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

Informe relativo a controles de autenticación y firma electrónica de sistema de receta médica privada electrónica

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

Introducción

El documento "Requerimientos para la auditoría de certificación de los Sistemas de Prescripción y Repositorios de Prescripciones del Sistema de Receta Electrónica privada", de julio de 2020, contiene 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.

En concreto, 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.

Estos objetivos de control se corresponden de forma estricta con las exigencias que impone el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación[1].

El control [SC01] de acceso del profesional prescriptor al sistema de receta

Como se indica en el documento de Requerimientos para la auditoría,

> En este control se revisa el cumplimiento de la obligación 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

[1] https://www.boe.es/eli/es/rd/2010/12/17/1718/con

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

> servicios pondrán los medios necesarios para que puedan cumplirse estas obligaciones".

La redacción del Real Decreto 1718/2010 no impone de forma exclusiva un sistema de identificación en concreto por parte del profesional, cuestión que trata conjuntamente con la firma electrónica en el artículo 8.1, por lo que cabe remitirse a los sistemas de identificación electrónica regulados en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos[2], que actualmente se regulan en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas[3] y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público[4], en función del rol del agente (interesado o personal al servicio de la Administración, respectivamente).

La decisión sobre el sistema de identificación electrónica a utilizar no es libre, sino que se debe adoptar conforme a lo establecido de forma obligatoria por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica[5] – ENS, considerándose admisible el cumplimiento de las exigencias del nivel MEDIO, y admitiéndose, además, otros sistemas equivalentes al mismo.

Sin perjucio de lo anterior, en el artículo 14.2 sí que se ordena, en el caso de que no resulte posible realizar el acceso al sistema de receta médica privada electrónica mediante el certificado del DNI electrónico del paciente, que dicho acceso "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". El certificado de firma electrónica, al que se refiere esta norma, es un sistema de identificación de nivel MEDIO en el ENS.

A pesar de ello, para garantizar la coherencia en la aplicación del ENS, y para garantizar la mayor neutralidad tecnológica de las soluciones, máxime transcurridos más de 10 años desde el Real Decreto se admiten los restantes sistemas de identificación de nivel MEDIO.

A continuación se presentan las tres grandes opciones aplicables en el momento de diseñar el sistema de identificación del profesional.

---

[2] https://www.boe.es/eli/es/l/2007/06/22/11/con
[3] https://www.boe.es/eli/es/l/2015/10/01/39/con
[4] https://www.boe.es/eli/es/l/2015/10/01/40/con
[5] https://www.boe.es/eli/es/rd/2010/01/08/3/con

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

Opción 1

Con carácter general, el epígrafe 4.2 del Anexo II del ENS [op.acc] impone las siguientes exigencias de control de acceso:

> El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.
>
> El control de acceso que se implante en un sistema real será un punto de equilibrio entre la comodidad de uso y la protección de la información. En sistemas de nivel Bajo, se primará la comodidad, mientras que en sistemas de nivel Alto se primará la protección.
>
> En todo control de acceso se requerirá lo siguiente:
>
> a) Que todo acceso esté prohibido, salvo concesión expresa.
> b) Que la entidad quede identificada singularmente [op.acc.1].
> c) Que la utilización de los recursos esté protegida [op.acc.2].
> d) Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización [op.acc.4].
> e) Serán diferentes las personas que autorizan, usan y controlan el uso [op.acc.3].
> f) Que la identidad de la entidad quede suficientemente autenticada [mp.acc.5].
> g) Que se controle tanto el acceso local ([op.acc.6]) como el acceso remoto ([op.acc.7]).
>
> Con el cumplimiento de todas las medidas indicadas se garantizará que nadie accederá a recursos sin autorización. Además, quedará registrado el uso del sistema ([op.exp.8]) para poder detectar y reaccionar a cualquier fallo accidental o deliberado.
>
> Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se acompañarán de los

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

> correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).

Por lo que se refiere a la actuación del profesional prescriptor, por tanto, se deben diferenciar dos controles: el control relativo a la previa identificación singular del profesional prescriptor, y la autenticación de la identidad del profesional prescriptor.

