CONSEJO GENERAL
DEL PODER JUDICIAL

TEST DE COMPATIBILIDAD DE LOS SISTEMAS INFORMÁTICOS DE GESTIÓN PROCESAL

Diciembre de 2.011

CONTENIDO

CONTROL DE CAMBIOS DEL DOCUMENTO

Fecha cambios	Versión que modifica	Descripción de cambios
16/03/2010	**Versión aprobada por el Pleno del CGPJ el 25 de junio de 2008 (v. 2.2-20091110)**	**Capítulo III.** Se establece el módulo básico de cumplimiento del Test de Compatibilidad. **Capítulo III.2.** Dentro del objetivo de registro homogéneo, se concreta que las especificaciones de compatibilidad en este aspecto son las que se detallan en el Reglamento 2/2010, sobre criterios generales de homogeneización de las actuaciones de los servicios comunes procesales. Queda derogada la Instrucción 1/2009 sobre normas para el registro de asuntos en los sistemas de gestión procesal. **Anexo XIV.** Se modifica el cuestionario relativo a las normas para el registro de asuntos, para adecuarlo al reglamento 2/2010.
10/11/2009	**Versión aprobada por el Pleno del CGPJ el 25 de junio de 2008 (v. 2.2-20080625).**	**Capítulo III.2.** Dentro del objetivo de registro homogéneo, se concreta que las especificaciones de compatibilidad en este aspecto son las que se detallan en la Instrucción 1/2009 sobre normas para el registro de asuntos en los sistemas de gestión procesal. **Capítulo III.5.** Se añade un apartado relativo a la obligatoriedad de los sistemas de gestión procesal de incorporar un sistema de alertas para los asuntos de violencia de género. **Anexo XIV.** Se añade el cuestionario relativo a las normas para el registro de asuntos. **Anexo XV.** Se añade el cuestionario relativo al sistema de alertas para los asuntos de violencia de género.
23/6/2008	**Versión aprobada por la Comisión de Informática el 18 de julio de 2.007**	**Capítulo I.** Ajuste del redactado acorde a esta segunda etapa de revisión del Test. **Capítulo III.** Concreción de los objetivos de esta segunda etapa. **Anexos I y III.** Concreción de que el dato "tipoFallo", como la codificación utilizada el mismo, aluden única y exclusivamente a las resoluciones que se remiten al Cendoj. Al mismo se tiempo se revisa la definición del dato "tipoResolucion", así como la codificación utilizada para el mismo, para que recoja las terminaciones anómalas de procedimiento así como para que permita el desglose de los distintos tipos de autos, sentencias y decretos. **Anexo XII.** Se conreta que la situación procesal 2 en los Alardes significa "Pendiente exclusivamente de sentencia o de dictar resolución".
03/12/2007	**v.2.1 de 12 de abril de 2.007**	**Capítulo III**. Se ha actualizado la lista de objetivos, reflejando lo establecido hasta le reunión de Pamplona (15-16/11/2007). También se ha actualizado el párrafo donde se marcan los objetivos a cumplir en esta segunda etapa. **Capítulo III.3.** Segundo párrafo. Se ha ampliado con la

	mención del intercambio de asuntos, recursos y resoluciones al CENDOJ. **Capítulo III.4.** Se ha corregido el año del Primer Test de Compatibilidad: 1999 en vez de 2000. **Capítulo III.4.** El último párrafo se ha modificado en el sentido de hacer una remisión al anexo XIII, sobre los "Criterios de seguridad en los sistemas de información al servicio de la Administración de Justicia", aprobados por el Pleno del CGPJ en septiembre de 2007. **Capítulo III.6.** Se ha añadido el capítulo entero, relativo a los Alardes. **Capítulo IV.1.** Se ha actualizado la tabla informativa de los cuestionarios a cumplimentar. Asimismo se ha eliminado el párrafo en el que se indicaba que para el envío de asuntos, recursos y resoluciones se mantenía el modelo de datos del Test del año 1999. **Capítulo IV.2.** Se ha eliminado el párrafo en el que se indicaba que un sistema es compatible si cumplía con los datos de envío para asuntos, recursos y resoluciones previstos en el Test del año 1999. Al final del capítulo, en conclusiones, se ha añadido la mención a los Alardes. **Capítulo V.1.** Se ha cambiado el título de este capítulo. Antes: "Cuestionarios de intercambio de información". Ahora: "Cuestionarios de especificaciones de información e intercambio". **Capítulo V.4.** Se ha añadido este capítulo, relativo a la guía de lectura de los cuestionarios de alarde. **Anexo XI**. Especificaciones para el intercambio. Se han añadido en sus subcapítulos, las referencias al envío de resoluciones al CENDOJ. **Anexo XII. Se ha añadido este anexo completo. Cuestionario de Alarde.** **Anexo XIII. Se ha añadido este anexo completo. Criterios de seguridad en los sistemas de información al servicio de la Administración de Justicia.**

El control de cambios para las especificaciones de información (tablas de códigos, datos de intercambio, etc) y envios, se reflejan conjuntamente con las especificaciones técnicas.

I - INTRODUCCIÓN.

Por atribución del artículo 230.5 de la Ley Orgánica del Poder Judicial (LOPJ), el Consejo General del Poder Judicial (CGPJ) debe asegurar la compatibilidad de los sistemas informáticos de gestión procesal que se utilicen en la Administración de Justicia: «*... Los programas y aplicaciones informáticas que se utilicen en la Administración de Justicia deberán ser previamente aprobados por el Consejo General del Poder Judicial, quien garantizará su compatibilidad.*

Los sistemas informáticos que se utilicen en la Administración de Justicia deberán ser compatibles entre sí para facilitar su comunicación e integración, en los términos que determine el Consejo General del Poder Judicial. »

El Título VI del Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales (aprobado por Acuerdo del CGPJ de 15 de septiembre de 2005), desarrolla el mandato establecido en el artículo ya mencionado de la LOPJ, estableciendo la creación de la Comisión de Informática Judicial, quién deberá proponer al Pleno del CGPJ la determinación de los elementos que han de reunir los sistemas informáticos que se utilicen en la Administración de Justicia para cumplir las exigencias de compatibilidad necesaria en cuanto a su comunicación, integración y seguridad. Dicha Comisión estará compuesta por el Vocal delegado para la oficina judicial y la informática, que la presidirá, y por cuatro Magistrados, uno por cada orden jurisdiccional. En este aspecto se mantiene la redacción y contenido del Título VI del anterior reglamento 5/1995.

