
# Bases del Esquema judicial de interoperabilidad y seguridad

ÍNDICE

## INTRODUCCIÓN

La Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia pretende la efectiva y general utilización de las tecnologías de la información y comunicación en la Administración de Justicia, e igualmente por parte de los ciudadanos y de los profesionales de la justicia, en sus relaciones con dicha Administración y en las relaciones entre ésta con el resto de Administraciones y organismos públicos, de modo que se garantice, en dicho ámbito, el acceso, autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad, conservación e interoperabilidad de los datos, informaciones y servicios gestionados. Para ello el Preámbulo de la precitada Ley señala como uno de sus objetivos, definir el conjunto de requisitos mínimos de interconexión, interoperabilidad y seguridad necesarios a fin de garantizar la seguridad en la transmisión de los datos y cuantas otras exigencias se contengan en las leyes procesales.

A su vez, dada la concurrencia de diversas Administraciones e instituciones con diferentes títulos competenciales en materia de justicia, la Ley prevé un concreto marco de cooperación y colegiación entre todas ellas, destacando la creación de un órgano llamado a desempeñar una esencial actividad en la implantación de la Administración judicial electrónica en España. Dicho órgano fue desarrollado por el Real Decreto 396/2013, de 7 de junio, regulador del Comité técnico estatal de la Administración judicial electrónica que, en su artículo 3 señala su naturaleza, al concebirlo expresamente como el órgano de cooperación en materia de Administración judicial electrónica. (CTEAJE).

Desde la dimensión tecnológica, entre las funciones de este Comité destaca especialmente la producción del desarrollo de las normas técnicas previsto en los artículos 51 y siguientes de la referida Ley 18/2011, de 5 de julio, materia de la que se ocupa el presente texto sobre Bases del Esquema judicial de interoperabilidad y seguridad.

Las presentes Bases, que constituyen, junto con sus guías y normas técnicas, el desarrollo del Esquema Judicial de interoperabilidad y seguridad en la Administración de Justicia, han sido elaboradas atendiendo a las necesidades y requerimientos específicos de la actividad judicial, y respetando el principio de neutralidad tecnológica, teniendo en cuenta que existen preceptos del Esquema Nacional de Interoperabilidad y en el Esquema Nacional de Seguridad de válida aplicación en Justicia, a los que las presentes Bases se acogen evitando con ello su reproducción literal, y dotando de regulación específica y diferenciada a aquellos aspectos que son particulares y necesarios en el ámbito de la Justicia, así como el resto de las normas y recomendaciones invocadas en el artículo 47.3 de la Ley 18/2011, de 5 de julio.Sin perjuicio de lo establecido en el artículo 6.g del Real Decreto 396/2013, de 7 de junio, regulador del Comité técnico estatal de la Administración judicial electrónica, las normas técnicas aprobadas en su seno, se publicarán en el denominado Test de Compatibilidad

del Consejo General del Poder Judicial para su conocimiento por las Administraciones, usuarios y operadores jurídicos y al objeto de su evaluación y cumplimiento.

A continuación, sin más, se incluye el detalle del texto que se propone:

# DISPOSICIONES GENERALES.

## I. Del ámbito de aplicación y los principios generales

### 1. Objeto.

1.1. Este documento tiene por objeto desarrollar las Bases del Esquema judicial de interoperabilidad y seguridad establecido en el artículo 47 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y comunicación en la Administración de Justicia.

1.2. De conformidad con dicha Ley, el documento sobre Bases del Esquema judicial de interoperabilidad y seguridad será aplicado en la Administración de Justicia para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y la conservación de los datos, informaciones, documentos y servicios, utilizados por medios electrónicos que gestionen los distintos órganos judiciales en el ejercicio de sus competencias. Y todo ello se llevará a efecto con observancia de las prescripciones que en adelante se establecen y de los requisitos funcionales aplicables.

1.3. El ámbito de la interoperabilidad comprenderá los criterios tecnológicos y recomendaciones de seguridad, conservación, normalización y volcado de datos de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las distintas instituciones y Administraciones competentes en materia de justicia, para la toma de decisiones tecnológicas a fin de asegurar la referida interoperabilidad y el cumplimiento de los requisitos funcionales, de acuerdo con lo que se establece en el Test de Compatibilidad.

1.4. El ámbito de la seguridad, a estos efectos, albergará la política de seguridad en la utilización de medios electrónicos y el establecimiento de los principios básicos y requisitos mínimos que permitan una protección adecuada de la información de conformidad con el marco jurídico.

### 2. Ámbito de aplicación.

2.1. El ámbito de aplicación de estas Bases es el ya establecido en el artículo 2 de la propia Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

2.2. En aquellos aspectos relacionados con la interoperabilidad y seguridad que sean regulados en las presentes Bases, prevalecerán sus conceptos y principios sobre el Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad. A su vez, aquellos preceptos regulados en el

Esquema Nacional de Interoperabilidad y en el Esquema Nacional de Seguridad que sean de aplicación a la Administración de justicia, no se regularán en el presente texto.

## II. Garantías de Cumplimiento

### 3. Mecanismos de control.

3.1. El CTEAJE velará por el establecimiento de los mecanismos de control para garantizar de forma efectiva el cumplimiento de las Bases aquí expresadas, en cumplimiento de lo dispuesto en el artículo 49.3 de la reiteradamente invocada Ley 18/2011, de 5 de julio, y del artículo 6.h) del Real Decreto 396/2013, de 7 de junio, regulador del Comité técnico estatal de la Administración judicial electrónica, sin perjuicio de las competencias del Consejo General del Poder Judicial en los términos que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial establece.

### 4. Declaración de Conformidad.

4.1. En las sedes judiciales electrónicas correspondientes se publicarán las declaraciones de conformidad, compatibilidad y otros posibles distintivos de interoperabilidad y seguridad obtenidos respecto al cumplimiento de las exigencias aquí expresadas y de acuerdo con los criterios que se adopten en el CTEAJE.

### 5. Criterios y recomendaciones en materia de seguridad.

5.1. El CTEAJE recomendará criterios y contenidos mínimos en materia de seguridad que las Administraciones competentes en la materia deberán aplicar, siempre de conformidad con el marco jurídico.

5.2. A tal fin, sin perjuicio de las competencias de cada uno de los integrantes que componen el CTEAJE, utilizarán como instrumento de control las auditorías que resultan imprescindibles para la mejora continua de la seguridad, eficacia y eficiencia de los procesos y sistemas que gestionen.

5.3. En los supuestos de actuaciones judiciales automatizadas, el CTEAJE establecerá, como instrumento de control, las auditorías del sistema de información, de su código fuente y de los indicadores de gestión, en el ámbito de la interoperabilidad, de acuerdo con el artículo 42, de la ley 18/2011, de 5 de julio, y art. 6, letra l) del Real Decreto 396/2013, de 7 de junio, por el que se regula el Comité técnico estatal de la Administración judicial electrónica.

## DE LA INTEROPERABILIDAD JUDICIAL.

### I.- Principios básicos y dimensiones de la interoperabilidad judicial

#### 6. Principios básicos de la interoperabilidad judicial.

6.1. La aplicación de la Interoperabilidad Judicial y, en su caso, el cumplimiento de las Disposiciones Generales emanadas de estas Bases se desarrollarán de acuerdo con los principios generales establecidos en los Títulos I, II y V de la misma Ley 18/2011, de 5 de julio, observando los siguientes principios específicos de la interoperabilidad judicial:

a) Interoperabilidad como cualidad integral. La interoperabilidad se tendrá presente de forma integral desde la concepción de los servicios y sistemas y a lo largo de su ciclo de vida, incluyendo: planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión con los mismos.

b) Carácter multidimensional de la interoperabilidad. La interoperabilidad se entenderá contemplando sus dimensiones organizativa, semántica jurídica y técnica. La cadena de interoperabilidad se manifiesta en la práctica en los convenios correspondientes, en el despliegue de los sistemas y servicios, en la determinación y uso de estándares, en las infraestructuras y servicios básicos de las Administraciones con competencias en materia de justicia y en la publicación y reutilización de sus aplicaciones, de la documentación asociada y de otros objetos de información. Todo ello sin olvidar la dimensión temporal que ha de garantizar el acceso a la información a lo largo del tiempo.

c) Enfoque de soluciones multilaterales. Se favorecerá la aproximación multilateral a la interoperabilidad de forma que se puedan obtener las ventajas derivadas de la escalabilidad, de la aplicación de las arquitecturas modulares y multiplataforma, de compartir, de reutilizar y de colaborar.

### II.- Interoperabilidad organizativa

#### 7. Ámbitos de la interoperabilidad organizativa.

7.1. Interoperabilidad en la Administración de Justicia. El CTEAJE en el marco institucional de cooperación en materia de administración electrónica establecerá por medio de estas Bases las pautas y especificaciones técnicas para asegurar la interoperabilidad total de los sistemas y aplicaciones al servicio de la Administración de Justicia, y con ello la efectiva implantación de la Administración judicial electrónica.

7.2. Interoperabilidad con Ciudadanos y Profesionales. Se realizarán a través de sedes judiciales electrónicas y otros sistemas de comunicación electrónica especializados todas las actuaciones, procedimientos y servicios que requieran la autenticación de la Administración de Justicia o de los ciudadanos y profesionales por medios electrónicos.

Las sedes y subsedes judiciales electrónicas serán accesibles a través del Punto de acceso general de la Administración de Justicia que contendrá el directorio de todas ellas. Este punto de acceso podrá permitir el acceso a servicio e informaciones correspondientes a otras Administraciones públicas, según corresponda.

