NORMA DE SEGURIDAD DE LOS SISTEMAS DE FIRMA ELECTRÓNICA

MUFACE

Documentación: MUFACE -Seguridad

Oficina de Seguridad de la Información

Referencia: Seguridad de la Información

Versión del documento 1.0

INDICE

INTRODUCCIÓN....4

6 SISTEMAS DE FIRMA INCLUIDOS EN EL ÁMBITO DE LA NORMA....7

7 CONSIDERACIONES GENERALES A TODOS LOS SISTEMAS DE FIRMA ELECTRÓNICA....9

7.1 Política de Firma Electrónica.... 9

7.2 Identificación de documentos que deben ser firmados 10

7.3 Procedimientos de firmado 10

7.4 Algoritmos criptográficos 10

7.5 Firma longeva y sellado de tiempo.... 11

7.6 Intercambio electrónico de datos en entornos cerrados de comunicación . 11

8 Consideraciones específicas para Sistemas de Firma de Sistemas de Información de nivel bajo respecto a las dimensiones de Integridad y Autenticidad 11

9 CONSIDERACIONES ESPECÍFICAS PARA SISTEMAS DE FIRMA DE SISTEMAS DE INFORMACIÓN DE NIVEL MEDIO RESPECTO A LAS DIMENSIONES DE INTEGRIDAD Y AUTENTICIDAD....12

10 CONSIDERACIONES ESPECÍFICAS PARA SISTEMAS DE FIRMA EN SISTEMAS DE INFORMACIÓN DE NIVEL ALTO RESPECTO A LAS DIMENSIONES DE INTEGRIDAD Y AUTENTICIDAD....13

11 REPORTES DE INCIDENTES DE SEGURIDAD. 14

12 RESPONSABILIDADES. 14

13 REVISIÓN DE LA NORMA....14

ANEXO I: REFERENCIAS....15

14.1 Medida mp.info.3.... 16

14.2 Medida op.pl.5 17

14.3 Medida op.exp.11 17

14.4 Medida mp.info.5.... 17

Cuadro Resumen del Documento

Tipo de Documento	Norma sobre responsabilidad de la información y criterios para su calificación
Autor	Oficina de Seguridad de la Información MUFACE
Fecha de elaboración	03/10/2025
Revisado por	Leonardo González García
Aprobado por	Silvia Lacleta (Responsable de Seguridad)

Control de Cambios

Versión	Fecha	Descripción de la modificación
1.0	03/10/2025	Versión inicial

1 Introducción

El Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (ENS) en el ámbito de aplicación al sector público, según el artículo 2 de la Ley 40/2015 del 1 de octubre, y según el artículo 156.2, establece los principios básicos y requisitos mínimos requeridos para proteger la información. Las Administraciones Públicas deberán aplicarlo para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), establece que los mecanismos de firma electrónica se aplicarán en los términos indicados en el Anexo II de dicha norma y de acuerdo con lo preceptuado en la política de firma electrónica y de certificados, según se establece en el Esquema Nacional de Interoperabilidad (en adelante ENI), aprobado por Real Decreto 4/2010, de 8 de enero.

El objeto de esta norma es el de establecer los requisitos de seguridad que deben cumplir los sistemas de firma empleados en los sistemas de información de MUFACE y las medidas de seguridad a adoptar durante su desarrollo, adquisición, integración, configuración o utilización.

2 Ámbito de aplicación

Esta norma aplica a todo el personal (funcionarios, personal laboral y personal externo, tanto de Servicios Centrales como de Servicios Periféricos y de los organismos autónomos adscritos) de la Secretaría de Estado de Administraciones Públicas (en adelante SEAP) que intervengan de alguna manera en la definición de requisitos, selección, desarrollo, integración, configuración o uso de sistemas de firma electrónica.

El ámbito de aplicación estricto se refiere a aquellos productos y servicios relacionados con el ejercicio de derechos, con el cumplimiento de deberes por medios electrónicos o con el acceso por medios electrónicos de los ciudadanos a la información, los servicios y al procedimiento administrativo, de acuerdo con lo previsto en la Ley 11/2007, de 22 de Junio, Acceso Electrónico de los Ciudadanos a los Servicios Públicos y con lo establecido por el ENS.