Para abordar este mandato el CGPJ aprobó el 8 de septiembre de 1999 el denominado "Test de compatibilidad", en el que se fijaba un modelo de datos lógico para conseguir un intercambio de información entre sistemas (asuntos, recursos y exhortos), así como unos requisitos mínimos de seguridad. También se dejaron establecidas algunas bases esenciales para la elaboración de la estadística judicial. Bases que no fueron posteriormente desarrolladas.

Uno de los aspectos que se tuvo en cuenta, y que se elaboró en parte, fue la codificación de aquellas tablas de valores necesarias para llevar a cabo el intercambio de información. Codificación que se efectuó a modo de recopilación de los sistemas informáticos implantados en ese momento. Estos valores de dominio no fueron validados por ninguna comisión o grupo de trabajo al margen del que elaboraba el Test, por lo que su aplicación práctica se dejó a la decisión de cada administración competente.

La compatibilidad de todos los sistemas quedó acreditada en fases sucesivas, pero sin que se llevara a la práctica la aplicación deseada: el intercambio telemático.

La Administración de Justicia y, en concreto, el panorama de la informática judicial española, ha sufrido importantes avances, tanto tecnológicos como funcionales, derivados también de profundas reformas legislativas e iniciativas de modernización (LOPJ, Carta de Derechos de los Ciudadanos, Plan de Transparencia Judicial, etc.). También es de destacar las nuevas necesidades que las distintas administraciones han de cubrir, derivadas básicamente de su atribución competencial. Así, se establece una nueva y progresiva revisión del Test que se contempla en varias etapas, acometiéndose ahora la segunda.

Este documento presenta las especificaciones concretas de los distintos objetivos de compatibilidad exigibles a los sistemas de información al servicio de la Administración de Justicia. Asimismo se presenta una metodología para utilizar en la aplicación del test de compatibilidad y una guía de lectura de los cuestionarios. Para ello, el presente documento se desarrolla con la siguiente estructura de capítulos y anexos:

ÁMBITO DE APLICACIÓN

Qué sistemas informáticos al Servicio de la Administración de Justicia están incluidos en las exigencias de compatibilidad.

OBJETIVOS DEL TEST.

En este capítulo se describen los elementos objeto del Test así como la organización de la documentación y productos que se manejan en el mismo.

PROTOCOLO PARA LA APLICACIÓN DEL TEST DE COMPATIBILIDAD A LOS SISTEMAS INFORMÁTICOS DE GESTIÓN PROCESAL.

Donde se describen los objetivos y métodos para la aplicación del Test: desde la identificación de los cuestionarios a manejar hasta la elaboración del informe de resultado de aplicación del Test.

GUÍA DE LECTURA DE LOS CUESTIONARIOS.

Donde se facilitan las claves de lectura de las especificaciones de los cuestionarios.

ANEXOS.

Los cuestionarios propiamente del Test, la codificación utilizada y otros documentos de detalle sobre aspectos relevantes de la compatibilidad,

II - ÁMBITO DE APLICACIÓN

De acuerdo al artículo 98.1 del Reglamento 1/2005 de los aspectos accesorios de las actuaciones judiciales, en relación con el artículo 230.5 de la LOPJ, corresponde al Pleno del Consejo General del Poder Judicial, a propuesta de la Comisión de Informática Judicial, establecer las características que han de reunir los sistemas informáticos que se utilicen en la Administración de Justicia. Son por tanto estos sistemas los que constituyen el ámbito de aplicación del presente Test de compatibilidad.

Sin embargo no hay que olvidar que estos sistemas conviven dentro de un entorno informático con otras aplicaciones y que tienen que interactuar con otros servicios. Por esta razón se procurará tener en cuenta estas necesidades para facilitar la coordinación y compatibilidad con el resto de aplicaciones y sistemas con los que tengan que comunicarse.

Parece oportuno, en estos momentos, hacer mención a los sistemas informáticos que han sido o están siendo implantados, fruto de las iniciativas e inquietudes de las distintas Administraciones competentes.
Su desarrollo tecnológico y la implantación[1] han sido abordados y solventados con las más diversas fórmulas y modalidades de promoción, actuación y cooperación:

- Desarrollo realizado directamente por la administración pública promotora.

[1] Capacitación de los utilizadores del sistema y acciones tendentes a alcanzar el correcto y completo uso del sistema.

- Desarrollo realizado por una firma privada especializada, por encargo específico de una administración pública competente.
- Desarrollo realizado por una firma privada especializada, por su propia iniciativa, y adquisición posterior por una administración pública con competencias.
- Desarrollo mediante una combinación mixta de las modalidades anteriores.
- Implantación llevada a cabo por la administración pública en cuestión y empresas privadas, conjuntamente.

Tal diversidad de escenarios es una consecuencia natural de la gran envergadura que, normalmente, tienen este tipo de proyectos y la marcada especificidad y especialización requeridas en su aplicación en el sector judicial.

III - OBJETIVOS DEL TEST.

El Test de Compatibilidad se aprobó el 8 de septiembre de 1999 con la misión de establecer los criterios necesarios para comprobar el cumplimiento de los objetivos señalados en el propio Test. Objetivos que incidían en la seguridad de los sistemas, la compatibilidad entre ellos, la capacidad de generar información para el conocimiento y las funcionalidades que deben proporcionar. Los criterios exigidos se establecían según los siguientes componentes:

1. Intercambio de información entre sistemas (cooperación jurisdiccional, recursos, expedientes, envío de resoluciones al Centro de Documentación Judicial –CENDOJ-, y comunicación con otros organismos externos).
2. Criterios de seguridad y auditoria (seguridad y acceso a la información, autenticidad e integridad de la misma, alardes, etc.).
3. Plan de explotación para la obtención de estadísticas.