Los profesionales de la justicia, en los términos previstos en la Ley 18/2011, de 5 de julio, tienen el deber de utilizar los medios electrónicos, las aplicaciones o los sistemas establecidos por las Administraciones competentes en materia de justicia, respetando en todo caso las garantías y requisitos previstos en el procedimiento que se trate.

Asimismo, en el ámbito de la práctica de los actos procesales de comunicación y de traslado de copias previas entre los Procuradores de los Tribunales y para garantizar su interoperabilidad con los sistemas informáticos de gestión procesal, el CTEAJE colaborará con el Consejo General de Procuradores de los Tribunales de acuerdo con lo previsto en el Real Decreto 396/2013, de 7 de junio, por el que se regula el Comité técnico estatal de la Administración judicial electrónica.

7.3. Interoperabilidad con el resto de Administraciones públicas. El CTEAJE promoverá la cooperación de otras Administraciones públicas con la Administración de Justicia para suministrar a los órganos judiciales y las unidades funcionales a su servicio, a través de las plataformas de interoperabilidad establecidas por el Consejo General del Poder Judicial y por las Administraciones competentes en materia de justicia, la información que precisen en el curso de un proceso judicial en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y en las leyes procesales.

Asimismo, y en cumplimiento de lo previsto en el art. 37.4 de la Ley 18/2011, de 5 de julio, en materia de tramitación del procedimiento por medios telemáticos, es necesaria la colaboración con otras Administraciones y organismos públicos, para asegurar que los expedientes y demás actuaciones que deban ser remitidos se realicen en todo caso por vía telemática a través de la correspondiente sede judicial electrónica y otros sistemas de comunicación electrónica especializados, con los requisitos previstos.

## 8. Inventarios de información judicial.

8.1. Las Administraciones con competencias en materia de justicia publicarán y mantendrán actualizado, en sus sedes judiciales electrónicas, un inventario de información que incluirá los procedimientos y servicios que prestan de forma clasificada y homogénea, con indicación del nivel de informatización de los mismos. Igualmente, mantendrán una relación actualizada de los órganos judiciales teniendo en cuenta la evolución histórica de sus denominaciones y funciones.

8.2. El CTEAJE regulará la forma de creación y mantenimiento de este inventario. En el nivel técnico de la descripción y modelización de los procedimientos y servicios que los soportan será de aplicación lo previsto sobre estándares en el apartado 10 de este texto.

# III.- Interoperabilidad semántica jurídica

## 9. Conceptos de semántica jurídica.

9.1. Los modelos de datos de intercambio cumplirán las voces definidas en el Test de Compatibilidad. Las Administraciones con competencias en materia de justicia dispondrán, en su caso, de sistemas de traducción de las voces contenidas en sus modelos de datos y cuantas exigencias sean necesarias a fin de cubrir todas las necesidades de gestión procesal, de manera que permitan la interoperabilidad con el resto de las aplicaciones, entendiendo la misma no solo en lo referente al intercambio entre sistemas de información sino cualquier entrada o salida de datos y documentos de los Sistemas de Gestión Procesal, tales como: registro de datos, impresión de documentos, etc.

9.2. En orden al favorecimiento de la compatibilidad, el CTEAJE impulsará los requerimientos semánticos de las diferentes Administraciones con competencias en materia de justicia, para su posible inclusión en el Test de compatibilidad, de conformidad con el CGPJ.

9.3. Con la misma finalidad de desempeñar las competencias asignadas al CTEAJE, en orden de asegurar la interoperabilidad, dicho órgano publicará en su sede electrónica, una vez sea creada, y provisionalmente en aquella que se determine al efecto, el conjunto de modelos de datos de intercambio comunes aprobados internamente y, eventualmente, los enlaces a otros repositorios que incluyan modelos de datos específicos.

## IV.- Interoperabilidad técnica

### 10. Estándares aplicables.

10.1. Sin perjuicio de lo dispuesto en el artículo 11 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad, para la presentación de los escritos telemáticos se utilizará preferentemente el formato PDF; y para la presentación de documentos multimedia y de elementos de prueba, se admitirá cualquier formato, siempre que se aporte el software que permite tratarlo y entender los aspectos que determinan su pertinencia, o bien se adjunten los informes periciales que detallen la interpretación que se derive de su aportación.

10.2. El CTEAJE se ajustará al Catálogo de Estándares definido en el marco de desarrollo del ENI, sin perjuicio de su competencia a elaborar y publicar una guía de interoperabilidad y seguridad relativa a estándares, para lo no previsto.

## V. Comunicaciones de la Administración de Justicia

### 11. Redes de comunicaciones de la Administración de Justicia.

11.1. Las Administraciones con competencias en materia de justicia, para comunicarse entre sí, utilizarán preferentemente la red de comunicaciones del Punto Neutro Judicial (PNJ) desarrollada por el Consejo General del Poder Judicial, la Nueva Red Judicial (NRJ) creada por el Ministerio de Justicia, así como otras redes de ámbito común que, en su caso, se establezcan. Para ello conectarán sus redes y nodos de interoperabilidad a aquéllas, de forma que se facilite el intercambio de información y servicios entre las mismas, así como con el resto de Administraciones.

11.2. En su caso, se establecerá la posibilidad de facilitar la conectividad de las redes orientadas a la Administración de Justicia, con otras de las Instituciones, tanto de la Unión Europea y sus Estados miembros, como fuera de ella, incluyendo las redes iberoamericanas, mediante la Red de comunicaciones de las Administraciones públicas.

## VI.- Reutilización y transferencia de tecnología

### 12. Condiciones de licenciamiento aplicables.

12.1. Sin perjuicio de lo dispuesto en el artículo 16 del Esquema Nacional de Interoperabilidad y en el artículo 55 de la Ley 18/2011 de 5 de julio, podrán cederse aplicaciones judiciales entre

Administraciones o para su uso por terceros utilizando licencias de fuentes abiertas. En dicha cesión se tendrá en cuenta que el fin perseguido es el aprovechamiento, reutilización y protección contra su apropiación en exclusiva por parte de terceros, en términos que eximan de responsabilidad al cedente por un posible mal uso del cesionario o de terceros ya sea consentido o fraudulento.

### 13. Directorios de aplicaciones reutilizables.

13.1. El Ministerio de Justicia mantendrá, en el Punto de Acceso General de la Administración de Justicia, el directorio general de aplicaciones judiciales para su libre reutilización, de acuerdo con lo que se establece en el artículo 56 de la Ley 18/2011, de 5 de julio, y con los instrumentos derivados de la Unión Europea, e impulsará el mantenimiento del mismo, en colaboración con el resto de Administraciones competentes en materia de justicia, para lo que, en su caso, podrá tener en cuenta lo dispuesto en el artículo 6 p) del Real Decreto 396/2013, de 7 de junio, regulador del Comité técnico estatal de la Administración judicial electrónica. Se promoverá el desarrollo de guías técnicas, formatos y estándares comunes de especial interés para el desarrollo de la Administración judicial electrónica en el marco institucional de cooperación en materia de administración electrónica.

13.2. Para el mantenimiento del directorio general de aplicaciones judiciales, el Ministerio de Justicia podrá hacer uso de recursos ya existentes orientados a la gestión de software de fuentes abiertas gestionado por entidades especializadas en dicha actividad.

## VII. Firma electrónica

### 14. Interoperabilidad en la política de firma electrónica y de certificados.

14.1. El CTEAJE en el uso de sus competencias definirá, aprobará y publicará en su sede y en el Punto de Acceso General a la Administración de Justicia, una vez sean creadas, y provisionalmente en aquella que se determine al efecto, una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad.

14.2. Las Administraciones con competencias en materia de justicia adoptarán la política marco de firma electrónica y de certificados de la Administración de Justicia publicada por el CTEAJE, y sólo de forma justificada, aprobarán y publicarán otras diferentes en la correspondiente sede judicial electrónica.

14.3. La política marco estará dividida en dos secciones: la política de generación y la de comprobación.

a) En la sección de generación de firmas electrónicas se establecerán las condiciones para la generación de documentos firmados o sellados electrónicamente por el personal al servicio de la

Administración de Justicia, y por los sistemas de firma electrónica o de sello electrónico automatizados utilizados en su ámbito.

b) En la sección de comprobación de firmas electrónicas se establecerán las condiciones para la comprobación de validez de documentos firmados electrónicamente por ciudadanos o por sus representantes, y profesionales que se relacionan con la misma, o sellados electrónicamente por empresas, entidades y organismos que se relacionan con la Administración de Justicia. Esta sección se definirá de forma que se acepten todos los certificados cualificados emitidos con arreglo a lo dispuesto en el artículo 22 del Reglamento europeo 910/2014, de 23 de julio, de Identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior.

14.4. Las oficinas judiciales receptoras de documentos electrónicos, documentos administrativos electrónicos y documentos judiciales electrónicos permitirán la validación de firmas electrónicas que incluyan referencias a otras políticas de firma, cuando no contradigan la política general relativa a la aceptación de firmas electrónicas.

Las sedes y subsedes judiciales electrónicas deberán equiparse con certificados electrónicos que garanticen el cifrado de las comunicaciones desde su establecimiento, cumpliendo así lo previsto en el artículo 18.1 de la Ley reguladora. Los certificados utilizados para cifrar las comunicaciones con las páginas de internet de sedes y subsedes judiciales electrónicas, así como con los registros judiciales electrónicos, deberán adquirirse a Prestadores de Servicios de Certificación incluidos en los aplicativos de navegación de páginas internet comúnmente utilizados.

## 15. Aspectos de interoperabilidad judicial relativos a los prestadores de servicios de certificación.

15.1. Los prestadores de servicios de certificación, en materia de compatibilidad, interoperabilidad y seguridad, deberán actuar de conformidad con lo previsto en la Ley 18/2011, de 5 de julio, en el Reglamento europeo UE 910/2014 de 23 de julio, en el presente texto y su normativa de desarrollo.