Respecto a la identificación singular del profesional prescriptor, resulta aplicable el control [op.acc.1], que se describe en el epígrafe 4.2.1 del Anexo II del ENS en los siguientes términos:

> La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:
>
> 1. Se podrán utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación.
>
> 2. Cuando el usuario tenga diferentes roles frente al sistema (por ejemplo, como ciudadano, como trabajador interno del organismo y como administrador de los sistemas) recibirá identificadores singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad.
>
> 3. Cada entidad (usuario o proceso) que accede al sistema, contará con un identificador singular de tal forma que:
>
> a) Se puede saber quién recibe y qué derechos de acceso recibe.
> b) Se puede saber quién ha hecho algo y qué ha hecho.
>
> 4. Las cuentas de usuario se gestionarán de la siguiente forma:
>
> a) Cada cuenta estará asociada a un identificador único.
> b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario.

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

> c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará periodo de retención.
>
> 5. En los supuestos contemplados en el Capítulo IV relativo a "Comunicaciones Electrónicas", las partes intervinientes se identificarán de acuerdo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento n.º 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 el que se deroga la Directiva 1999/93/CE:
>
> - Si se requiere un nivel BAJO en la dimensión de autenticidad (anexo I): Nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento n.º 910/2014)
> - Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento n.º 910/2014)
> - Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento n.º 910/2014).

Como se puede ver, se establecen unas medidas mínimas para la identificación, que aplican a todos los niveles de seguridad, desde el BAJO hasta el ALTO, en cuya virtud los profesionales que deban hacer uso del sistema de receta electrónica deben disponer de un identificador único.

Respecto a la autenticación de la identidad del profesional prescriptor, resulta aplicable el control [op.acc.5], que se describe en el epígrafe 4.2.5 del Anexo II del ENS en los siguientes términos:

> Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación:
>
> - "algo que se sabe": contraseñas o claves concertadas.

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

- "algo que se tiene": componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, tokens).
- "algo que se es": elementos biométricos.

Los factores anteriores podrán utilizarse de manera aislada o combinarse para generar mecanismos de autenticación fuerte.

Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados para cada nivel.

Las instancias del factor o los factores de autenticación que se utilicen en el sistema, se denominarán credenciales.

Antes de proporcionar las credenciales de autenticación a los usuarios, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración. Se contemplan varias posibilidades de registro de los usuarios:

- Mediante la presentación física del usuario y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello.
- De forma telemática, mediante DNI electrónico o un certificado electrónico cualificado.
- De forma telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los contemplados en la normativa de aplicación.

Nivel BAJO

a) Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.
b) En el caso de utilizarse como factor "algo que se sabe", se aplicarán reglas básicas de calidad de la misma.
c) Se atenderá a la seguridad de las credenciales de forma que:

1. Las credenciales se activarán una vez estén bajo el control efectivo del usuario.
2. Las credenciales estarán bajo el control exclusivo del usuario.

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

3. 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, protección de su confidencialidad e información inmediata en caso de pérdida.
4. Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
5. Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

Nivel MEDIO

a) Se exigirá el uso de al menos dos factores de autenticación.
b) En el caso de utilización de "algo que se sabe" como factor de autenticación, se establecerán exigencias rigurosas de calidad y renovación.
c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo:

1. Presencial.
2. Telemático usando certificado electrónico cualificado.
3. Telemático mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

Por ello, si se aplican acumulativamente los controles [op.acc.1] y [op.acc.5], sólo puede autorizarse un sistema de identificación del profesional prescriptor que cumpla con las siguientes exigencias mínimas:

1. Cada profesional debe disponer de un identificador único.
2. El identificador único del profesional debe permitir saber quién recibe y qué derechos de acceso recibe, y qué ha hecho, como profesional.
3. El sistema de autenticación del profesional debe exigir el uso de, al menos, dos factores de autenticación.
4. En el caso de utilización de "algo que se sabe" como factor de autenticación, como se establecerán exigencias rigurosas de calidad y renovación.
5. Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo: 1. Presencial, o 2. Telemático usando certificado electrónico cualificado, o 3. Telemático mediante una autenticación con una credencial electrónica obtenida tras un registro previo