Se consideró que: «el Test de compatibilidad ha de ser, obviamente, un tema abierto, atendiendo al panorama actual: actualización constante en el desarrollo de sistemas informáticos por parte de las Administraciones competentes, evolución de las exigencias del Consejo General del Poder Judicial en materia estadística y de inspección, cambios legislativos ya anunciados y reformas estructurales previstas.»

Al amparo de esta declaración, se modifican los objetivos del Test:

1. Que los Sistemas de Gestión Procesal existentes, así como los futuros, utilicen los conceptos jurídicos expresados en las **tablas de códigos**

incluidas en el presente documento, de acuerdo a lo descrito en el Capítulo V.1: "*Criterios Generales sobre Tablas de Códigos*"

2. **Registro homogéneo de asuntos** en los Sistemas Informáticos de Gestión Procesal.
3. **Intercambio de información entre sistemas**:
    a. **Itineración de exhortos**.
    b. **Itineración de recursos y asuntos**.
    c. **Envío de resoluciones al Centro de Documentación Judicial (CENDOJ)**.
    d. **Envío de información al Fondo de Garantía Salarial (FOGASA)**.
    e. **Envío de datos a Registros Centrales.**
4. **Seguridad y auditoría**.
5. **Gestión del conocimiento**. Definición y establecimiento de los **hitos relevantes** en la tramitación procesal de los expedientes.
6. **Alardes**.
7. Establecimiento de las **funcionalidades mínimas** que deben contener los sistemas Informáticos de Gestión Procesal.
8. **Libros de Registro.**

Por la propia evolución de los sistemas de información al servicio de la Administración de Justicia, así como por las necesidades crecientes de interoperabilidad, es previsible que el alcance de estos objetivos se vea afectado o, incluso, surjan de nuevos.

Para ello, el Test de Compatibilidad ha de ser una especificación flexible que permita abordar la consecución de todos los objetivos por etapas; en primer lugar, porque algunos son consecuencia de los anteriores, y en segundo lugar, porque no resulta factible acometer de una sola vez todas las adaptaciones que necesitan los sistemas para contemplar los requisitos de la revisión del Test de Compatibilidad.

Los objetivos referidos a tablas de códigos, registro homogéneo (Instrucción 1/2009), itineración de exhortos, seguridad e hitos ya se abordaron en etapas anteriores, siendo aprobados por el Pleno del Consejo General del Poder.

En la etapa actual se establece un **módulo básico de cumplimiento** del Test de Compatibilidad que incluye la consecución de los objetivos **1, 2, 3-a, 3-b, 3-c, 4, 5 y 6.** Algunos ya se aprobaron con anterioridad, pero han evolucionado hacia nuevos requerimientos (es el caso del registro homogéneo, donde se ha actualizado conforme al Reglamento 2/2010). Otros se han añadido (por ejemplo, envío de resoluciones al CENDOJ). En concreto, el módulo básico de cumplimiento queda conformado en:

- **Objetivo 1:** tablas de códigos
- **Objetivo 2:** registro homogéneo de asuntos, según Reglamento 2/2010.
- **Objetivo 3:** intercambio de información. Como módulo básico de cumplimiento se establece:
    a. la obligatoriedad en la recepción de exhortos, recursos y asuntos itinerados electrónicamente desde órganos judiciales radicados fuera del territorio ministerial o autonómico propio.
    b. Envío de resoluciones al Cendoj
        i. Remitir, de forma estructurada, los datos básicos del asunto y de la resolución, adjuntando el texto completo en un formato estándar.
- **Objetivo 4:** medidas de seguridad.
- **Objetivo 5:**
    a. hitos relevantes de la tramitación aprobados hasta la fecha.

b. sistema de alertas / avisos para los asuntos de violencia de género.

- **Objetivo 6:** alardes.

III.1 - PRIMER OBJETIVO. CODIFICACIÓN DE VALORES

Este primer objetivo persigue que, al amparo del Plan de Transparencia acordado por el Consejo de Ministros de 21 de octubre de 2005, los Sistemas de Gestión Procesal, compatibles conforme establece el presente Test, recojan en sus modelos de datos los conceptos imprescindibles para que cualquier juez, magistrado, secretario judicial o personal de los cuerpos de funcionarios de la Administración de Justicia utilice los mismos conceptos con independencia del Sistema de Gestión Procesal utilizado. De esta forma, la extracción de datos de los Sistemas de Gestión Procesal que contempla el Plan de Transparencia será más fácil, por cuanto se ofrecerá a la Comisión Nacional de Estadística un rango de valores consensuado por todas las Administraciones.

El Plan de Transparencia Judicial, en el último párrafo del punto 2.1 del apartado 2. Tecnologías de la información y comunicaciones, del título IV. Instrumentos del Plan de Transparencia Judicial, considera necesaria «*la convergencia entre los modelos de datos coexistentes, los rangos en los dominios de valores –asuntos, procedimientos, fases, estados-, la convergencia tecnológica…*».

Teniendo en cuenta que la explotación estadística de los sistemas ya fue acordada como un objetivo en el Test de Compatibilidad, y se continúa contemplando en los puntos 5 y 6, el objetivo ahora fijado ayudará a la consecución de dicha explotación.

III.2 - SEGUNDO OBJETIVO. REGISTRO HOMOGÉNEO DE ASUNTOS

El segundo objetivo, que parece muy ambicioso, no es sino una consecuencia del primero.

Existe una serie de datos, como la identificación de demandante y demandado, nombre y apellidos de procurador y abogado, número de colegiado de los representante legales, etcétera, que son obligatorios pues las leyes procesales exigen su constancia por ser necesarios para que jueces y magistrados ejerzan su labor jurisdiccional

La implantación de un registro homogéneo conseguirá que todos los asuntos que se registren en cualquier órgano judicial, lo sean de conformidad a los conceptos jurídicos reflejados en las tablas del presente documento. De esta forma, los asuntos o procedimientos se denominarán igual en cualquier órgano judicial y la materia de la que traten se limitará a una de las voces proporcionadas en dichas tablas.