Asimismo, deberán cumplir con lo previsto por los organismos de normalización en relación con los estándares y normas técnicas aplicables, especialmente respecto a los requisitos técnicos y operacionales que posibilitan la expedición de certificados cualificados. Cuando emitan certificados de personal al servicio de la Administración de Justicia, o para los sistemas de firma electrónica o de sello electrónico automatizados, podrán incluir en los campos de unidad organizativa, la información necesaria para identificar adecuadamente al ente u órgano titular del sello, de conformidad con el artículo 20 de la Ley 18/2011, de 5 de julio.

15.2. Los prestadores de servicios de certificación incluidos en las listas TSL (Trusted Service Status List, listado de prestadores de servicios de certificación de confianza) administradas en el ámbito de la Unión Europea y en los organismos de supervisión y acreditación de prestadores de servicios de certificación de los países miembros, gozarán de presunción de admisibilidad en la política de firma, de comprobación de firmas y sellos electrónicos de la Administración de Justicia de conformidad con lo dispuesto en el artículo 22 del Reglamento europeo UE 910/2014 de 23 de julio.

15.3. Los prestadores de servicios de certificación, de conformidad con lo descrito en su Declaración de Prácticas de Certificación, aplicarán lo siguiente:

a) Los estándares relativos a políticas y prácticas de certificación y generación de certificados electrónicos; estado de los certificados; dispositivos cualificados de creación de firma; programas controladores; dispositivos criptográficos; interfaces de programación; tarjetas criptográficas; conservación de documentación relativa a los certificados y servicios; y límites de los certificados, conforme a lo establecido en el antecedente apartado 14.

b) La incorporación, dentro de los certificados, de información relativa a las direcciones de Internet donde se ofrecen servicios de validación del propio certificado sin coste alguno.

## 16. Plataformas de validación de certificados electrónicos y de firma electrónica.

16.1. Los certificados admisibles deberán contener la dirección electrónica del servicio de comprobación de validez individual del certificado. Opcionalmente pueden contener, además, la dirección electrónica de otro servicio de comprobación de validez que otorgue acceso a lista de certificados revocados y no caducados del mismo tipo que el cuestionado, igualmente sin coste alguno.

16.2. Los certificados podrán ser validados mediante plataformas de validación de certificados electrónicos y de firma electrónica, que proporcionarán servicios de confianza a las aplicaciones usuarias o consumidoras de los servicios de certificación y firma, proporcionando servicios de validación de los certificados y firmas generadas y admitidas en diversos ámbitos de las Administraciones con competencias en materia de justicia.

16.3. Estas plataformas incorporarán las listas de confianza de los certificados interoperables entre las distintas Administraciones nacionales y europeas según el esquema operativo de gestión correspondiente de la lista de confianza (TSL), de acuerdo con en el artículo 22 del Reglamento UE 910/2014, de 23 de julio.

## VIII. Recuperación y conservación del documento judicial electrónico

### 17. Condiciones para la recuperación y conservación de documentos judiciales electrónicos.

17.1. Las Administraciones con competencias en materia de justicia adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos judiciales electrónicos a lo largo de su ciclo de vida. Tales medidas, sin perjuicio de lo establecido en las guías de interoperabilidad y seguridad, garantizarán en todo caso:

a) La definición de una política de gestión de documentos judiciales electrónicos en cuanto al tratamiento, de acuerdo con las normas y procedimientos específicos que se hayan de utilizar en la formación y gestión de los documentos y expedientes judiciales electrónicos.

b) La inclusión en los expedientes judiciales electrónicos de un índice electrónico firmado por la oficina judicial actuante, que garantice la integridad de aquellos expedientes y permita su recuperación siempre que sea preciso.

c) La identificación única e inequívoca de cada documento judicial electrónico a través de las convenciones adecuadas, que permitan clasificarlo, recuperarlo y referirse al mismo con facilidad.

d) La asociación de los metadatos obligatorios y, en su caso, complementarios, al documento judicial electrónico, a lo largo de su ciclo de vida, e incorporación al esquema de metadatos.

e) La clasificación y tipología de los documentos judiciales electrónicos, prevista en la guía de interoperabilidad y seguridad del Documento judicial electrónico, respetando lo dispuesto en las leyes procesales, y en el Test de Compatibilidad de los Sistemas Informáticos de Gestión Procesal.

f) El período de conservación de los documentos judiciales electrónicos, fijado en las normas procesales y demás legislación aplicable, atendiendo asimismo, a lo dispuesto en el presente texto sobre conservación de la información.

g) El acceso completo e inmediato a los documentos judiciales electrónicos, cuando corresponda, a través de métodos de consulta en línea, que permitan la visualización de los documentos con todo el detalle de su contenido, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los formatos originales y la impresión en papel de aquellos documentos que sean necesarios, de conformidad con lo dispuesto en las normas procesales y reguladoras del acceso a las actuaciones judiciales. En tal sentido, el sistema permitirá la consulta de la firma

electrónica y sello de tiempo del documento judicial electrónico, y de los metadatos asociados durante todo el período de conservación del mismo.

h) La adopción de medidas para asegurar la conservación de los documentos judiciales electrónicos a lo largo de su ciclo de vida procesal, conforme a lo previsto en el apartado 18 de este documento. A tal fin, se deberá asegurar la recuperación durante el plazo mínimo de conservación determinado por las normas procesales, garantizar su conservación a largo plazo y preservar la transparencia, memoria e identificación de los órganos u oficinas judiciales que ejerzan la competencia sobre los expedientes o documentos judiciales electrónicos.

i) La coordinación horizontal entre el responsable de gestión de documentos judiciales y los restantes servicios interesados en materia de archivos judiciales.

j) El borrado de la información o, en su caso, la destrucción física de los soportes en los que está fijada dicha información si, conforme a la normativa sobre expurgo de actuaciones judiciales, así procediera tras el resultado del procedimiento de evaluación documental, dejando registro de su eliminación.

k) Transferencia, en su caso, de los expedientes judiciales electrónicos entre los diferentes repositorios de los órganos judiciales a efectos de conservación, de conformidad con lo establecido en la legislación en materia de archivos, de manera que se pueda asegurar la conservación y recuperación de dichos expedientes a medio y largo plazo.

l) La formación tecnológica del personal responsable de la ejecución y del control de la gestión de documentos, así como de su tratamiento y conservación en archivos o repositorios electrónicos.

m) La documentación de los procedimientos que garanticen la interoperabilidad a medio y largo plazo, así como las medidas de identificación, recuperación, control y tratamiento de los documentos judiciales electrónicos.

17.2. A los efectos de lo dispuesto en el precedente apartado sobre archivos o repositorios, las Administraciones con competencias en materia de justicia crearán los repositorios electrónicos complementarios respecto de los archivos convencionales y destinados a cubrir el conjunto del ciclo de vida de los documentos judiciales electrónicos.

## 18. Seguridad del documento judicial electrónico.

18.1. Los documentos judiciales electrónicos, desde que se encuentren custodiados en el sistema de gestión procesal, gozarán de la presunción de que los certificados electrónicos con los que se

firmaron eran válidos en el momento de la realización de la firma electrónica, incluso cuando haya transcurrido el período de validez de cada certificado.

18.2. Cuando los documentos judiciales electrónicos incluyan un Código Seguro de Verificación, su autenticidad podrá cotejarse en la sede o subsede electrónica del órgano que lo expidió, en virtud de las medidas de seguridad empleadas para su custodia. Al acceder, en la sede o subsede judicial electrónica, al documento referenciado por el Código Seguro de Verificación, se obtendrá el documento judicial electrónico que incluirá, en su caso, las firmas electrónicas que correspondan. Los documentos judiciales electrónicos que se impriman serán válidos en su forma impresa siempre que puedan cotejarse de la manera indicada.

## 19. Digitalización certificada de documentos en soporte papel en el ámbito de la Administración de Justicia.

19.1. Las oficinas judiciales y el resto de órganos relacionados con la Administración de Justicia podrán proceder a la digitalización certificada de documentos presentados y conservados en papel que tengan el carácter de original. Los documentos así digitalizados tendrán la consideración de copias auténticas y surtirán el efecto del original, con su misma validez y eficacia, de acuerdo con lo que establece el artículo 28 de la Ley 18/2011, de 5 de julio.

19.2. Se entiende por digitalización certificada el proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico, en uno o varios ficheros electrónicos que contengan la imagen codificada, fiel e íntegra de tal documento, conforme a alguno de los formatos estándares de uso común.

Dicho proceso deberá incluir información relativa al proceso de digitalización indicada en sus metadatos; un nivel de resolución adecuado al tipo de documento; y un mecanismo de preservación de la integridad, tal como una firma electrónica de un secretario judicial o un sello electrónico del órgano aplicado al documento y al sistema de control de la llevanza de la digitalización. Para satisfacer los requisitos de integridad de los sistemas de control en los procesos de digitalización también serán válidos sistemas de sello de tiempo cualificado según lo previsto en el artículo 42 del Reglamento UE 910/2014 de 23 de julio. En la digitalización certificada se hará uso de un software de digitalización certificado conforme a lo que se prevea en la guía de Interoperabilidad y Seguridad de Digitalización Certificada en la Administración de Justicia.

## DE LA SEGURIDAD JUDICIAL ELECTRÓNICA.

### I. Principios básicos de la seguridad judicial electrónica

#### 20. Dimensiones de seguridad

20.1. Son dimensiones de la seguridad judicial electrónica de los servicios o de la información:

a) Autenticidad (A).

b) Confidencialidad (C).

c) Integridad (I).

d) Disponibilidad (D).

e) Trazabilidad (T).

f) Conservación (Cs).