No obstante, lo establecido en el presente documento podrá ser, asimismo, de aplicación a todos aquellos sistemas o servicios que no queden contenidos en el ámbito de aplicación del ENS, si así se determinara por los responsables competentes.

3 Contexto

La presente norma se integra a su vez dentro del desarrollo normativo de seguridad derivado de la Política de Seguridad de la Información (en adelante PSI) de MUFACE, que está alineado con los principios básicos y los requisitos mínimos definidos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

El Responsable de Seguridad aprobará los procedimientos específicos que sean necesarios para el desarrollo de esta norma.

4 Vigencia

El presente documento producirá efectos desde la fecha de aprobación, indicada en la segunda página del mismo, y hasta que sea reemplazado por una nueva versión.

Las versiones anteriores que hayan podido distribuirse constituyen borradores o versiones obsoletas, por lo que su vigencia queda anulada por la última versión de este documento. En cualquier caso, toda la información referente a versiones, modificaciones, etc., aparece descrita en la ficha de versiones al inicio del documento.

5 Terminología relevante

A lo largo del texto de los documentos de desarrollo normativo de seguridad requeridos por la PSI de MUFACE se citan una serie de definiciones, entre ellas algunas figuras o roles, a los que se aludirá siguiendo esta nomenclatura:

- **Sistema de Información**: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
- **Usuario:** la persona o sistema que utiliza los sistemas de información de MUFACE, y/o a la información contenida en ellos.

- **Unidad TIC**: unidad encargada del desarrollo, mantenimiento y explotación del sistema de información al que estemos haciendo referencia.
- **Responsable del Sistema**: según define la PSI, esta responsabilidad recaerá en los titulares de los órganos responsables del desarrollo, mantenimiento y explotación del sistema de información que soporte los servicios correspondientes. Por tanto, según esta definición, recae sobre el titular de la Unidad TIC.
- **Responsable de Seguridad**: según define la PSI, la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y servicios.
- **Responsables de la Información:** según define la PSI, la persona que establece las necesidades de seguridad de la información que se maneja y efectúa las valoraciones del impacto que tendría un incidente que afectara a la seguridad. Esta responsabilidad recaerá en el titular del órgano o unidad administrativa que gestione el procedimiento o trámite.
- **Responsables del Servicio:** según define la PSI, la persona que determina los requisitos de seguridad de los servicios prestados. Esta responsabilidad recaerá en el titular del órgano o unidad administrativa de cada servicio.
- **Norma específica de cada ámbito:** Una norma específica desarrolla con mayor detalle la norma correspondiente de aplicación general dentro del ámbito de competencia de cada Responsable de Seguridad, si se considera necesario por parte de éste. En caso de existencia de norma específica y de discrepancia entre ésta y la norma general, prevalecerá lo indicado en la específica para la información y servicios afectados por los sistemas de información gestionados por el ámbito de competencia del Responsable de Seguridad correspondiente.
- **Firma electrónica:** conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante
- **Certificado electrónico:** documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
- **Certificado electrónico reconocido:** certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en la LFE en cuanto a la comprobación de la identidad y demás circunstancias de los

solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten

- **Dispositivo de creación de firma:** programa o sistema informático que sirve para aplicar los datos de creación de firma.
- **Dispositivo seguro de creación de firma:** dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:
  a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.
  b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.
  c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.
  d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.
- Sellado de tiempo: **acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción** por medios electrónicos.

6 Sistemas de firma incluidos en el ámbito de la norma

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (PAC en adelante), en su artículo 9, establece que los interesados podrán optar por relacionarse con las Administraciones Públicas a través de medios electrónicos, y se considerarán válidos a efectos de firma los siguientes:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".
b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".

c) Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud.

En el caso de firma por parte de las Administraciones públicas, la PAC señala que éstas podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan:

a) Sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".
b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico expedidos por prestador incluido en la "Lista de confianza de prestadores de servicios de certificación".
c) Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud.