Sin perjuicio de lo anterior, los Sistemas de Gestión Procesal podrán realizar desgloses de mayor detalle si las Salas de Gobierno o las Comisiones Mixtas previstas en el artículo 17 del Reglamento 1/2000, de los Órganos de Gobierno de los Tribunales, allí donde existan, lo consideran necesario, pero la raíz del desglose será una voz existente en cualquier Sistema.

Debe aclararse que, si los Sistemas de Gestión Procesal tienen una codificación de las voces o conceptos distinta a la utilizada en las Tablas, podrán mantenerla, aunque se recomienda que, progresivamente, vayan actualizando los códigos y conceptos de los asuntos y procedimientos en trámite.

En consonancia con los objetivos del registro homogéneo, el 12 de abril entró en vigor el Reglamento 2/2010, sobre criterios generales de homogeneización de las actuaciones de los servicios comunes procesales. Dicho Reglamento acomete una serie de normas y reglas que deben cumplirse en el tratamiento informático de registro de asuntos y, por tanto, serán consideradas para la evaluación de los sistemas de gestión procesal. Para ello se ha incorporado en el Test la especificación de la información (datos) para el registro de asuntos (Homogeneización Asuntos.xsd) y el cuestionario de evaluación.

III.3 - TERCER OBJETIVO. INTERCAMBIO DE INFORMACIÓN ENTRE SISTEMAS

El tercer objetivo fue considerado como fundamental en la primera redacción del Test de Compatibilidad.

En la primera y segunda etapa de la revisión del Test se han acordado unos formatos de intercambio para los exhortos (solicitudes y devoluciones de cooperación jurisdiccional), recursos (envío y devolución), asuntos (envío) y resoluciones (envío al CENDOJ), recogidos en documentos XML-Schema. Los Sistemas de Gestión Procesal deberán de ser capaces de generar **todos los datos** contenidos en dichas especificaciones. Sin embargo, se han introducido, para cada dato, las variables de obligatoriedad y opcionalidad respondiendo así a distintas situaciones:

- Determinados datos procesalmente no son siempre exigibles (por ejemplo, la fecha de vencimiento del exhorto).
- Aún siendo exigibles, no lo son hasta un determinado momento procesal (defensa y representación del demandado, ...).
- Por regla general, los sistemas de gestión procesal, previendo estas situaciones, tienen establecidos como opcionales un determinado número de campos de la base de datos. Este aspecto puede

provocar que, aun siendo conocida la información, el personal encargado no la actualice.

Así, los campos señalados como "obligatorios" son los mínimos imprescindibles para que la itineración se realice de forma correcta y el Sistema de Gestión pueda declararse compatible en el apartado de comunicación conforme a las reglas de este Test.

En el caso de los exhortos, para asegurar que se remiten todos los datos, tal como establece la Ley de Enjuiciamiento Civil, aquellos que están definidos como opcionales deberán estar también incluidos en el "documentoSolicitud" (copia del exhorto, tal y como lo genera el Sistema de Gestión Procesal), siempre y cuando sean procedentes desde el punto de vista procesal.

Así, un exhorto podrá o no tener una fecha determinada antes de la cual deberán de practicarse las diligencias interesadas. En el documento exhorto.xsd, este dato recibe el nombre de "fechaVencimiento". El Sistema de Gestión Procesal deberá poder transmitir ese dato dentro del elemento "fechaVencimiento" y dentro de "documentoSolicitud". Es un dato obligatorio, como el resto de los contemplados en la especificación, y su envío será obligatorio siempre y cuando procesalmente deba de transmitirse.

Las especificaciones indicadas en los correspondientes anexos expresan la información que debe contener cada uno de los diferentes tipos de intercambio, independientemente de la Instancia Judicial y Ámbito Jurisdiccional, y reflejan por un lado la colección de datos para cada uno de estos intercambios, y por otro lado cómo entenderse para llevar a cabo los intercambios.

Todas las especificaciones se presentan utilizando el estándar propuesto en la versión anterior del Test, concretamente la familia de lenguajes XML (siglas de e*Xtended Markup Language)*.

Las especificaciones de los datos y estructuras de datos de intercambio se realizan con el lenguaje XML-Schema, estándar definido y publicado por la W3C (siglas de *World Wide Web Consortium*), obteniendo documentos de especificación denominados XSD (siglas de *XML-Schema Document)*.

Los dominios de valores de los datos tratados como códigos, dada su extensión y variabilidad, se definen externamente a los documentos XML-Schema y se presentan en documentos XML. Así pues, el dominio de valores de un dato, o también conocida como tabla de códigos, como puede ser el caso del código de Unidad Funcional y la tabla de todos los distintos Juzgados y Tribunales del Estado, se recoge en un documento XML independientemente de los documentos XSD.

SOAP (siglas de *Simple Object Access Protocol*) es el protocolo a utilizar para los intercambios de información, ya que se trata del protocolo estándar definido y publicado por la W3C para el intercambio de datos XML.

El formato y operaciones SOAP concretas para materializar los intercambios de información, de acuerdo a las especificaciones de datos y estructuras definidas, se especifica como un servicio web utilizando el lenguaje WSDL (siglas de *Web Service Definition Language).*

Para conocer un mayor detalle de la especificación técnica de los intercambios ver los anexos correspondientes.

III.4 - CUARTO OBJETIVO. SEGURIDAD

Uno de los principales componentes del Test de Compatibilidad, ya establecido en el año 1999, hace mención a los requerimientos de seguridad que han de cumplir los sistemas informáticos de gestión procesal. El CGPJ, al amparo de lo dispuesto en el artículo 230 de la Ley Orgánica del Poder Judicial y Título V del Reglamento núm. 1/2005, de 15 de septiembre, de los Aspectos Accesorios de las Actuaciones Judiciales, tiene el mandato de establecer y aprobar dichos requerimientos.