20.2. Respecto al Esquema Nacional de Seguridad, en el ámbito de la Administración de Justicia se considera una dimensión adicional la conservación. Esta dimensión se tendrá en cuenta al determinar la categoría de los sistemas que en adelante se refieren, en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios, con perjuicio para todas las dimensiones de seguridad señaladas en el apartado anterior, siguiendo el procedimiento establecido en el Anexo I.

#### 21. Niveles de seguridad.

21.1. En aplicación del artículo 53 de la Ley 18/2011 de 5 de julio, el sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad que permite una gestión de incidentes más adecuada.

21.2. Los niveles de seguridad se aplican a las dimensiones de seguridad de los servicios o de la información y a las categorías de los sistemas de información. La categoría de un sistema, que podrá ser Básica, Media o Alta, se determinará por la máxima clasificación que alcance una o más de las dimensiones de seguridad respecto a los servicios que presta o la información que maneja. Las dimensiones de seguridad se clasifican como de nivel Bajo, Medio o Alto, según el impacto o perjuicio que suponga un incidente de seguridad sobre las funciones de la organización, sus activos o las personas que intervienen.

# II. Organización, gestión y requisitos mínimos de seguridad

## 22. Requisitos mínimos de seguridad.

22.1. En lo que se refiere a los sistemas de información, para garantizar los aspectos de seguridad judicial electrónica, se enumeran los requisitos mínimos que todas las Administraciones con competencias en materia de justicia deben cumplir. Dichos requisitos serán desarrollados mediante la guía técnica de seguridad.

22.2. Todos los órganos superiores de las Administraciones con competencias en materia de justicia deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se adoptará en base a los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos.

h) Seguridad por defecto.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de actividad.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

o) Mejora continua del proceso de seguridad.

Todos estos requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, según lo descrito en el artículo 12 y siguientes del Esquema Nacional de Seguridad.

## 23. Cumplimiento de requisitos mínimos.

23.1. Para dar cumplimiento a los requisitos mínimos anteriormente establecidos, las Administraciones con competencias en materia de justicia e instituciones judiciales aplicarán las medidas de seguridad indicadas en el Anexo II incorporado a este documento, que tiene en cuenta aspectos específicos respecto a las dimensiones de seguridad aplicables en la Administración de Justicia, así como lo indicado en el Anexo II del Esquema Nacional de Seguridad.

23.2. La relación de medidas seleccionadas del Anexo II se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de seguridad.

23.3. Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de seguridad

## 24. Guía técnica de seguridad.

24.1. El CTEAJE, en el ejercicio de sus competencias, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento en la Administración de Justicia bajo la forma de guía técnica de seguridad. Para ello tendrá en cuenta las guías de seguridad de las tecnologías de la información y las comunicaciones elaboradas por el Centro Criptológico Nacional.

24.2. La guía técnica de seguridad tendrá en cuenta las normas armonizadas a nivel europeo que resulten de aplicación.

# III. Comunicaciones electrónicas

## 25. Condiciones técnicas de seguridad de las comunicaciones, notificaciones y publicaciones electrónicas.

25.1. Las condiciones técnicas de seguridad de las comunicaciones electrónicas, se fijarán de acuerdo a lo establecido en las normas procesales y en la Ley 18/2011, de 5 de julio, y serán implementadas conforme a las presentes Bases.

25.2. Las comunicaciones a través de medios electrónicos se realizarán, en todo caso, con sujeción a lo dispuesto en la legislación procesal y serán válidas siempre que exista constancia de la transmisión, y se puedan acreditar los siguientes aspectos: su puesta a disposición, su recepción o acceso al contenido por el destinatario, sus fechas respectivas, la integridad del contenido de las comunicaciones, y la identificación, con la autenticación que sea exigible al remitente y al destinatario de las mismas, con posibilidad de acreditar todos estos aspectos.

25.3. Los requisitos de seguridad e integridad de las comunicaciones, publicaciones y notificaciones electrónicas se establecerán en cada caso de forma apropiada al carácter de los datos objeto de aquéllas, de acuerdo con criterios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal y en las leyes procesales.

25.4. Las comunicaciones, publicaciones y notificaciones electrónicas realizadas en los términos indicados en el apartado anterior, tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la norma procesal aplicable al supuesto concreto.

25.5. Para las publicaciones edictales electrónicas, se garantizará la autenticidad del organismo que lo publique, así como la integridad de la información publicada, en la sede o subsede judicial electrónica.

## IV. Estado de seguridad de los sistemas

### 26. Informe del estado de la seguridad.

26.1. El CTEAJE articulará los procedimientos necesarios para conocer regularmente el estado de las principales variables tecnológicas de la seguridad, en los sistemas de información a los que se ha hecho referencia, de forma que permita elaborar un perfil general del estado de la seguridad de la Administración de Justicia.

26.2. Con este objeto, el CTEAJE recomendará indicadores de la seguridad para dichos sistemas de información que tendrán en cuenta los procedimientos y metodologías que elabore el Centro Criptológico Nacional.

# V. Respuesta a los incidentes de seguridad

## 27. Coordinación frente a incidentes de seguridad de la información.

27.1. Dentro del CTEAJE se fomentará el establecimiento de los protocolos y acuerdos de colaboración con el Centro Criptológico Nacional (CCN) para la coordinación y prestación de servicios de respuesta a incidentes de seguridad.

# VI. Categorización y medidas de seguridad de los sistemas de la Administración de Justicia

## 28. Categorías de seguridad.

28.1. En el ámbito de la Administración de Justicia se establecen dimensiones de seguridad que añaden la conservación a las definidas en el marco del Esquema Nacional de Seguridad. En relación con las categorías de seguridad, se ha tenido en cuenta lo dispuesto en el artículo 43 del Esquema Nacional de Seguridad cual se refleja en el Anexo I del presente documento.

## 29. Medidas de seguridad.

29.1. De acuerdo a los niveles y categorías establecidas en el Anexo II y según los criterios de gravedad establecidos en el Anexo I los sistemas de la Administración de Justicia aplicarán las medidas de seguridad correspondientes.

# ACTUALIZACIÓN, DESARROLLO Y FORMACIÓN

## I. Desarrollo de las Bases del Esquema judicial de interoperabilidad y seguridad

### 30. Actualización permanente.

30.1. Para el desarrollo, perfeccionamiento y la actualización de las presentes Bases, el CTEAJE elaborará:

a) Las correspondientes guías y normas técnicas de aplicación.

b) Una guía técnica de seguridad que desarrolle los requisitos mínimos de seguridad fijados en este documento

c) En el marco de sus competencias, cualquier otra normativa cuya necesidad venga impuesta por el desarrollo de la Administración judicial electrónica.

### 31. Formación

31.1. Los funcionarios de los cuerpos al servicio de la Administración de Justicia y demás personal de la misma, recibirán la formación necesaria para garantizar el conocimiento de estas Bases, a cuyo fin las diferentes Administraciones e instituciones judiciales competentes dispondrán lo necesario para que dichos funcionarios reciban la formación necesaria y adecuada a sus tereas respectivas.

### 32. Desarrollo

32.1. De conformidad con lo dispuesto en el Título V de la Ley 18/2011, de 5 de julio, y en el Real Decreto 396/2013, de 7 de junio, el CTEAJE elaborará, aprobará y difundirá las guías de interoperabilidad y seguridad de las tecnologías de la información y las comunicaciones (GIS), sin perjuicio de la aprobación por el Consejo General del Poder Judicial de aquellas guías que afecten a la compatibilidad, materia reservada a dicho Órgano en el art. 230.5, párrafos segundo y tercero, de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

A estos efectos se establece como lista inicial de guías a desarrollar, las siguientes:

a) Expediente judicial electrónico: tratará de su estructura y formato, así como de las especificaciones técnicas de los servicios de remisión y puesta a disposición.

b) Documento judicial electrónico: tratará los metadatos exigibles en el mismo y su carácter, la asociación de los datos y metadatos de firma o de sellado de tiempo y los formatos de documento.

c) Digitalización certificada en la Administración de Justicia: tratará los formatos y estándares aplicables, los niveles de calidad, las condiciones técnicas y los metadatos asociados al proceso de digitalización, así como el procedimiento de homologación de las soluciones de digitalización certificada.

d) Procedimientos de copiado auténtico y conversión entre documentos judiciales electrónicos, así como desde papel u otros medios físicos a formatos electrónicos.

e) Protocolos de intermediación de datos: tratará las especificaciones de los protocolos de intermediación de datos que faciliten la integración y reutilización de servicios en la Administración de Justicia y que serán de aplicación para los prestadores y consumidores de tales servicios.

f) Relación de modelos de datos que tengan el carácter de comunes en la Administración de Justicia y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos, profesionales de la justicia y otras Administraciones.

g) Política de gestión de documentos electrónicos: incluirá pautas para la asignación de responsabilidades, tanto directivas como profesionales; la definición de los programas, procesos y controles de gestión de documentos; así como la administración de los repositorios electrónicos y la documentación de los mismos, a desarrollar por la Administración de Justicia.

h) Declaraciones de conformidad con las Bases del Esquema judicial de interoperabilidad y seguridad: establecerá las reglas para la aplicación de lo dispuesto en el apartado 4 de este documento.

i) Guía técnica de seguridad.

j) Cualquier otra guía de interoperabilidad y seguridad que el CTEAJE considere necesaria para regular otros aspectos de la interoperabilidad y seguridad judiciales que, con suficiente entidad, no estuviere contemplado en los puntos anteriores.

