperabilidad relacionados con los certificados, tales como el análisis de los campos y extracción univoca de la información pertinente. En particular, se tendrán en cuenta los estándares europeos de las Organizaciones Europeas de Estandarización en el campo de las Tecnologías de Información y Comunicación aplicadas a la firma electrónica.
    - Incorporar las listas de confianza de los certificados interoperables entre las distintas Administraciones públicas nacionales y europeas según el esquema operativo de gestión correspondiente de la lista de confianza, a efectos de operaciones transfronterizas.
- Revisión técnica: Se verifica el funcionamiento correcto del sistema de verificación de certificados, mediante un juego de pruebas de certificados, vigentes y revocados.

3.5 Controles de protección de datos de carácter personal

3.5.1 [PD01] Cláusula de información de protección de datos personales

Descripción detallada del control:

En este control se revisa el cumplimiento de la obligación establecida en el artículo 3.2, último párrafo, del RD 1718/2010, en virtud de la cual "En […] la hoja de información al paciente para el caso de receta electrónica se incluirá una cláusula que informe al paciente", hoy en los términos establecidos en el RGPD y la LOPDGDD".

Conforme al anexo del RD 1718/2010, adecuado a la normativa actualmente vigente, se deberá emplear el siguiente modelo de cláusula:

"El paciente autoriza el acceso por el farmacéutico a los tratamientos incluidos en esta relación.

El paciente conservará este documento de información durante el período de validez del tratamiento.

En cumplimiento del RGPD y de la LOPDGDD se le informa que sus datos personales serán tratados con la exclusiva finalidad de facilitarle asistencia médica y farmacéutica al paciente, en el marco del Sistema de Receta Electrónica Privada, como sistema de información basado en receta médica en soporte electrónico, establecido por los Consejos Generales de Farmacéuticos, Médicos, Odontólogos y Podólogos al amparo de lo dispuesto en el artículo 14.4. del RD 1718/2010. En este sentido, […] actuará como responsable del tratamiento en relación sus datos clínicos, pudiendo acceder a los mismos la oficina de farmacia de su elección para poder garantizar la correcta asistencia farmacéutica y la organización farmacéutica colegial para la interoperabilidad que garantiza su derecho como paciente a que los tratamientos que le hayan sido prescritos en receta médica privada electrónica puedan ser dispensados en cualquier oficina de farmacia del territorio nacional, así como la trazabilidad de las actuaciones profesionales farmacéuticas en su dispensación. Puede ejercitar sus derechos ante […], a través de la dirección […].".

a. Este control debe diferenciar, y tener en cuenta para la auditoría, dos situaciones:

i. **La receta electrónica ha sido emitida por un prescriptor que presta sus servicios en un centro sanitario, que usa su propio software para recetas electrónicas, o lo adquiere a un tercero, inscrito en el REGCESS.** En este caso, la cláusula de protección de datos debe contemplar que los centros sanitarios son los responsables del tratamiento de datos de los pacientes.

ii. **La receta electrónica ha sido emitida por un prescriptor que presta sus servicios en su propia consulta privada y emplea un software para la prescripción de recetas electrónicas.** En este caso, la cláusula de protección de datos debe contemplar que el prescriptor es el responsable del tratamiento de los datos de los pacientes.

Documentación acreditativa a presentar en la justificación del cumplimiento:

- Modelos-tipo de documento de información al paciente y, en su caso, de hoja de medicación activa que incluya la cláusula de protección de datos.
- Ejemplos de documentos de información al paciente y, en su caso, de hojas de medicación activa que incluyan la cláusula de protección de datos.

Contenido de las pruebas y revisiones de cumplimiento a practicar por el auditor, para acreditar el cumplimiento de los controles:

- Revisión documental: existen ejemplos de documentos de información al paciente y, en su caso, de hojas de medicación activa que incluyan la cláusula de protección de datos.
- Revisión técnica: se expide una receta electrónica de prueba al auditor, y se verifica la producción y entrega del documento de información al paciente y, en su caso, de la hoja de medicación activa, con la cláusula informativa en términos de protección de datos.