Estos sistemas implementan firmas electrónicas clasificables, en virtud de las garantías ofrecidas respecto a la integridad del contenido y la autenticidad del firmante, en uno de estos tres tipos de firma electrónica recogidos por la LFE.

- firma electrónica: conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante
- firma electrónica avanzada, que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- firma electrónica reconocida, firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

El ENS establece en su medida **mp.info.3** que para determinar los requisitos de seguridad relativos a los sistemas de firma, se analizarán los niveles de las dimensiones de integridad y autenticidad. Y establece unas medidas distintas en función del nivel determinado.

7 Consideraciones generales a todos los sistemas de firma electrónica

7.1 Política de Firma Electrónica

MUFACE se adhiere a la Política de Firma electrónica y de certificados de la AGE, cuyo acuerdo de publicación se aprueba por Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas.

La Política de Firma electrónica y certificados de la AGE sigue las directrices establecidas en la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de Certificados de la Administración, aprobada por Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, en desarrollo del ENI.

El ámbito de dicha Política se circunscribe a los certificados previstos en la Ley 39/2015 expedidos para su empleo por la AGE y los organismos públicos vinculados o dependientes de ésta y a los sistemas de firma electrónica basados en certificados recogidos en el Real

Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos

La presente norma de seguridad de sistemas de firma electrónica establece medidas de seguridad para todos los sistemas de firma admitidos por la PAC, tanto los que se encuentran en el ámbito de la Política de firma electrónica y de certificados de la AGE como los que no, estando en el primer caso supeditada a lo que se indique en dicha Política

7.2 Identificación de documentos que deben ser firmados

El ENI establece en su artículo 21 que entre las medidas que las Administraciones públicas deben adoptar con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida se debe incluir la definición de una política de gestión de documentos 23. En el marco de la Política de Gestión de Documentos Electrónicos de aplicación en el ámbito de MUFACE se determinará el procedimiento para identificar los documentos que deban estar firmados, teniendo en cuenta las consideraciones generales que se mencionan en los siguientes párrafos.

Los documentos administrativos electrónicos, y aquellos susceptibles de formar parte de un expediente, tendrán siempre asociada al menos una firma electrónica de acuerdo con la normativa aplicable.
Las copias electrónicas auténticas serán firmadas mediante alguno de los sistemas de firma previstos en la Ley 39/2015.

7.3 Procedimientos de firmado

En el marco de la Política de Gestión de Documentos Electrónicos que resulte de aplicación en MUFACE, existirán procedimientos documentados para firmar y para verificar y validar las firmas durante el tiempo que se establezca como necesario, en función del valor administrativo, jurídico, fiscal u otros que se determinen en base a la legislación aplicable en cada caso.

7.4 Algoritmos criptográficos

Los sistemas de firma de MUFACE utilizarán algoritmos criptográficos acreditados por el CCN para el uso en el ENS y que han sido incluidos en la guía CCN-STIC-807.

En lo relativo a la protección y custodia de las claves criptográficas durante el ciclo de vida, se atenderá a lo dispuesto en la medida de protección op.ex.11 del ENS y a lo indicado en la Norma de autorización y acceso al servicio.

7.5 Firma longeva y sellado de tiempo

En todos los Sistemas de Información cuyo nivel de trazabilidad sea alto y en todos los casos en que se identifique que la fiabilidad de la firma deba ser garantizada a lo largo del tiempo, ésta se complementará con la información del estado del certificado asociado en el momento en que se produjo y/o información no repudiable incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.
La Política de Firma Electrónica y Certificados de la AGE establece las condiciones para considerar una firma electrónica longeva, para el archivado y custodia de las firmas, las reglas aplicables a los sellos de tiempos y las reglas de confianza para firmas longevas.

Tal y como se establece en la medida mp.info.4, los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada (en el caso que ocupa a esta norma, la firma electrónica) a efectos de disponibilidad, integridad y confidencialidad.