32.2. Asimismo, será de aplicación por parte de la Administración de Justicia, cuando corresponda, la norma técnica de interoperabilidad de Catálogo de estándares, que venga a establecer el conjunto de dichos estándares que deban satisfacer de forma estructurada y con indicación de los criterios de selección y ciclo de vida aplicados, lo previsto en el apartado 10 de este mismo documento.

## 33. Adecuación de sistemas, aplicaciones y servicios

33.1. En los nuevos sistemas, aplicaciones y servicios se observará lo establecido en las presentes Bases desde la configuración de los mismos, y respecto de los ya existentes a la definitiva adopción de estos criterios, adecuándose a ellos de forma que permitan su cumplimiento.

33.2. De conformidad con la disposición adicional tercera de la Ley 18/2011, de 5 de julio, y con el artículo 6 del Real Decreto 396/2013, de 7 de junio, regulador del Comité técnico estatal de la Administración judicial electrónica, las Administraciones competentes en materia de justicia, dentro del plazo legal, deberán informar a dicho Órgano de coordinación, del cumplimiento de la interoperabilidad, elaborando y remitiendo al mismo, en caso contrario, un plan de adecuación de las actuaciones, así realizadas como previstas, para garantizar la interoperabilidad.

## ANEXO I. CATEGORÍAS DE LOS SISTEMAS

Los sistemas que prestan servicios en la Administración de Justicia o gestionan la información de su ámbito, en lo que se refiere a su seguridad, se clasifican como de categoría Básica, Media o Alta. Esta clasificación se determina por el mayor nivel que alcanza una o más de las dimensiones de seguridad señaladas en el apartado 20, por cada servicio prestado o información gestionada en el sistema, en función del impacto o de las consecuencias que un incidente de seguridad pueda tener sobre ellas. Los niveles aplicables a las dimensiones de seguridad son Bajo, Medio o Alto.

Para determinar la categoría de un sistema, hay que tener en cuenta, por tanto, los servicios que presta y la información que gestiona, y cómo se ven afectados por los incidentes de seguridad en función de cada dimensión de seguridad, de forma que para cada servicio o información se determine el nivel que corresponde la dimensión aplicable.

Para determinar la categoría de un sistema, es de aplicación el Anexo I del Esquema Nacional de Seguridad, teniendo en cuenta la salvedad de que en el marco del presente texto se considera, por imperativo de la aplicación del artículo 53 de la Ley 18/2011 de 5 de julio, una dimensión de seguridad adicional muy relevante en el ámbito judicial, cual es la de Conservación, identificada abreviadamente como “Cs”.

## ANEXO II. MEDIDAS DE SEGURIDAD

En las Bases del Esquema judicial de interoperabilidad y seguridad se detallan las medidas de seguridad que son de aplicación a los sistemas informáticos judiciales siguiendo la estructura del Anexo II del Esquema Nacional de Seguridad.

Sin embargo no todas las medidas se aplican de la misma forma que en el Esquema Nacional de Seguridad, y por ello, en este Anexo se detallan los aspectos en los que las Bases del Esquema judicial de interoperabilidad y seguridad se diferencian del Esquema Nacional de Seguridad. Al final del Anexo se incluye un cuadro que expresa por adición, no solo las diferentes, sino el conjunto de medidas de seguridad aplicables a los sistemas informáticos empleados en la Administración de Justicia.

Todos los sistemas utilizados en la Administración de Justicia deben cumplir con los requisitos mínimos de seguridad definidos en política de seguridad a que se refiere el apartado 22 del cuerpo de este mismo documento.

Para garantizar el cumplimiento de estos requisitos deben aplicarse las medidas de seguridad adecuadas, que se describen en el presente Anexo.

Las medidas de seguridad se estructuran en base:

- Al marco organizativo
- Al marco operacional
- A su categorización como medida de protección

Para determinadas categorías de sistemas serán de aplicación o no ciertas medidas de seguridad, y, además, respecto a algunas medidas, las exigencias de sistemas de una determinada categoría serán superiores a los de categoría inferior.

Cuando se considera la categoría del sistema para establecer una medida de seguridad, se valorarán todas las dimensiones. Sin embargo, para algunas medidas de seguridad solo se consideran algunas de las dimensiones de seguridad.

Para entender la tabla siguiente, debe considerarse que algunas medidas de seguridad son de carácter general, y se aplican tomando en consideración la categoría del sistema (B: Básica, M: Media, A: Alta), lo que implica que en la valoración del sistema se han considerado para los servicios que presta o la información que gestiona el impacto de incidentes de seguridad en todas las dimensiones aplicables e identificadas por sus iniciales: D [Disponibilidad], A [Autenticidad], I [Integridad], C [Confidencialidad], T [Trazabilidad] y Cs [Conservación].

Cuando se toma en consideración, no la categoría del sistema, sino solo ciertas dimensiones de seguridad, lo que es el caso en alguna de las medidas de seguridad de posible aplicación, las iniciales determinan el nivel de seguridad requerido por la dimensión (B; Bajo, M: Medio, A: Alto).

Además, se emplean las siguientes convenciones:

a) Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad en algún nivel determinado se utiliza la voz «aplica».

b) «n.a.» significa «no aplica ».

c) Para indicar que las exigencias de un nivel son iguales a los del nivel inferior se utiliza el signo «=».

d) Para indicar el incremento de exigencias graduado en función del nivel de la dimensión de seguridad, se utilizan los signos «+» y «++».

e) Para indicar que una medida protege específicamente una cierta dimensión de seguridad, ésta se explicita mediante su inicial.

f) En las tablas del presente Anexo se han empleado colores verde, amarillo y rojo de la siguiente forma: el color verde para indicar que una cierta medida se aplica en sistemas de categoría BASICA o superior; el amarillo para indicar las medidas que empiezan a aplicarse en categoría MEDIA o superior; el rojo para indicar las medidas que sólo son de aplicación en categoría ALTA.

A los efectos de facilitar el cumplimiento de lo dispuesto en este Anexo, cuando en un sistema de información existan subsistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse la información y los servicios afectados.

| Bases del Esquema judicial de interoperabilidad y seguridad | | | | | |
|---|---|---|---|---|---|
| Medidas de Seguridad | | Niveles | | | Dimensiones Categorías |
| | | B | M | A | Afectadas |
| | Marco organizativo | | | | |
| Org.4 | Proceso de autorización | aplica | = | + | categoría |
| | Marco operacional | | | | |
| | Planificación | | | | |
| Op.pl.3 | Adquisición de nuevos componentes | aplica | + | = | categoría |
| Op.pl.4 | Dimensionamiento / Gestión de capacidades | n.a. | aplica | = | D,Cs |
| | Explotación | | | | |
| Op.exp.5 | Gestión de cambios | n.a. | aplica | + | categoría |

| | | | | | |
|---|---|---|---|---|---|
| Op.exp.7 | Gestión de incidencias | aplica | = | = | categoría |
| Op.exp.10 | Protección de los registros de actividad | n.a. | n.a. | aplica | I,C,A,T |
| | Medidas de protección | | | | |
| | Protección de las instalaciones e infraestructuras | | | | |
| Mp.if.2 | Identificación de las personas | aplica | = | + | categoría |
| Mp.if.6 | Protección frente a inundaciones | aplica | = | = | D |
| | Gestión del personal | | | | |
| Mp.per.3 | Concienciación | aplica | + | = | categoría |
| Mp.per.4 | Formación | aplica | + | = | categoría |
| | Protección de los soportes de información | | | | |
| Mp.si.1 | Etiquetado | aplica | = | = | C,Cs |
| Mp.si.5 | Borrado y destrucción | aplica | + | = | C,Cs |
| | Protección de las aplicaciones informáticas | | | | |
| Mp.sw.1 | Desarrollo de aplicaciones | aplica | = | = | categoría |
| | Protección de la información | | | | |
| Mp.info.2 | Calificación de la información | aplica | + | = | C,Cs |
| Mp.info.4 | Firma electrónica | aplica | + | ++ | I,A,Cs |
| Mp.info.5 | Sellos de tiempo | n.a. | n.a. | aplica | T,Cs |
| Mp.info.6 | Limpieza de documentos | aplica | = | = | C,Cs |
| Mp.info.9 | Copias de seguridad (backup) | aplica | = | = | D,Cs |

## 1. Marco organizativo [org].

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad. Específicamente:

- Política de seguridad [org.1].
- Normativa de seguridad [org.2].
- Procedimientos de seguridad [org.3].
- Proceso de autorización [org.4].

De todas ellas, se detalla la que difiere de lo descrito en el Anexo II del Esquema Nacional de Seguridad.

### 1.1. Proceso de autorización [Org.4].

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | X | X | X | X | X |

| Categoría | Básica | Media | Alta |
|---|---|---|---|
| | aplica | = | + |

CATEGORÍA BÁSICA

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información:

a) Utilización de instalaciones, habituales y alternativas.

b) Entrada de equipos en producción, en particular, equipos que involucren criptografía.

c) Entrada de aplicaciones en producción.

d) Establecimiento de enlaces de comunicaciones con otros sistemas.

e) Utilización de medios de comunicación, habituales y alternativos.

f) Utilización de soportes de información.

g) Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDA, u otros de naturaleza análoga.

h) Utilización de servicios de terceros, bajo contrato o Convenio.

CATEGORÍA ALTA

Se creará para cada proceso una matriz de roles y responsabilidades que delimiten las responsabilidades para cada actuación.

## 2. Marco operacional [op].

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin. Se agrupan en varios ámbitos según se describe a continuación:

- Planificación [op.pl].
  - Análisis de riesgos [op.pl.1].
  - Arquitectura de seguridad [op.pl.2].