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

presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

Opcion 2

Sin embargo, si se aplica únicamente el control [op.acc.1], apartado 5, del ENS, por entenderse que la relación con el profesional prescriptor es un caso de comunicación electrónica previsto en el Capítulo IV del ENS, entonces podrán alternativamente aplicarse las siguientes exigencias, previstas en el Anexo I del 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 arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) n° 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior[6], para el nivel de seguridad SUSTANCIAL:

2.1. *Inscripción*

2.1.1. Solicitud y registro

Nivel de seguridad	Elementos necesarios
Bajo	1. Asegurarse de que el solicitante conozca los términos y condiciones relacionados con el uso de los medios de identificación electrónica. 2. Asegurarse de que el solicitante conozca las precauciones de seguridad recomendadas relacionadas con los medios de identificación electrónica. 3. Recopilar los datos de identidad pertinentes necesarios para la prueba y verificación de la identidad.
Sustancial	Igual que el nivel bajo.

[6] http://data.europa.eu/eli/reg_impl/2015/1502/oj

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

2.1.2. Prueba y verificación de la identidad (persona física)

Nivel de seguridad	Elementos necesarios
Bajo	1. Se puede suponer que la persona está en posesión de pruebas reconocidas por el Estado miembro en el que se realiza la solicitud de los medios de identificación electrónica y que representan la identidad reclamada. 2. Se puede suponer que las pruebas son auténticas o que existen según una fuente auténtica y las pruebas parecen ser válidas. 3. Una fuente auténtica sabe de la existencia de la identidad reclamada y se puede suponer que la persona que reclama la identidad es la misma persona.
Sustancial	Nivel bajo y, además, se debe cumplir una de las alternativas indicadas en los puntos 1 a 4: 1) se ha verificado que la persona está en posesión de pruebas reconocidas por el Estado miembro en el que se realiza la solicitud de los medios de identificación electrónica y que representan la identidad reclamada, así como las pruebas se comprueban para determinar que son auténticas o, según una fuente auténtica, se sabe de su existencia y están relacionadas con una persona real, así como se han tomado medidas para reducir al mínimo el riesgo de que la identidad de la persona no sea la identidad reclamada, teniendo en cuenta, por ejemplo, el riesgo de pruebas perdidas, robadas, suspendidas, revocadas o expiradas;

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

	o bien 2) se presenta un documento de identidad durante un proceso de registro en el Estado miembro en el que se ha expedido el documento y el documento está referido a la persona que lo presenta, así como se han tomado medidas para reducir al mínimo el riesgo de que la identidad de la persona no sea la identidad reclamada, teniendo en cuenta, por ejemplo, el riesgo de documentos perdidos, robados, suspendidos, revocados o expirados; o bien 3) cuando los procedimientos utilizados anteriormente por una entidad pública o privada en el mismo Estado miembro para una finalidad distinta de la expedición de medios de identificación electrónica ofrecen una seguridad equivalente a la que proporcionan los establecidos en la sección 2.1.2 para el nivel de seguridad sustancial, no es necesario que la entidad responsable del registro repita esos primeros procedimientos, siempre que dicha seguridad equivalente esté confirmada por un organismo de evaluación de la conformidad de los que se hace referencia en el artículo 2, apartado 13, del Reglamento (CE) nº 765/2008 del Parlamento Europeo y del Consejo [(1)] o por un organismo equivalente; o bien 4) en los casos en que los medios de identificación se expidan sobre la base de un medio de identificación electrónica notificado válido que tenga el nivel de seguridad sustancial o alto, y teniendo en cuenta los riesgos de que se produzca un cambio en los datos de identificación de la persona, no es necesario

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

	repetir los procesos de prueba y verificación de la identidad; cuando los medios de identificación electrónica que sirven de base no se han notificado, el nivel de seguridad sustancial o alto deberá ser confirmado por un organismo de evaluación de la conformidad de los que se hace referencia en el artículo 2, apartado 13, del Reglamento (CE) nº 765/2008 o por un organismo equivalente.