En esta nueva versión del Test serán de aplicación y obligado cumplimiento para todos los sistemas lo establecido en el documento capítulo V.2 "**Criterios de seguridad en los sistemas de información al servicio de la Administración de Justicia**", aprobado por el Pleno del Consejo General del Poder Judicial, en su sesión de 13 de septiembre de 2007, a propuesta de la Comisión de Informática Judicial.

III.5 - QUINTO OBJETIVO. GESTIÓN DEL CONOCIMIENTO. HITOS RELEVANTES EN LA TRAMITACIÓN

Cuando se iniciaron los trabajos para desarrollar un nuevo sistema de Información para la Gestión Judicial, se fijó como objetivo primordial la obtención, mediante el análisis de ciertos datos proporcionados por los Sistemas de Gestión Procesal, de información real sobre la carga de trabajo de los órganos judiciales, de tal forma que dicha información pudiera ser utilizada, por el Consejo General del Poder Judicial y por los Gestores de las Administraciones con competencias asumidas en materia de Justicia, para una mejor distribución de los recursos materiales y humanos.

La información que los Sistemas de Gestión Procesal deben suministrar de cada asunto o procedimiento se limita a una relación de fechas correspondientes a hitos relevantes de su tramitación, que pueden considerarse como momentos iniciales o finales de determinadas etapas procesales. Para la selección de estos hitos se ha tenido en cuenta su futura explotación, que siempre tendrá presente el objetivo de prestar información a las Administraciones pero también, y fundamentalmente, de servir de control para la gestión de la tramitación en los propios órganos judiciales.

En el cuestionario correspondiente (ver Anexo VII) se recogen las fechas que definen los hitos procesales interesados, sin perjuicio de que el sistema pueda recoger otros hitos complementarios a los expresados. El volumen de la información recogida así como el resultado de su explotación determinará la evolución futura de esta información, pudiéndose aumentar el número de fechas solicitadas o acordar la supresión de alguna de ellas.

Lógicamente, los asuntos y procedimientos no podrán completar todas las fechas por dos sencillas razones: algunas de las fechas no les son aplicables por su propia definición y en algunos casos no se dictará nunca una resolución que de lugar al hito en la tramitación que aquí se determina mediante una fecha (por ejemplo, la admisión a trámite de la ejecución provisional, o la admisión a trámite del recurso de apelación).

III.5.1 - Sistema de alertas para los asuntos de violencia de género.

El Pleno del CGPJ, en su sesión de 23 de diciembre de 2008, acordó *"dirigirse al Ministerio de Justicia, así como a las Comunidades Autónomas con competencias en materia de Justicia, trasladándoles la necesidad de implantación, sin mayor dilación, en los sistemas informáticos de los*

órganos jurisdiccionales de su territorio que tengan encomendada la instrucción o enjuiciamiento de delitos vinculados con la Violencia de Género regulada por la Ley Orgánica 1/2004, de Medidas de Protección Integral contra la Violencia de Género, de alertas informáticas que adviertan de la inminencia de comunicar a las víctimas de delitos de Violencia de Género – bien denunciantes, bien ofendidas por el delito- de cualquier acto procesal que pueda afectar a su seguridad, como el alcance y vigencia de medidas cautelares adoptadas, la situación penitenciaria del imputado o condenado en sede de orden de protección, sobre el sobreseimiento de las actuaciones que pueda acordarse, sobre la fecha y lugar de celebración del juicio oral o sobre la sentencia recaída, tanto en primera como en segunda instancia, con el requisito de que los sistemas impidan la continuación de la tramitación en tanto no conste realizado el correspondiente acontecimiento informático que garantice haberse evacuado el acto de comunicación."

En ejecución de este acuerdo, la Comisión de Modernización e Informática del CGPJ acordó el catálogo de resoluciones que deben tener contemplado los sistemas de gestión procesal para ser notificadas a las víctimas. Asimismo estableció como fecha máxima la del 1 de septiembre de 2009 para que dichos sistemas incorporaran un sistema de alertas a los usuarios en relación con dichas resoluciones.

El contenido del acuerdo de la Comisión de Modernización e Informática será la base para la evaluación de los sistemas informáticos.

III.6 - SEXTO OBJETIVO. ALARDES

Los Alardes, regulados en los artículos 317.3 de la Ley Orgánica del Poder Judicial, y 158 a 169 del Reglamento 1/1995, de 7 de Junio, de la Carrera Judicial, tienen como finalidad constituir un **mecanismo de control sobre la situación del órgano jurisdiccional**, y de la actuación durante un tiempo determinado del Juez que cesa, a la vez que supone una garantía para

los propio Jueces entrante y saliente. Por su parte, el Servicio de Inspección del CGPJ tiene como función respecto de los Alardes, examinar su contenido, de modo que este sea coherente con el resto de la información obrante en el Consejo y, proponer, en su caso, las medidas correctoras que puedan proceder.

El Servicio de Inspección del CGPJ ha fijado el contenido de estos alardes, basándose en relaciones de todos los asuntos pendientes que tiene un órgano judicial, agrupadas en determinadas situaciones procesales. Asimismo, establece también la necesidad de obtener resúmenes totalizados.

El núcleo principal de los sistemas de gestión procesal es el registro y tramitación de los expedientes judiciales. Es en estas áreas donde se recogen los datos de identificación situación procesal de los asuntos, por lo que de dichos sistemas se puede obtener la información necesaria para confeccionar un Alarde Automatizado.

Ante estos supuestos, es objetivo del Test de Compatibilidad establecer los estándares que definen el contenido y formato de un alarde tanto parar su posterior envio al CGPJ como para su análisis local. Los SIGP podrán completar de forma separada el alarde con otra información que los responsables del órgano pudieran considerar necesaria. En esta etapa, se establecen los datos de los asuntos y escritos que se deben contemplar en las relaciones individualizadas, así como la información que debe contener el resumen totalizado. En etapas posteriores se establecerá el método de envío de esta información al CGPJ.

IV - PROTOCOLO PARA LA APLICACIÓN DEL TEST DE COMPATIBILIDAD A LOS SISTEMAS INFORMÁTICOS DE GESTIÓN PROCESAL.