- Adquisición de nuevos componentes [op.pl.3].
- Dimensión/gestión de capacidades [op.pl.4].
- Componentes certificados [op.pl.5]

- Control de acceso [op.acc].
  - Identificación [op.acc.1].
  - Requisitos de acceso [op.acc.2].
  - Segregación de funciones y tareas [op.acc.3].
  - Proceso de gestión de derechos de acceso [op.acc.4].
  - Mecanismos de autenticación [op.acc.5].
  - Acceso local [op.acc.6].
  - Acceso remoto [op.acc.7].
- Explotación [op.exp].
  - Inventario de activos [op.exp.1].
  - Configuración de seguridad [op.exp.2].
  - Gestión de la configuración [op.exp.3].
  - Mantenimiento [op.exp.4].
  - Gestión de cambios [op.exp.5].
  - Protección frente a código dañino [op.exp.6].
  - Gestión de incidencias [op.exp.7].
  - Registro de la actividad de los usuarios [op.exp.8].
  - Registro de la gestión de incidencias [op.exp.9].
  - Protección de los registros de actividad [op.exp.10].
  - Protección de claves criptográficas [op.exp.11].
- Servicios externos [op.ext].
  - Contratación y acuerdos de nivel de servicio [op.ext.1].

- Gestión diaria [op.ext.2].
- Medios alternativos [op.ext.9]

- Continuidad del servicio [op.cont].
  - Análisis de impacto [op.cont.1].
  - Plan de continuidad [op.cont.2].
  - Pruebas periódicas [op.cont.3].
- Monitorización del sistema [op.mon].
  - Detección de intrusión [op.mon.1].
  - Sistema de métricas [op.mon.2].

De todas ellas, solo se detallan las que difieren de lo descrito en el Anexo II del Esquema Nacional de Seguridad.

## *2.1. Planificación [op.pl].*

### *2.1.1. Adquisición de nuevos componentes [op.pl.3].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | X | X | X | X | X |

| Categoría | Básica | Media | Alta |
|---|---|---|---|
| | aplica | + | = |

CATEGORÍA BÁSICA

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

a) Atenderá a las conclusiones del análisis de riesgos: [op.pl.1].

b) Será acorde a la arquitectura de seguridad escogida: [op.pl.2].

c) Contemplará las necesidades técnicas, de formación y de financiación de forma conjunta.

CATEGORÍA MEDIA

Los productos adquiridos deberán seguir un proceso formal de pruebas y compra.

### *2.1.2. Dimensión/gestión de capacidades [op.pl.4].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | | | | X | | X |

| Nivel | Bajo | Medio | Alto |
|---|---|---|---|
| | n.a | aplica | = |

NIVEL MEDIO

Con carácter previo a la puesta en explotación, se realizará un estudio previo que cubrirá los siguientes aspectos:

a) Necesidades de procesamiento.

b) Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.

c) Necesidades de comunicación.

d) Necesidades de personal: cantidad y cualificación profesional.

e) Necesidades de instalaciones y medios auxiliares.

## *2.2. Explotación [Bases del Esquema judicial de interoperabilidad y seguridad-op.exp].*

### *2.2.1. Gestión de cambios [op.exp.5].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | X | X | X | X | X |

| Categoría | Básica | Media | Alta |
|---|---|---|---|
| | n.a. | aplica | + |

CATEGORÍA MEDIA

Se mantendrá un control continuo de cambios realizados en el sistema, de forma que:

a) Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no.

b) Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un equipo que no esté en producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban.

c) Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.

d) Mediante análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema.

e) Los cambios estarán sujetos a la previa aprobación del responsable del sistema.

f) Dichos cambios deberán de estar debidamente registrados, siguiendo los procedimientos establecidos por el responsable del sistema, de tal forma que se garantice la trazabilidad de la evolución del sistema.

CATEGORÍA ALTA

Mediante análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación por los responsables de la información y servicios que correspondan.

### *2.2.2. Gestión de incidencias [op.exp.7].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | X | X | X | X | X |

| Categoría | Básica | Media | Alta |
|---|---|---|---|
| | aplica | = | = |

Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo:

a) Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.

b) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.

c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

d) Procedimientos para informar a las partes interesadas, internas y externas.

e) Procedimientos para:

1. Prevenir que se repita el incidente.
2. Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.
3. Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidencias.

La gestión de incidentes que afecten a datos de carácter personal tendrá en cuenta lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por estas Bases

### *2.2.3. Protección de los registros de actividad [op.exp.10].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | X | X | | X | |

| Nivel | Bajo | Medio | Alto |
|---|---|---|---|
| | n.a. | n.a. | aplica |

NIVEL ALTO

Se protegerán los registros del sistema, de forma que:

a) Se determinará el periodo de retención de los registros.

b) Se asegurará la fecha y hora. Ver [Mp.info.5].

c) Los registros no podrán ser modificados ni eliminados por personal no autorizado.

d) Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.

e) La custodia del registro de auditoría deberá residir, en la medida de lo posible, en otra máquina diferente a la que lo produce y destinada a tal efecto cuyo acceso estará restringido según [op.acc.1].

f) Se debe garantizar la integridad y autenticidad del registro.

## 3. Medidas de protección [Bases del Esquema judicial de interoperabilidad y seguridad -mp].

Las medidas de protección, se centrarán en proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad. Se agrupan en varios ámbitos según se describe a continuación:

- Protección de las instalaciones e infraestructuras [Mp.if].
  - Áreas separadas y con control de acceso [Mp.if.1].
  - Identificación de las personas [Mp.if.2].
  - Acondicionamiento de los locales [Mp.if.3].
  - Energía eléctrica [Mp.if.4].
  - Protección frente a incendios [Mp.if.5].
  - Protección frente a inundaciones [Mp.if.6].
  - Registro de entrada y salida de equipamiento [Mp.if.7].
  - Instalaciones alternativas [Mp.if.9].
- Gestión de personal [Mp.per].
  - Caracterización del puesto de trabajo [Mp.per.1].
  - Deberes y obligaciones [Mp.per.2].
  - Concienciación [Mp.per.3].
  - Formación [Mp.per.4]
  - Personal alternativo [Mp.per.9].
- Protección de los equipos [Mp.eq]
  - Puesto de trabajo despejado [Mp.eq.1].
  - Bloqueo de puesto de trabajo [Mp.eq.2].
  - Protección de equipos portátiles [Mp.eq.3].
  - Medios alternativos [Mp.eq.9].
- Protección de las comunicaciones [Mp.com]
  - Perímetro seguro [Mp.com.1].

- Protección de la confidencialidad [Mp.com.2].
- Protección de la autenticidad y de la integridad [Mp.com.3].
- Segregación de redes [Mp.com.4].
- Medios alternativos [Mp.com.9].

- Protección de los soportes de información [Mp.si]
  - Etiquetado [Mp.si.1].
  - Criptografía [Mp.si.2].
  - Custodia [Mp.si.3].
  - Transporte [Mp.si.4].
  - Borrado y destrucción [Mp.si.5].
- Protección de las aplicaciones informáticas [Mp.sw].
  - Desarrollo de aplicaciones [Mp.sw.1].
  - Aceptación y puesta en servicio [Mp.sw.2].
- Protección de la información [Mp.info].
  - Datos de carácter personal [Mp.info.1].
  - Calificación de la información [Mp.info.2].
  - Cifrado de la información [Mp.info.3].
  - Firma electrónica [Mp.info.4].
  - Sellos de tiempo [Mp.info.5].
  - Limpieza de documentos [Mp.info.6].
  - Copias de seguridad (backup) [Mp.info.9].
- Protección de los servicios [Mp.s].
  - Protección del correo electrónico [Mp.s.1].
  - Protección de servicios y aplicaciones web [Mp.s.2].
  - Protección frente a la denegación de servicio [Mp.s.8].

- Medios alternativos [Mp.s.9].

De todas ellas, solo se detallan las que difieren de lo descrito en el Anexo II del Esquema Nacional de Seguridad.

### *3.1. Protección de las instalaciones e infraestructuras [Mp.if].*

#### *3.1.1. Identificación de las personas [Mp.if.2].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | X | X | X | X | X |

| Categoría | Básica | Media | Alta |
|---|---|---|---|
| | aplica | = | + |

CATEGORÍA BÁSICA

El mecanismo de control de acceso se atendrá a lo que se dispone a continuación:

a) Se identificará a todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información.

b) Se registrarán las entradas y salidas de personas.

CATEGORÍA ALTA

El acceso a las áreas donde se procesa o almacena información sensible debe estar controlado y restringido únicamente a personal autorizado. Para ello, se deben utilizar mecanismos como tarjetas de control de acceso con número de identificación personal, o mecanismos de acceso biométricos como son la huella digital o patrones oculares. Todo ello con arreglo a lo dispuesto en la normativa de protección de datos.

#### *3.1.2. Protección frente a inundaciones [Mp.if.6].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | | | | X | | |

| Nivel | Bajo | Medio | Alto |
|---|---|---|---|
| | aplica | = | = |

Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incidentes fortuitos o deliberados causados por el agua.

### *3.2. Gestión de personal [Mp.per].*

#### *3.2.1. Concienciación [Mp.per.3].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | X | X | X | X | X |

| Categoría | Básica | Media | Alta |
|---|---|---|---|
| | aplica | + | = |

CATEGORÍA BÁSICA

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

En particular, se recordará regularmente:

a) La normativa de seguridad relativa al buen uso de los sistemas.

b) La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.

c) El procedimiento de reporte de incidencias de seguridad, sean reales o falsas alarmas.

CATEGORÍA MEDIA

Debe elaborarse un plan anual de concienciación que tendrá que materializarse. Las instituciones judiciales serán las responsables de establecer los medios oportunos para tal fin.