7.6 Intercambio electrónico de datos en entornos cerrados de comunicación

En lo relativo al sistema de firma de uso por parte de las Administraciones públicas, se tendrá en cuenta, lo establecido en la medida mp.com.3 del ENS de protección de la autenticidad y de la integridad de las comunicaciones y en la *Norma de transmisión de la información*, además de lo dispuesto en el ENI y las Normas Técnicas de Interoperabilidad.

8 Consideraciones específicas para Sistemas de Firma de Sistemas de Información de nivel bajo respecto a las dimensiones de Integridad y Autenticidad

El ENS establece que en los Sistemas de Información de nivel bajo en cuanto a dimensiones de Integridad y Autenticidad se podrá emplear cualquier medio de firma electrónica de los previstos en la legislación vigente.

En el caso de usar para la actuación administrativa automatizada sistemas de código seguro de verificación, que hayan sido aprobados por orden ministerial o resolución del titular del organismo público, previo informe del Consejo Superior de Administración Electrónica, se tendrán en cuenta las siguientes consideraciones:

- Se garantizará la disponibilidad del mecanismo de verificación.
- Se garantizará la integridad del documento referenciado.
- Se aplicarán las medidas de seguridad y controles de acceso necesario para garantizar la confidencialidad de acuerdo con el nivel correspondiente a esta dimensión.

En el caso de que, como sistema de firma de ciudadano, se apruebe mediante orden Ministerial o resolución del titular del organismo público un sistema basado en claves concertadas en registro previo como usuario o de aportación de información conocida por ambas partes, se adoptarán las siguientes medidas:

- La clave o la información conocida por ambas partes deberá introducirse expresamente cada vez que se firme (no se conservará en memoria)
- Se conservará como evidencia el HMAC (documento + clave concertada)
- En el caso de claves concertadas, se conservará como evidencia el registro en que se establece la relación entre el ciudadano y su clave.

En lo relativo a la calidad de las claves utilizadas o las características del tipo de información aportada se tendrá en cuenta lo establecido en la Norma de autorización y acceso al servicio

Se informará al Responsable de Seguridad previamente al uso de sistemas de firma no basados en certificados.

9 Consideraciones específicas para Sistemas de Firma de Sistemas de Información de nivel medio respecto a las dimensiones de Integridad y Autenticidad

Se emplearán sistemas de firma electrónica avanzada.

En la medida de lo posible se emplearán dispositivos seguros de creación de firma para la creación de las firmas por parte de MUFACE.

En la creación y recepción de firmas, se anexará o referenciará sin ambigüedad el certificado, los datos de verificación y validación. Los procedimientos de firmado mencionados en las consideraciones generales incluirán la información necesaria sobre cómo hacerlo.

10 Consideraciones específicas para Sistemas de Firma en Sistemas de Información de nivel alto respecto a las dimensiones de Integridad y Autenticidad

El ENS, en su medida mp.info.3 establece que se empleará cualquier tipo de firma electrónica de los previstos en el vigente ordenamiento jurídico, entre ellos, los sistemas de código seguro de verificación vinculados a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos 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.

En cuanto a los certificados, cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

Además, deberán emplearse algoritmos y parámetros autorizados por el CCN o por un esquema nacional o europeo que resulte de aplicación.

Cuando proceda, 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 se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

Asimismo, se usará la firma electrónica avanzada basada en certificados cualificados complementada por un segundo factor del tipo «algo que se sabe» o «algo que se es».
La firma electrónica avanzada se usará empleando productos certificados de acuerdo a lo establecido en la medida op.pl.5 del ENS.

11 Reportes de incidentes de seguridad.

El usuario deberá reportar cualquier incidente que considere relevante y que pueda afectar a la seguridad física o lógica, tanto los relacionados con los servicios, como con el equipamiento informático y los sistemas de firma electrónica. Para ello utilizará los medios habilitados por MUFACE para la notificación de incidencias especificados en las intranets correspondientes y, en casos de gravedad, deberá también avisar a su superior inmediato.

12 Responsabilidades.

El contenido de esta norma es de obligado conocimiento y cumplimiento por parte de las personas involucradas directa o indirectamente con la implementación, desarrollo, adquisición o uso de los sistemas de firma en MUFACE pudiéndose derivar de su incumplimiento la pertinente responsabilidad en el ámbito disciplinario, si a ello hubiera lugar en la aplicación de las disposiciones reguladoras del estatuto jurídico del usuario.