2.2. *Gestión de medios de identificación electrónica*

2.2.1. Características y diseño de los medios de identificación electrónica

Nivel de seguridad	Elementos necesarios
Sustancial	1. El medio de identificación electrónica utiliza por lo menos dos factores de autenticación de distintas categorías. 2. El medio de identificación electrónica está diseñado de forma que se puede suponer que solo se utilizará bajo el control o la posesión de la persona a la que pertenece.

2.2.2. Expedición, entrega y activación

Nivel de seguridad	Elementos necesarios
Sustancial	Después de la expedición, el medio de identificación electrónica se entrega a través de un mecanismo mediante el cual se puede suponer que solo se entrega a la persona a la que pertenece.

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

2.2.3. Suspensión, revocación y reactivación

Nivel de seguridad	Elementos necesarios
Bajo	1. Es posible suspender o revocar un medio de identificación electrónica de manera eficaz y oportuna. 2. Se han tomado medidas para impedir la suspensión, revocación o reactivación no autorizadas. 3. La reactivación se llevará a cabo solo si se siguen cumpliendo los mismos requisitos de seguridad establecidos antes de la suspensión o revocación.
Sustancial	Igual que el nivel bajo.

2.2.4. Renovación y sustitución

Nivel de seguridad	Elementos necesarios
Bajo	Teniendo en cuenta los riesgos de un cambio en los datos de identificación de la persona, la renovación o sustitución debe cumplir los mismos requisitos de seguridad que la prueba y verificación de identidad inicial o basarse en un medio de identificación electrónica válido del mismo nivel de seguridad o de un nivel superior.
Sustancial	Igual que el nivel bajo.

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

2.3. *Autenticación*

Esta sección se centra en las amenazas asociadas al uso del mecanismo de autenticación y enumera los requisitos de cada nivel de seguridad. En esta sección se da por entendido que los controles están en consonancia con los riesgos en el nivel determinado.

2.3.1. Mecanismo de autenticación

La tabla siguiente establece los requisitos por nivel de seguridad con respecto al mecanismo de autenticación, a través del cual la persona física o jurídica utiliza los medios de identificación electrónica para confirmar su identidad a la parte usuaria.

Nivel de seguridad	Elementos necesarios
Bajo	1. La liberación de datos de identificación de la persona va precedida de una verificación fiable del medio de identificación electrónica y su validez. 2. Si se almacenan datos de identificación de la persona como parte del mecanismo de autenticación, dicha información está protegida con el fin de ofrecer protección contra la pérdida y contra cualquier peligro, incluido el análisis fuera de línea. 3. El mecanismo de autenticación aplica controles de seguridad para la verificación de los medios de identificación electrónica, por lo que es muy poco probable que actividades como intentos de adivinación, escucha, reproducción o manipulación de la comunicación por un atacante con potencial de ataque básico mejorado puedan alterar los mecanismos de autenticación.
Sustancial	Nivel bajo, además de lo siguiente: 1. La liberación de datos de identificación de la persona va precedida de una verificación fiable

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

	del medio de identificación electrónica y su validez por medio de una autenticación dinámica. 2. El mecanismo de autenticación aplica controles de seguridad para la verificación de los medios de identificación electrónica, por lo que es muy poco probable que actividades como intentos de adivinación, escucha, reproducción o manipulación de la comunicación por un atacante con potencial de ataque moderado puedan alterar los mecanismos de autenticación.

Esta alternativa permite más opciones para hacer una identificación inicial que la contenida en el ENS, pero se considera igualmente admisible. Resulta especialmente importante acreditar el cumplimiento de las exigencias del epígrafe 2.1.2.