#### *3.2.2. Formación [Mp.per.4].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | X | X | X | X | X |

| Categoría | Básica | Media | Alta |
|---|---|---|---|
| | aplica | + | = |

CATEGORÍA BÁSICA

Se formará regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones, en particular en lo relativo a:

a) Configuración de sistemas.

b) Detección y reacción a incidentes.

c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

CATEGORÍA MEDIA

Debe elaborarse un plan anual de formación que tendrá que materializarse. Las instituciones judiciales serán las responsables de establecer los medios oportunos para tal fin.

### *3.3. Protección de los equipos [Mp.eq].*

#### *3.3.1. Puesto de trabajo despejado [Mp.eq.1].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | X | X | X | X | X |

| Categoría | Básica | Media | Alta |
|---|---|---|---|
| | aplica | = | = |

Se exigirá que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.

El material documental se almacenará en un depósito destinado a tal efecto que cumpla con lo establecido en [Mp.si.3] y no en depósitos provisionales con un nivel de seguridad inferior. Este material se guardará en lugar cerrado cuando no se esté utilizando.

### *3.4. Protección de los soportes de información [Mp.si].*

#### *3.4.1. Etiquetado [Mp.si.1].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | | | | | X |

| Nivel | Bajo | Medio | Alto |
|---|---|---|---|
| | aplica | = | = |

Los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación.

Los usuarios han de estar capacitados para entender el significado de las etiquetas, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.

### *3.4.2. Borrado y destrucción [Mp.si.5].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | | | | | X |

| Nivel | Bajo | Medio | Alto |
|---|---|---|---|
| | aplica | + | = |

NIVEL BAJO

Con pleno respeto a las normas procesales sobre conservación de la información, custodia de las actuaciones y expurgo de los archivos, se aplicará en su caso la medida de borrado y destrucción de soportes de información a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su anterior contenido.

b) Se destruirán de forma segura los soportes, en los siguientes casos:

   1. Cuando la naturaleza del soporte no permita un borrado seguro.
   2. Cuando así lo requiera el procedimiento asociado al tipo de la información contenida.

c) Se emplearán, preferentemente, productos certificados [op.pl.5].

d) Se llevará un registro de la destrucción de soportes con información sensible, a efectos de auditoría.

e) Se procederá a retirar los soportes con autorización escrita expresa, manteniendo el registro actualizado (registro de salida).

f) La destrucción de los soportes se puede llevar a cabo mediante una empresa externa protegiendo su información a través de un acuerdo de confidencialidad. En tal caso, será obligatorio que dicha empresa realice un certificado de destrucción que garantice las obligaciones contractuales que ha adquirido.

NIVEL MEDIO

Se emplearán productos certificados.

### *3.5. Protección de las aplicaciones informáticas [Mp.sw].*

#### *3.5.1. Desarrollo de aplicaciones [Mp.sw.1].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | X | X | X | X | X |

| Categoría | Básica | Media | Alta |
|---|---|---|---|
| | aplica | = | = |

CATEGORÍA BÁSICA

a) El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción.

b) Se aplicará una metodología de desarrollo reconocida que:

1. Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
2. Trate específicamente los datos usados en pruebas.
3. Permita la inspección del código fuente.

c) Los siguientes elementos serán parte integral del diseño del sistema:

1. Los mecanismos de identificación y autenticación.
2. Los mecanismos de protección de la información tratada. Para su diseño se podrá utilizar información de contexto que informe del nivel de seguridad de la información manejada en el sistema de información judicial, conforme a la regulación legal en materia de seguridad aplicable.
3. La generación y tratamiento de pistas de auditoría.

d) Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

### *3.6. Protección de la información [Mp.info].*

#### *3.6.1. Calificación de la información [Mp.info.2].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|

| | | X | | X |
|---|---|---|---|---|
| | | Bajo | Medio | Alto |
| Nivel | aplica | + | = | |

NIVEL BAJO

a) Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma. Los procedimientos de calificación estarán también a lo que se establezca en la política de gestión de documentos de la institución judicial correspondiente (ver apartado 17).

b) La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.

c) La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el apartado 28 y los criterios generales prescritos en el Anexo I.

d) El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.

e) El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

f) La calificación de la información formará parte de la política de gestión documental que se siga dentro de la institución judicial estando incluida en las primeras fases de dicha gestión donde se estructurará la información en base a la finalidad de la misma.

NIVEL MEDIO

Se redactarán los procedimientos necesarios que describan, en detalle, la forma en que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere; y precisando cómo se ha de realizar:

a) Su control de acceso.

b) Su almacenamiento.

c) La realización de copias.

d) El etiquetado de soportes.

e) Su transmisión telemática.

f) Y cualquier otra actividad relacionada con dicha información.

### *3.6.2. Firma electrónica [Mp.info.4].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | | X | X | | | X |

| Nivel | Bajo | Medio | Alto |
|---|---|---|---|
| | aplica | + | ++ |

Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la vinculación entre el firmante y el contenido firmado, y de establecer la presunción de que existió intención de firmar, es decir, prestación del consentimiento en el sentido que se determine por el contexto (por ejemplo conformidad en recibir una notificación aunque no haya conformidad respecto al contenido de la notificación). Asimismo la firma electrónica debe permitir detectar modificaciones del contenido firmado si se producen.

NIVEL BAJO

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

NIVEL MEDIO

Se emplearán sistemas de firma electrónica avanzada.

Cuando se empleen sistemas de firma basados en certificados, estos serán preferentemente cualificados, según lo dispuesto en el Reglamento europeo UE 910/2014, de 23 de julio, y las normas técnicas publicadas en su desarrollo.

Cuando se reciban firmas basadas en certificados se comprobará su validez tan pronto como sea posible y, una vez bajo la custodia del sistema de gestión procesal se considerarán válidas indefinidamente sin ulteriores comprobaciones tecnológicas. Para ello se adjuntará a la firma, o se referenciará, toda la información pertinente para su fechado, verificación, validación y comprobación de la confiabilidad del prestador de servicios de confianza digital que expidió el certificado.

Cuando se emitan firmas basadas en certificados se incluirá en la firma la información del momento en que se han completado los procesos técnicos básicos de la firma y la información sobre su validez tan pronto como sea posible y, una vez bajo la custodia del sistema de gestión procesal se considerarán válidas indefinidamentesin ulteriores comprobaciones tecnológicas. Solo se usarán certificados expedidos por prestadores de servicios de confianza digital que figuren en la lista TSL de la Unión Europea (según lo dispuesto en el artículo 22 del

Reglamento europe 910/2014, de 23 de julio) y simultáneamente en la lista AATL cuando los documentos se firmen sobre el formato PDF.

Cuando se empleen sistemas de firma electrónica avanzada no basados en certificado se deberá garantizar el cumplimiento de los requisitos del artículo 26 del Reglamento europeo UE 910/2014, de 23 de julio y que los datos de creación de firma están cifrados, salvo puntualmente en caso de prueba pericial y solo si para realizarla fuera preciso que el perito accediera a dichos datos.

NIVEL ALTO

Se aplicarán las medidas de seguridad referentes a firma electrónica exigibles en el nivel Medio, además de las siguientes:

a) Cuando las firmas se basen en certificados, se usarán certificados cualiificados y dispositivos cualificados de creación de firma.

b) Se emplearán, preferentemente, productos certificados según lo indicado en [op.pl.5].

### *3.6.3. Sellos de tiempo [Mp.info.5].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | | | | | X | X |

| Nivel | Bajo | Medio | Alto |
|---|---|---|---|
| | n.a. | n.a. | aplica |

NIVEL ALTO

Los sellos de tiempo datarán de forma irrefutable un contenido como anterior al momento que indique el propio sello de tiempo l

a) Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.

b) Los datos fechados y sus sellos de tiempo se conservarán de forma semejante a los documentos electrónicos firmados electrónicamente. Cuando se gestionen sellos de tiempo se comprobará su validez y, una vez bajo la custodia del sistema de gestión procesal se considerarán válidos indefinidamente sin ulteriores comprobaciones tecnológicas.

c) Se utilizarán productos certificados (según [op.pl.5]) o servicios externos admitidos. Véase [op.exp.10].

d) Se emplearán “sellos cualificados de tiempo electrónicos” acordes con la normativa europea en la materia

### *3.6.4. Limpieza de documentos [Mp.info.6].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | X | | | | | X |

| Nivel | Bajo | Medio | Alto |
|---|---|---|---|
| | aplica | = | = |

En el proceso de limpieza de documentos, se retirará de los mismos, toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento y el emisor muestre su conformidad, siguiendo los procedimientos que se establezcan en la política de gestión de documentos de la institución judicial correspondiente (ver apartado 17).

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Se tendrá presente que el incumplimiento de esta medida puede perjudicar:

a) Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.

b) Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento.

c) A la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer.

### *3.6.5. Copias de seguridad (backup) [Mp.info.9].*

| Dimensiones | C | I | A | D | T | Cs |
|---|---|---|---|---|---|---|
| | | | | X | | X |

| Nivel | Bajo | Medio | Alto |
|---|---|---|---|
| | aplica | = | = |

Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada. Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo

que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad. Las copias de seguridad deberán abarcar:

1. Información de trabajo de la organización.
2. Aplicaciones en explotación, incluyendo los sistemas operativos.
3. Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.
4. Claves utilizadas para preservar la confidencialidad de la información.

a) Para asegurar la conservación con garantías óptimas, las copias de seguridad se realizarán en soporte electrónico, teniendo en cuenta la duración de los mismos y la evolución de su tecnología. Para ello, se reutilizarán los mismos soportes electrónicos o se migrará hacia otros más modernos.

b) Se deberá disponer de segundas copias de los repositorios utilizados en la actividad judicial. La ubicación de dichas copias deberá establecerse en una instalación distinta de la original.

c) Todas las copias de la información cuya destrucción esté autorizada deberán ser destruidas.