3.5.2 [PD02] Medidas de seguridad derivadas de confidencialidad de la información almacenada en el Repositorio

Descripción detallada del control:

En este control se revisa el cumplimiento de las obligaciones establecidas por el artículo 11 del RD 1718/2010, en virtud del cual "el sistema de receta médica electrónica garantizará la seguridad en el acceso y transmisión de la información, así como la protección de la confidencialidad de los datos, de conformidad con lo dispuesto en la normativa vigente en materia de protección de datos".

Asimismo, el artículo 19.1 del RD 1718/2010 establece que "en los trámites a que sean sometidas las recetas médicas y órdenes de dispensación hospitalaria, y especialmente en su tratamiento informático, así como en su proceso electrónico, deberá quedar garantizada, conforme previene la normativa específica de aplicación, la confidencialidad de la asistencia médica y farmacéutica, la intimidad personal y familiar de los ciudadanos y la protección de sus datos de carácter personal. A tal efecto, se implantarán en el tratamiento de los datos las medidas de seguridad técnicas y organizativas, que en cada caso correspondan, para garantizar un nivel de seguridad adecuado a los riesgos, conforme al artículo 32 del RGPD.

En concreto, podrán emplearse las siguientes medidas de seguridad (u otras que consigan un efecto equivalente a las mismas). Los documentos que se aporten en los siguientes 14 apartados, cuando sea oportuno, deben de disponer de la correspondiente aprobación de un responsable de la empresa propietaria de la plataforma de receta:

I. CONTROL DE ACCESOS FÍSICO

- Garantizar, mediante controles de entrada adecuados (PIN, tarjetas identificativas, huella, etc.), que únicamente se permite el acceso al centro de procesamiento de datos (en adelante, **"CPD"**) a personal autorizado.

- Aprobar y/o supervisar los accesos al CPD y registrar la fecha y hora de entrada y salida. Cumplimentar un libro de registro (físico o digital) de todos los accesos.

- Revisar de forma periódica el registro de accesos al CPD, para comprobar su correcta cumplimentación. La periodicidad de la revisión debe fijarse en función de la sensibilidad de la información contenida en el CPD.

- Almacenar el registro de accesos durante un periodo de tiempo estipulado, que permita depurar responsabilidades en caso de accesos indebidos (se recomienda un plazo mínimo de 5 años).

II. GESTIÓN DE SOPORTES

- Inventariar los soportes de información que contengan datos de carácter personal. El inventario ha de mantenerse actualizado y reflejar todos los dispositivos empleados (discos duros, portátiles, smartphones).

- Implementar un protocolo de etiquetado anonimizado de los soportes que contengan datos personales, de modo que se pueda identificar el soporte y su contenido sin revelar el tipo de información contenida a terceros.

- Implementar procedimientos para el control, autorización y registro de la entrada y salida de soportes que contengan datos personales. Dentro de lo posible, registrar efectivamente las salidas de soportes realizadas.

- Implementar un protocolo de etiquetado anonimizado de los soportes que contengan datos personales, de modo que se pueda identificar el soporte y su contenido sin revelar el tipo de información contenida a terceros.

- En caso de estar autorizado el uso de soportes titularidad de los usuarios, deberá ponerse a su disposición técnicas criptográficas que permitan proteger los datos contenidos en los mismos cuando puedan incluir las categorías especiales de datos personales o altamente confidenciales.

- Usar un sistema de cifrado para proteger los datos personales sensibles almacenados o transportados en cualquier soporte, incluido dispositivos móviles, portátiles o soportes extraíbles.

- En los casos en los que no sea necesario mantener los datos contenidos en un soporte o este vaya a ser reutilizado, borrar la información contenida en el mismo de modo que se garantice que los datos son irrecuperables. Cuando el soporte vaya a ser desechado, proceder a la destrucción física del mismo, de modo que se impida definitivamente su reutilización.