Opción 3, en relación con la inscripción del profesional

También se considera admisible, a efectos de la verificación de la identidad de los profesionales prescriptores (en la inscripción en el servicio), el uso de los sistemas de identificación a distancia previstos en el artículo 12 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

En el marco del artículo 12.1.c) de la Ley 10/2010, el artículo 21.1.d) del RD 304/2014 autoriza el establecimiento de relaciones de negocio o la ejecución de operaciones a través de medios telefónicos, electrónicos o telemáticos con clientes que no se encuentren físicamente presentes, cuando la identidad del cliente quede acreditada mediante el empleo de otros procedimientos seguros de identificación de clientes en operaciones no presenciales, siempre que tales procedimientos hayan sido previamente autorizados por el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias[7]:

1. Autorización de procedimientos de identificación no presencial mediante videoconferencia, de 12 de febrero de 2016[8] (procesos asistidos por operador), efectiva a partir del día 1 de marzo de 2016.

[7] https://www.sepblac.es/es/
[8] https://www.sepblac.es/wp-content/uploads/2018/02/autorizacion_identificacion_mediante_videoconferencia.pdf

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

2. Autorización de procedimientos de vídeo-identificación, de 11 de mayo de 2017[9] (procesos no asistidos por operador), efectiva a partir del día 1 de junio de 2017.

Pautas adicionales

Se aconseja la revisión de la Guía de Seguridad de las TIC. CCN-STIC 857, del Centro Criptológico Nacional, Requisitos de Seguridad para Aplicaciones de Cibersalud en el contexto del ENS[10], en especial su epígrafe 3.1.6.

En la realización de la auditoría, se aconseja seguir las pautas de la Guía de Seguridad de las TIC. CCN-STIC 808, del Centro Criptológico Nacional, Verificación del Cumplimiento del ENS[11].

El control [FD02] de firma electrónica

Como se indica en el documento de Requerimientos para la auditoría,

> En este control se revisa el cumplimiento de la obligación del prescriptor prevista en el artículo 3.2.c.6°) 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

[9] https://www.sepblac.es/wp-content/uploads/2018/02/Autorizacion_video_identificacion.pdf
[10] https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/5326-ccn-stic-857-requisitos-seguridad-para-aplicaciones-cibersalud/file.html
[11] https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens-borrador/file.html

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

> 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).

La firma electrónica se encuentra regulada, con carácter general, en 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 el que se deroga la Directiva 1999/93/CE[12] – Reglamento eIDAS, y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza[13].

El Reglamento eIDAS establece el efecto jurídico de equivalencia entre la firma electrónica cualificada y la firma manuscrita, mientras que la Ley 6/2020 establece, además, la presunción de autenticidad de dicha firma electrónica cualificada, por lo que se trata del mecanismo preferible en todo caso.

El artículo 3 del Real Decreto 1718/2010 no impone de forma exclusiva el uso de la firma electrónica cualificada, sino que remite a los sistemas de firma electrónica regulados en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que actualmente se regulan en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en función del rol del firmante (interesado o personal al servicio de la Administración, respectivamente).

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 o sin certificado, en su caso cualificado) y sistemas de firma electrónica cualificada.

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, que dedica a ello el control [mp.info.4]:

> Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la

[12] http://data.europa.eu/eli/reg/2014/910/2014-09-17
[13] https://www.boe.es/eli/es/l/2020/11/11/6/con

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

procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.

La integridad y la autenticidad de los documentos se garantizarán por medio de firmas electrónicas con los condicionantes que se describen a continuación, proporcionados a los niveles de seguridad requeridos por el sistema.

En el caso de que se utilicen otros mecanismos de firma electrónica sujetos a derecho, el sistema debe incorporar medidas compensatorias suficientes que ofrezcan garantías equivalentes o superiores en lo relativo a prevención del repudio, usando el procedimiento previsto en el punto 5 del artículo 27.

Nivel BAJO

Se empleará cualquier tipo de firma electrónica de los previstos en la legislación vigente.

Nivel MEDIO

a) Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

b) Se emplearán algoritmos y parámetros acreditados por el Centro Criptológico Nacional.

c) Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin:

d) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:

1. Certificados.

2. Datos de verificación y validación.

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

e) El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes 1 y 2 del apartado d).

f) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes 1 y 2.