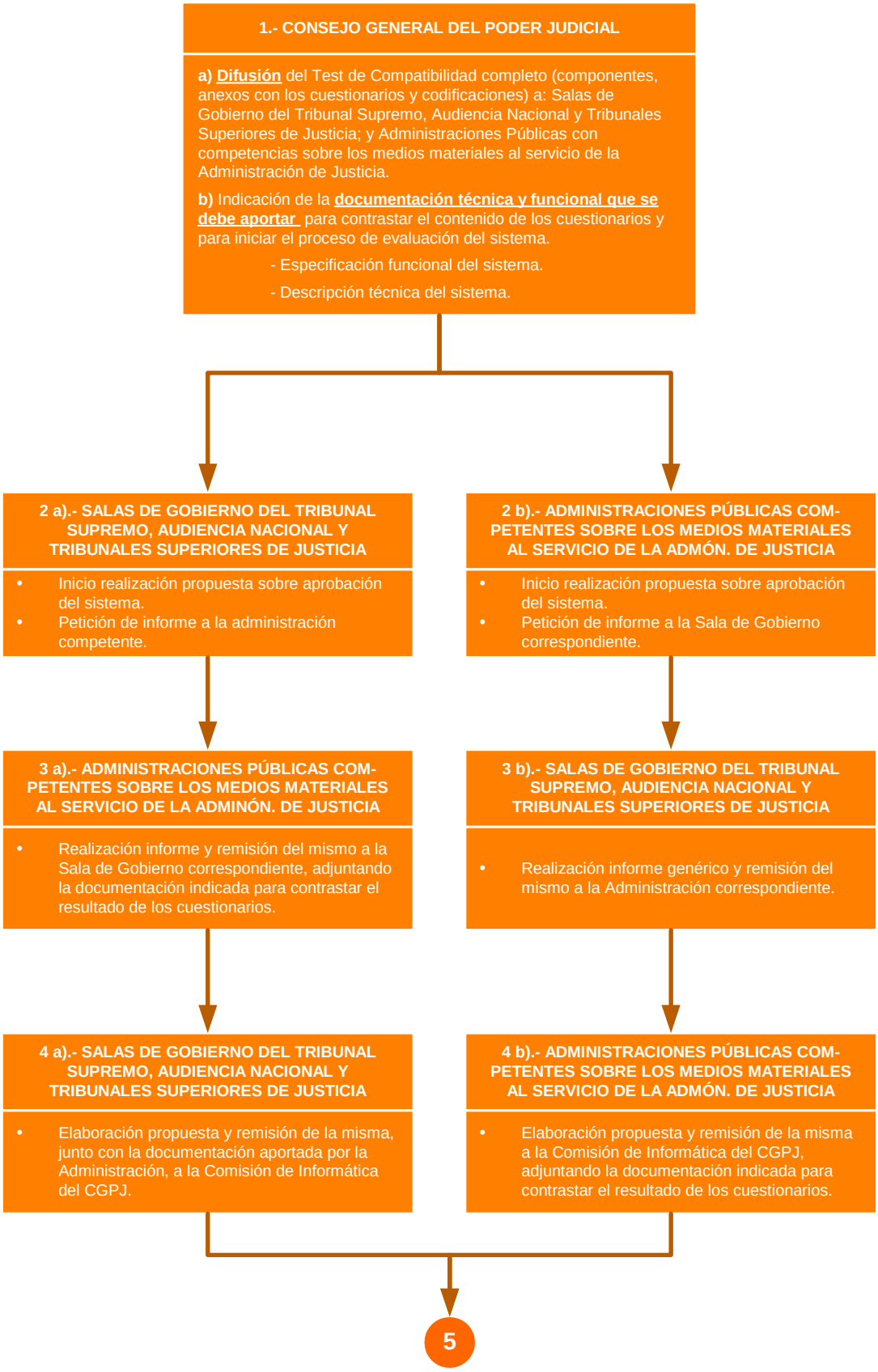
El Título VI del Reglamento 1/2005, de los Aspectos Accesorios de las Actuaciones Judiciales, aprobado por Acuerdo del Pleno del Consejo General del Poder Judicial de 15 de septiembre de 2005, establece ya el procedimiento de aprobación de los programas, aplicaciones y sistemas informáticos de la Administración de Justicia.