Las responsabilidades asociadas a cada componente de la estructura organizativa para la gestión de la seguridad en MUFACE es la definida en la Norma de Organización de Seguridad y Responsabilidades.

La detección de actuaciones irregulares, ilícitas o ilegales podrá acarrear la iniciación de las medidas disciplinarias oportunas y, en su caso, de las acciones legales correspondientes.

13 Revisión de la norma.

La presente norma y cualquier modificación de la misma, entrará en vigor en el momento en que sea aprobada por el Comité de Seguridad de la Información de MUFACE, lo que se notificará oportunamente mediante su publicación en la Intranet de MUFACE.

Las modificaciones totales o parciales de la presente normativa, así como la referencia de los documentos o versiones que sustituyen a este documento serán registradas mediante control de cambios y versión del documento.

Anexo I: Referencias

Se deberán tomar en consideración los siguientes textos y normativas:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Real Decreto 4/2010 de 8 de enero, por el que se regula el Esquema Nacional.
- de Interoperabilidad en el ámbito de la Administración Electrónica
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- PSI Política de Seguridad de la Información de MUFACE.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-800: Esquema Nacional de Seguridad - Glosario de Términos y Abreviaturas
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-804: Esquema Nacional de Seguridad. Guía de implantación.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-808: Verificación del cumplimiento de las Medidas en el ENS.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-809: Declaración de Conformidad del Esquema Nacional de Seguridad.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-813: Componentes certificados en el ENS.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad.

Las directrices estipuladas en esta norma se fundamentan en los requisitos establecidos en el ENS que se mencionan a continuación.

14.1 Medida mp.info.3

Se empleará cualquier tipo de firma electrónica de los previstos en el vigente ordenamiento jurídico, entre ellos, los sistemas de código seguro de verificación vinculados a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos 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.

Refuerzo R1-Certificados cualificados.

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

Refuerzo R2-Algoritmos y parámetros autorizados.

- Se emplearán algoritmos y parámetros autorizados por el CCN o por un esquema nacional o europeo que resulte de aplicación.

  El CCN determinará los algoritmos criptográficos que hayan sido autorizados nominalmente para su uso en el Esquema Nacional de Seguridad conforme a la Instrucción Técnica de Seguridad Criptología de empleo en el ENS.

Refuerzo R3-Verificación y validación de firma.

- Cuando proceda, 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 se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

Refuerzo R4-Firma electrónica avanzada basada en certificados cualificados.

- Se usará firma electrónica avanzada basada en certificados cualificados complementada por un segundo factor del tipo «algo que se sabe» o «algo que se es».

Refuerzo R5-Firma electrónica cualificada.

- Se usará firma electrónica cualificada, empleando productos certificados conforme a lo establecido en [op.pl.5].

14.2 Medida op.pl.5

Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto.

En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.

Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad.

Si el sistema suministra un servicio de seguridad a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19.

14.3 Medida op.exp.11

Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.

Los medios de generación estarán aislados de los medios de explotación.

Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Refuerzo R1-Algoritmos autorizados.

- Se emplearán algoritmos y parámetros autorizados por el CCN.

14.4 Medida mp.info.5

La utilización de sellos de tiempo exigirá adoptar las siguientes cautelas:

- Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.
- Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
- Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte, en su caso.
- Se emplearán "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) n.º 910/2014 y normativa de desarrollo.

14.5 Medida mp.com.3

En comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información. (Ver [op.acc.5]).

Se prevendrán ataques activos garantizando que al ser detectados se activarán los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos:

a) La alteración de la información en tránsito.
b) La inyección de información espuria.
c) El secuestro de la sesión por una tercera parte.

Se aceptará cualquier mecanismo de identificación y autenticación de los previstos en el ordenamiento jurídico y en la normativa de aplicación.

Refuerzo R1-Redes privadas virtuales.

- Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

Refuerzo R2-Algoritmos y parámetros autorizados.

- Se emplearán algoritmos y parámetros autorizados por el CCN.