## 4. Visión completa

La visión completa del conjunto de medidas a implementar en función de los niveles afectados en las dimensiones aplicables a la información o a los servicios y las categorías de los sistemas se forma mediante la siguiente tabla, en la que se distinguen con la mención “ENS” las medidas de seguridad descritas en el Esquema Nacional de Seguridad, y con la mención “BI”, las medidas descritas en este Anexo:

| Bases del Esquema judicial de interoperabilidad y seguridad | | | | | | |
|---|---|---|---|---|---|---|
| Medidas de Seguridad | | | Niveles | | | Dimensiones Categorías |
| | | | B | M | A | Afectadas |
| | | Marco organizativo | | | | |
| Org.1 | ENS | Política de seguridad | aplica | = | = | categoría |
| Org.2 | ENS | Normativa de seguridad | aplica | = | = | categoría |
| Org.3 | ENS | Procedimientos de seguridad | aplica | = | = | categoría |
| Org.4 | BI | Proceso de autorización | aplica | = | + | categoría |
| | | Marco operacional | | | | |
| | | Planificación | | | | |
| Op.pl.1 | ENS | Análisis de riesgos | aplica | + | ++ | categoría |
| Op.pl.2 | ENS | Arquitectura de seguridad | aplica | + | ++ | categoría |
| Op.pl.3 | BI | Adquisición de nuevos componentes | aplica | + | = | categoría |
| Op.pl.4 | BI | Dimensionamiento / Gestión de capacidades | n.a. | aplica | = | D,Cs |

| | | | | | | |
|---|---|---|---|---|---|---|
| Op.pl.5 | ENS | Componentes certificados | n.a. | n.a. | aplica | categoría |
| | | Control de acceso | | | | |
| Op.acc.1 | ENS | Identificación | aplica | = | = | A,T |
| Op.acc.2 | ENS | Requisitos de acceso | aplica | = | = | I,C,A,T |
| Op.acc.3 | ENS | Segregación de funciones y tareas | n.a. | aplica | = | I,C,A,T |
| Op.acc.4 | ENS | Proceso de gestión de derechos de acceso | aplica | = | = | I,C,A,T |
| Op.acc.5 | ENS | Mecanismo de autenticación | aplica | + | ++ | I,C,A,T |
| Op.acc.6 | ENS | Acceso local | aplica | + | ++ | I,C,A,T |
| Op.acc.7 | ENS | Acceso remoto | aplica | + | = | I,C,A,T |
| | | Explotación | | | | |
| Op.exp.1 | ENS | Inventario de activos | aplica | = | = | categoría |
| Op.exp.2 | ENS | Configuración de seguridad | aplica | = | = | categoría |
| Op.exp.3 | ENS | Gestión de la configuración | n.a. | aplica | = | categoría |
| Op.exp.4 | ENS | Mantenimiento | aplica | = | = | categoría |
| Op.exp.5 | BI | Gestión de cambios | n.a. | aplica | + | categoría |
| Op.exp.6 | ENS | Protección frente a código dañino | aplica | = | = | categoría |
| Op.exp.7 | BI | Gestión de incidencias | aplica | = | = | categoría |
| Op.exp.8 | ENS | Registro de la actividad de los usuarios | aplica | + | ++ | T |
| Op.exp.9 | ENS | Registro de la gestión de incidencias | n.a. | aplica | = | categoría |
| Op.exp.10 | BI | Protección de los registros de actividad | n.a. | n.a. | aplica | I,C,A,T |
| Op.exp.11 | ENS | Protección de claves criptográficas | aplica | + | = | categoría |
| | | Servicios externos | | | | |
| Op.ext.1 | ENS | Contratación y acuerdos de nivel de servicio | n.a. | aplica | = | categoría |
| Op.ext.2 | ENS | Gestión diaria | n.a. | aplica | = | categoría |
| Op.ext.9 | ENS | Medios alternativos | n.a. | n.a. | aplica | D |
| | | Continuidad del servicio | | | | |
| Op.cont.1 | ENS | Análisis de impacto | n.a. | aplica | = | D |
| Op.cont.2 | ENS | Plan de continuidad | n.a. | n.a. | aplica | D |
| Op.cont.3 | ENS | Pruebas periódicas | n.a. | n.a. | aplica | D |
| | | Monitorización del sistema | | | | |
| Op.mon.1 | ENS | Detección de intrusión | n.a. | aplica | = | categoría |
| Op.mon.2 | ENS | Sistema de métricas | n.a. | n.a. | aplica | categoría |
| | | Medidas de protección | | | | |
| | | Protección de las instalaciones e infraestructuras | | | | |
| Mp.if.1 | ENS | Áreas separadas y con control de acceso | aplica | = | = | categoría |
| Mp.if.2 | BI | Identificación de las personas | aplica | = | + | categoría |
| Mp.if.3 | ENS | Acondicionamiento de los locales | aplica | = | = | categoría |
| Mp.if.4 | ENS | Energía eléctrica | aplica | + | = | D |
| Mp.if.5 | ENS | Protección frente a incendios | aplica | = | = | D |
| Mp.if.6 | BI | Protección frente a inundaciones | aplica | = | = | D |
| Mp.if.7 | ENS | Registro de entrada y salida de equipamiento | aplica | = | = | categoría |

| | | | | | | |
|---|---|---|---|---|---|---|
| Mp.if.9 | ENS | Instalaciones alternativas | n.a. | n.a. | aplica | D |
| | | Gestión del personal | | | | |
| Mp.per.1 | ENS | Caracterización del puesto de trabajo | n.a. | aplica | = | categoría |
| Mp.per.2 | ENS | Deberes y obligaciones | aplica | = | = | categoría |
| Mp.per.3 | BI | Concienciación | aplica | + | = | categoría |
| Mp.per.4 | BI | Formación | aplica | + | = | categoría |
| Mp.per.9 | ENS | Personal alternativo | n.a. | n.a. | aplica | D |
| | | Protección de los equipos | | | | |
| Mp.eq.1 | ENS | Puesto de trabajo despejado | aplica | + | = | categoría |
| Mp.eq.2 | ENS | Bloqueo de puesto de trabajo | n.a. | aplica | + | A |
| Mp.eq.3 | ENS | Protección de equipos portátiles | aplica | = | + | categoría |
| Mp.eq.9 | ENS | Medios alternativos | n.a. | aplica | = | D |
| | | Protección de las comunicaciones | | | | |
| Mp.com.1 | ENS | Perímetro seguro | aplica | = | + | categoría |
| Mp.com.2 | ENS | Protección de la confidencialidad | n.a. | aplica | + | C |
| Mp.com.3 | ENS | Protección de la autenticidad y de la integridad | aplica | + | ++ | I,A |
| Mp.com.4 | ENS | Segregación de redes | n.a. | n.a. | aplica | categoría |
| Mp.com.9 | ENS | Medios alternativos | n.a. | n.a. | aplica | D |
| | | Protección de los soportes de información | | | | |
| Mp.si.1 | BI | Etiquetado | aplica | = | = | C,Cs |
| Mp.si.2 | ENS | Criptografía | n.a. | aplica | + | C,I |
| Mp.si.3 | ENS | Custodia | aplica | = | = | categoría |
| Mp.si.4 | ENS | Transporte | aplica | = | = | categoría |
| Mp.si.5 | BI | Borrado y destrucción | aplica | + | = | C,Cs |
| | | Protección de las aplicaciones informáticas | | | | |
| Mp.sw.1 | BI | Desarrollo de aplicaciones | aplica | = | = | categoría |
| Mp.sw.2 | ENS | Aceptación y puesta en servicio | aplica | + | ++ | categoría |
| | | Protección de la información | | | | |
| Mp.info.1 | ENS | Datos de carácter personal | aplica | = | = | categoría |
| Mp.info.2 | BI | Calificación de la información | aplica | + | = | C,Cs |
| Mp.info.3 | ENS | Cifrado de la información | n.a. | n.a. | aplica | C |
| Mp.info.4 | BI | Firma electrónica | aplica | + | ++ | I,A,Cs |
| Mp.info.5 | BI | Sellos de tiempo | n.a. | n.a. | aplica | T,Cs |
| Mp.info.6 | BI | Limpieza de documentos | aplica | = | = | C,Cs |
| Mp.info.9 | BI | Copias de seguridad (backup) | aplica | = | = | D,Cs |
| | | Protección de los servicios | | | | |
| Mp.s.1 | ENS | Protección del correo electrónico | aplica | = | = | categoría |
| Mp.s.2 | ENS | Protección de servicios y aplicaciones web | aplica | = | = | categoría |
| Mp.s.8 | ENS | Protección frente a la denegación de servicio | n.a. | aplica | + | D |
| Mp.s.9 | ENS | Medios alternativos | n.a. | n.a. | aplica | D |

En los aspectos no descritos en el presente Anexo se estará a lo dispuesto en el Anexo II del Esquema Nacional de Seguridad.

## 5. Interpretación

La interpretación del presente Anexo se realizará de conformidad con el contexto normativo en la materia y con la guía técnica de seguridad del ámbito de la Administración de Justicia en relación a las recomendaciones de implementación de la seguridad de la información, de forma que las instituciones judiciales den cumplimiento a los requisitos mínimos de seguridad marcados en el presente texto y en las instrucciones técnicas CCN-STIC correspondientes a la implementación y a diversos escenarios de aplicación, atendiendo el espíritu y finalidad de aquellas.