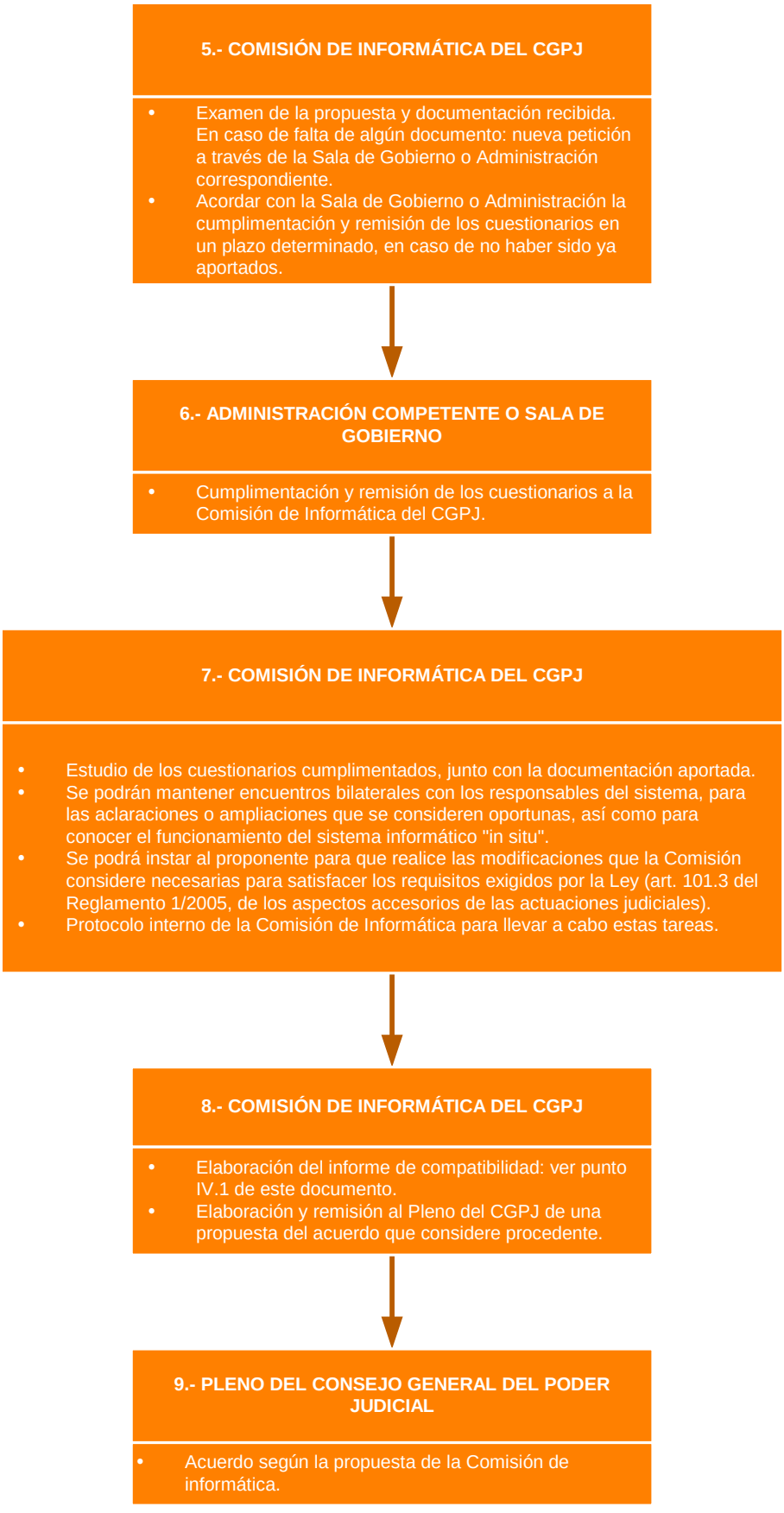
Básicamente, es el artículo 101 el que establece los procedimientos a seguir:

> *"**Art. 101. 1**. La Comisión de Informática Judicial deliberará y resolverá sobre las propuestas de aprobación de programas y aplicaciones que le eleven las Salas de Gobierno de los Tribunales Superiores de Justicia, de la Audiencia Nacional y del Tribunal Supremo. Cada propuesta deberá ir acompañada del informe de los órganos con competencias sobre medios materiales al Servicio de la Administración de Justicia. A dichas Salas corresponde recabarlo.*
>
> ***2**. También podrán presentar propuestas las Administraciones Públicas con competencias sobre los medios materiales al servicio de la Administración de Justicia. Cada propuesta deberá ir acompañada del informe de la Sala de Gobierno del Tribunal Superior de Justicia, de la Audiencia Nacional o del Tribunal Supremo.*
>
> ***3**. La Comisión de Informática Judicial podrá instar al proponente para que realice las modificaciones que la Comisión considere necesarias para satisfacer los requisitos exigidos por la Ley.*
>
> ***4**. Una vez instruida al efecto, la Comisión de Informática Judicial propondrá al Pleno del Consejo la adopción del acuerdo que considere procedente."*

El protocolo que se propone en el presente documento parte de la base y complementa dicho reglamento, estableciéndose unas pautas de actuación y una metodología concreta para la aplicación del Test de compatibilidad a los distintos sistemas.

En los siguientes gráficos se especifica el protocolo:


1.- CONSEJO GENERAL DEL PODER JUDICIAL
a) Difusión del Test de Compatibilidad completo (componentes, anexos con los cuestionarios y codificaciones) a: Salas de Gobierno del Tribunal Supremo, Audiencia Nacional y Tribunales Superiores de Justicia; y Administraciones Públicas con competencias sobre los medios materiales al servicio de la Administración de Justicia.
b) Indicación de la documentación técnica y funcional que se debe aportar para contrastar el contenido de los cuestionarios y para iniciar el proceso de evaluación del sistema.
- Especificación funcional del sistema.
- Descripción técnica del sistema.
2 a).- SALAS DE GOBIERNO DEL TRIBUNAL SUPREMO, AUDIENCIA NACIONAL Y TRIBUNALES SUPERIORES DE JUSTICIA
• Inicio realización propuesta sobre aprobación del sistema.
• Petición de informe a la administración competente.
2 b).- ADMINISTRACIONES PÚBLICAS COMPETENTES SOBRE LOS MEDIOS MATERIALES AL SERVICIO DE LA ADMÓN. DE JUSTICIA
• Inicio realización propuesta sobre aprobación del sistema.
• Petición de informe a la Sala de Gobierno correspondiente.
3 a).- ADMINISTRACIONES PÚBLICAS COMPETENTES SOBRE LOS MEDIOS MATERIALES AL SERVICIO DE LA ADMINÓN. DE JUSTICIA
• Realización informe y remisión del mismo a la Sala de Gobierno correspondiente, adjuntando la documentación indicada para contrastar el resultado de los cuestionarios.
3 b).- SALAS DE GOBIERNO DEL TRIBUNAL SUPREMO, AUDIENCIA NACIONAL Y TRIBUNALES SUPERIORES DE JUSTICIA
• Realización informe genérico y remisión del mismo a la Administración correspondiente.
4 a).- SALAS DE GOBIERNO DEL TRIBUNAL SUPREMO, AUDIENCIA NACIONAL Y TRIBUNALES SUPERIORES DE JUSTICIA
• Elaboración propuesta y remisión de la misma, junto con la documentación aportada por la Administración, a la Comisión de Informática del CGPJ.
4 b).- ADMINISTRACIONES PÚBLICAS COMPETENTES SOBRE LOS MEDIOS MATERIALES AL SERVICIO DE LA ADMÓN. DE JUSTICIA
• Elaboración propuesta y remisión de la misma a la Comisión de Informática del CGPJ, adjuntando la documentación indicada para contrastar el resultado de los cuestionarios.
5