Como se puede ver, en nivel MEDIO no se exige la firma electrónica avanzada, pero si la misma se utiliza, se deben obligatoriamente aplicar las reglas que exige el ENS:

1. Los certificados cualificados deben ser expedidos por un prestador de servicios de confianza cualificado que, por tanto, se encuentre incluido en la lista de confianza expedida por el organismo de supervisión del Estado de establecimiento del prestador. En el caso de España, dicha lista se encuentra accesible en https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeinformationURI_es.aspx
2. Sólo resultan accesibles los certificados cualificados que contengan la información suficiente para la identificación unívoca de la identidad del profesional. No se admiten los certificados con seudónimo.
3. Se admite el uso de la firma electrónica avanzada basada en certificado cualificado sin dispositivo cualificado de creación de firma electrónica, como por ejemplo en formato P12, pero los datos de creación de firma (i.e. la clave privada) no pueden entregarse a la plataforma de receta electrónica. El organismo de supervisión ha indicado en una Nota informativa que la cesión de los datos de creación de firma electrónica a un tercero contraviene la normativa europea y española de firma electrónica, por lo que no se pueden admitir sistemas que implementen esta práctica.
4. Se admite el uso de la firma electrónica cualificada con generación y gestión de datos de creación de firma electrónica a cargo de un prestador de servicios de confianza cualificado.
5. Se admite también el uso de la firma electrónica avanzada basada en certificado cualificado con generación y gestión de datos de creación de firma electrónica a cargo de un prestador de servicios de confianza, inclusive sin cualificación, pero en este caso la auditoría debe verificar el cumplimiento de las exigencias de la especificación técnica ETSI TS 119 431-1 y, por referencia desde ésta, de la norma técnica CEN EN 419 241-1.

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

6. La plataforma de prescripción que desee ofrecer este servicio debe, por tanto, constituirse como prestador de servicios de confianza, y se recuerda que, en caso de operar sin cualificación, conforme al artículo 12 de la Ley 6/2020 se debe comunicar el inicio de esta actividad al órgano de supervisión.
7. Se admite el uso de los algoritmos previstos en el Guía CCN-STIC 807 a efectos de firma electrónica.
8. Para la representación de la firma puede hacerse uso de cualquiera de los formatos aprobados en la Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) n° 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior[14], o versiones más actualizadas de los mismos.
9. El sistema debe validar la firma electrónica conforme a lo establecido en la norma ETSI EN 319 102-1, conservando las correspondientes evidencias electrónicas.

Cuando se haga uso de un sistema que diferente de la firma electrónica avanzada basada en certificado cualificado, el mismo deberá apoyarse necesariamente en una previa identificación electrónica de nivel medio por parte del profesional, conforme a las exigencias anteriormente presentadas, y aportar garantías adicionales para la integridad y el no-repudio de la receta expedida.

Se consideran, a estos efectos, apropiadas las garantías contenidas en la Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos[15], con excepción de lo establecido sobre justificante de firma, que no debe entregarse.

También resultan admisibles sistemas de protección de registros de bases de datos y logs con incorporación de sello de tiempo cualificado, unitario para cada registro o entrada de log, o para proteger la raiz de un árbol de Merkle que agrupe los anteriores (por ejemplo, producidos para agrupar las recetas producidas en un periodo dado, que no puede superar las 6 horas); esto es, se

[14] http://data.europa.eu/eli/dec_impl/2015/1506/oj
[15] https://www.boe.es/eli/es/res/2017/07/14/(2)

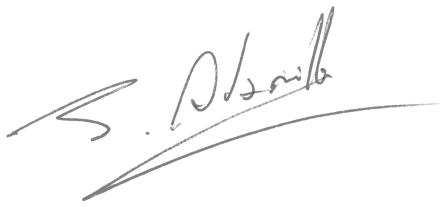
Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

debe garantizar que toda la información de la receta, de la identidad del profesional y de su actuación queda protegida frente a su alteración.

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.

En Madrid, a 4 de marzo de 2021



Fdo. Ignacio Alamillo Domingo
Doctor en Derecho, CISA, CISM, COBIT 5-f, ITIL v3-f