III. CONTROL DE ACCESOS LÓGICOS

- Establecer y documentar una política de control de acceso lógico a los datos, de acuerdo con las funciones asignadas a cada usuario y atendiendo a los requisitos operativos y de seguridad de la información, y elaborar y mantener permanentemente actualizado un listado de los usuarios con acceso autorizado a los datos, de acuerdo con las funciones asignadas a cada usuario y atendiendo a los requisitos de negocio y de seguridad de la información.

- Determinar las reglas apropiadas para categorizar perfiles de acceso a los datos, identificando los derechos y las restricciones de acceso para los diferentes roles, de acuerdo con las funciones asignadas a cada perfil de usuarios y atendiendo a los requisitos de negocio y de seguridad de la información.

- Elaborar y mantener permanentemente actualizado un listado de los usuarios con permisos para la administración del sistema, de acuerdo con los requisitos operativos y de seguridad de la información.

- Crear un mecanismo que bloquee automáticamente a los usuarios que no acceden al sistema durante un periodo temporal definido previamente.

- Facilitar a cada usuario del sistema un medio de identificación y autentificación único. No pudiendo existir identificaciones generales o comunes.

- Cuando se usen contraseñas como medio de autenticación, el sistema debe obligar a que estas cuenten con una longitud mínima de caracteres.

- De forma periódica, el sistema debe obligar a los usuarios a modificar la contraseña empleada.

- Cuando se usen contraseñas como medio de autenticación, el sistema debe obligar a que estas cuenten con complejidad mínima (composición de diferentes tipos de caracteres).

- En el caso en que un usuario intente acceder al sistema introduciendo varias veces una contraseña errónea, que pueda interpretarse como un intento de acceso por un usuario no autorizado, el sistema deberá bloquear al usuario hasta que transcurra un periodo de tiempo determinado o, en su caso, sea rehabilitado por un administrador del sistema.

- En el momento de actualizar o cambiar las contraseñas asociadas a los identificadores, la nueva contraseña no podrá coincidir con contraseñas anteriormente utilizadas.

- Cuando se asigne por primera vez a un usuario del sistema una contraseña, el sistema deberá obligar al usuario deberá modificarla tras su primer acceso.

- Las contraseñas asignadas a cada usuario deberán almacenarse y transmitirse aplicando sistemas de cifrado, que impidan su conocimiento a cualquier usuario.

IV. REGISTRO DE ACCESOS

- El sistema debe registrar y monitorizar, de manera segura, todos los accesos realizados por parte de los usuarios.

- El sistema debe registrar la fecha y la hora de entrada y salida de los usuarios.

- El sistema debe registrar las acciones realizadas por el usuario (campo concreto o auditoría del objeto accedido o modificado).

- De forma periódica deberá revisarse el registro de accesos al sistema por parte de los usuarios.

- Almacenar el registro de accesos durante un periodo estipulado de tiempo, que permita depurar responsabilidades en caso de accesos indebidos (se recomienda un plazo mínimo de 5 años).

V. COPIAS DE SEGURIDAD

- Establecer y documentar una política de realización periódica de copias de seguridad del sistema, en un plazo que pueda minimizar la posible pérdida de información.

- Las copias de seguridad deberán ser almacenadas en un emplazamiento distinto del sistema, una distancia suficiente para evitar cualquier daño proveniente de un desastre en el emplazamiento original del sistema.

- Verificar las copias de seguridad periódicamente, de acuerdo a la política de copias de seguridad establecida.

- Comprobar periódicamente el procedimiento de restauración de las copias de seguridad, para asegurarse de que puede responder en caso de uso de emergencia cuando sea necesario.

- Las copias de seguridad deberán ser protegidas mediante mecanismos de cifrado que impidan la recuperación de los datos por parte de usuarios no autorizados.

VI. FICHEROS TEMPORALES

- Establecer un mecanismo de eliminación de los datos registrados temporalmente en carpetas compartidas de intercambio.

VII. CONTINUIDAD DE NEGOCIO

- Establecer mecanismos que permitan la redundancia del sistema de tratamiento de los datos, para garantizar la recuperación y disponibilidad en caso de caída del sistema principal.

- Elaborar e implementar un procedimiento de continuidad de negocio.

VIII. INCIDENCIAS

- Articular un procedimiento de registro de incidencias, con el objetivo de permitir comunicar y llevar un control y seguimiento de todas las incidencias detectadas y/o notificadas.

- Establecer un procedimiento de notificación de Brechas de Seguridad, tanto a nivel interno, como a la autoridad de control o a las personas afectadas, cuando sea preciso.

IX. COMUNICACIONES

- Implementar controles para garantizar la seguridad de la información en las redes y la protección de servicios conectados frente a accesos no autorizados (firewall, filtrado IP, IDS, etc.).
- Encriptar los contenidos relativos a datos que se consideren críticos o sensibles que transmitidos mediante redes de comunicaciones para salvaguardar la confidencialidad e integridad de los datos.

- Encriptar las comunicaciones realizadas a través de redes públicas o de redes inalámbricas para salvaguardar la confidencialidad e integridad de los datos.

- Verificar periódicamente la seguridad del sistema de encriptación empleado, para garantizar su efectividad respecto a nuevas amenazas.

X. AUDITORÍAS

- Realizar auditorías periódicas de seguridad de los sistemas (evaluación de las medidas de seguridad, test de penetración, etc.)

XI. VULNERABILIDADES TÉCNICAS

- Instalar sistemas de protección antivirus y/o antimalware para prevenir vulnerabilidades, que permitan una actualización adecuada ante nuevas amenazas.

- Obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados (incluidos sistemas operativos host y virtuales, aplicaciones y bases de datos), evaluar la exposición a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado).

- Realizar un mantenimiento y control de las actualizaciones de las versiones de las aplicaciones, software y bases de datos de manera gestionada o automatizada, para evitar las vulnerabilidades detectadas y controlar la compatibilidad de las versiones.

XII. SEGURIDAD EN EL EQUIPO LOCAL

- Implementar procedimientos para controlar la instalación del software en los equipos de los usuarios, limitando esta posibilidad a los administradores de sistemas.

- Establecer políticas para evitar el almacenamiento de información en los equipos locales (incluida su restricción técnica), con el objetivo de minimizar los riesgos asociados de perdida y desactualización de los datos.

XIII. ENTORNOS

- Separar los entornos de desarrollo, prueba y producción, de manera que este último este a salvo de cualquier posible consecuencia derivada de las incidencias ocurridas en los otros entornos.

- Evitar el uso de datos reales en entornos diferentes a producción que no puedan garantizar las mismas medidas de seguridad que el entorno de producción.
- Establecer las mismas medidas seguridad que en el entorno de producción en el caso de que se utilicen datos reales en entornos diferentes.

XIV. PSEUDONIMIZACIÓN EN BASE DE DATOS

- Pseudonimizar los datos, a través de técnicas que dificulten la reasociación de los mismos con su titular, en todos los procesos que no requieran de su identificación, cuando ello sea técnicamente viable.

- Anonimizar los datos, a través de técnicas que impidan definitivamente la posterior reasociación de los mismos con su titular, una vez que la identificación deje de ser necesaria y sea precisa la conservación de la información disociada.

4 Control de versiones

Julio 2020	Creación documento	V 1.0	CGCOM
Octubre 2022	Modificación control FT05	V 1.1 (0.1)	CGCOM
08/11/2022	Se realizan propuestas en los controles: FT05, FT11, FD02, SC01, SC03, IN03, PD02. Se añaden los controles SC01 bis y SC01 ter.	V 1.1 (0.2 a 0.4)	CGCOM
17/11/2022	Se realiza una propuesta para incrementar los controles en el control FD01	V 1.1 (0.5)	CGCOF
22/11/2022	Revisión	V 1.1 (0.6)	CGCOM
27/11/2024	Reordenación controles FT. Cambios en los controles [FT05], [FT06], [FT11], [FT10], [SC01], [SC01bis], [SC01ter], [SC03], [SC06], [SC09] y [PD01] Se añade el control [SC03bis]	V 1.2	CGCOM