5.- COMISIÓN DE INFORMÁTICA DEL CGPJ
• Examen de la propuesta y documentación recibida. En caso de falta de algún documento: nueva petición a través de la Sala de Gobierno o Administración correspondiente.
• Acordar con la Sala de Gobierno o Administración la cumplimentación y remisión de los cuestionarios en un plazo determinado, en caso de no haber sido ya aportados.
6.- ADMINISTRACIÓN COMPETENTE O SALA DE GOBIERNO
• Cumplimentación y remisión de los cuestionarios a la Comisión de Informática del CGPJ.
7.- COMISIÓN DE INFORMÁTICA DEL CGPJ
• Estudio de los cuestionarios cumplimentados, junto con la documentación aportada.
• Se podrán mantener encuentros bilaterales con los responsables del sistema, para las aclaraciones o ampliaciones que se consideren oportunas, así como para conocer el funcionamiento del sistema informático "in situ".
• Se podrá instar al proponente para que realice las modificaciones que la Comisión considere necesarias para satisfacer los requisitos exigidos por la Ley (art. 101.3 del Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales).
• Protocolo interno de la Comisión de Informática para llevar a cabo estas tareas.
8.- COMISIÓN DE INFORMÁTICA DEL CGPJ
• Elaboración del informe de compatibilidad: ver punto IV.1 de este documento.
• Elaboración y remisión al Pleno del CGPJ de una propuesta del acuerdo que considere procedente.
9.- PLENO DEL CONSEJO GENERAL DEL PODER JUDICIAL
• Acuerdo según la propuesta de la Comisión de informática.

IV.1 - CUESTIONARIOS E INFORME DE COMPATIBILIDAD.

Los documentos básicos que constituyen la aplicación del Test sobre un sistema de información concreto son:

1) Cuestionarios del Test cumplimentados.
2) Informe de Compatibilidad.

Cuestionarios

Los cuestionarios del Test a cumplimentar, Anexos de este documento, son los siguientes:

Tipo	Denominación	Especificación	Cuestionario
General	Tablas de códigos	Tablas de códigos a utilizar tanto para el registro homogéneo como para los intercambios.	Anexo II
Intercambio entre sistemas	Solicitud de Cooperación Jurisdiccional	Datos para solicitar la realización de un exhorto a una Unidad Funcional (U.F.)	Anexo III.1
Intercambio entre sistemas	Devolución Cooperación Jurisdiccional	Datos para comunicar el resultado de un exhorto a la U. F. exhortante.	Anexo III.2
Intercambio entre sistemas	Envío de recurso interpuesto	Datos para elevar un recurso	Anexo IV.1
Intercambio entre sistemas	Devolución de recurso	Datos para comunicar la resolución de un recurso a la U. F. recurrida..	Anexo IV.2
Intercambio entre sistemas	Remisión de asunto completo	Datos para remitir o elevar un asunto completo a una Unidad Funcional.	Anexo V.1
Intercambio con CENDOJ	Envío a CENDOJ	Datos para incluir resoluciones de las UU.FF. como jurisprudencia.	Anexo VI.1
Gestión del conocimiento	Hitos procesales	Relación de fechas correspondientes a hitos relevantes de la tramitación de los expedientes, para su posterior explotación	Anexo VII
Gestión del conocimiento	Alardes	Relación de datos relativos a asuntos y escritos pendientes, así como resúmenes globalizados	Anexo VIII

Para evitar información de carácter repetitivo, se proporcionan en el Anexo I aquellas definiciones que son comunes en los distintos tipos de intercambio.

El formato y lectura de los mismos se detalla en el capítulo siguiente.

Informe de compatibilidad.

El informe de compatibilidad es el producto principal que se obtiene de la aplicación del Test. Para realizarlo, previamente se tendrán que haber cumplimentado los cuestionarios del Test.

Este informe ha de mostrar, fundamentalmente, los aspectos que el sistema de información debe subsanar para llegar a ser compatible. Pudiendo éstos ser ninguno, uno o varios. Por ejemplo: diferencias de formato del dato NIG o inexistencia del mismo.

IV.2 - CRITERIOS PARA DETERMINAR LA COMPATIBILIDAD DEL SISTEMA

Para la cumplimentación de los **cuestionarios de intercambio** debe tenerse en cuenta que todos los datos definidos son de obligado cumplimiento y, más concretamente que:

- Un sistema ha de poder recibir y tratar un mensaje de Intercambio con todos y cada uno de los datos definidos, independientemente de su calidad de opcional u obligatorio. Este aspecto debe tratarse en la totalidad y en caso de un sistema que no cumpla este principio, la casilla RESULTADO DEL TEST será negativa y el sistema considerado NO COMPATIBLE.

Capacidad de enviar/recibir esta información de acuerdo a las especificaciones de intercambio? ☐

RESULTADO DEL TEST
☐

- **Un sistema ha de poder enviar todos y cada uno de los datos definidos con las mismas características.** Este aspecto debe tratarse dato por dato requiriendo tener cumplimentadas afirmativamente las casillas "Existe?", para señalar si el sistema puede enviar el dato con las mismas características de formato y dominio de valores que los definidos en el tipo de datos correspondiente. En caso de no producirse en alguno de ellos el RESULTADO DEL TEST será negativo y el sistema considerado NO COMPATIBLE.

Para la cumplimentación del **cuestionario de tablas de códigos** debe tenerse en cuenta que el sistema debe contemplar todos los conceptos determinados por el CGPJ (ver capítulo V.1, de criterios generales sobre la codificación)

Existen los mismos conceptos? ☐
Se utilizan con los mismos códigos? ☐

El sistema será compatible si se ha verificado positivamente que "Existen los mismos conceptos", es decir que internamente los sistemas contemplen éstos y no otros. Se permitirá, no obstante, tener desgloses de conceptos, tal como queda reflejado en los Criterios Generales (ver capítulo V.1).

El Test, por ejemplo, para una tabla fija los siguientes elementos:

Código	Concepto
0301	Lesiones
0302	Lesiones cualificadas
0303	Lesiones imprudentes

Suponiendo que tenemos 4 sistemas de gestión procesal con el siguiente resultado para esta tabla:

SISTEMA 1		SISTEMA 2		SISTEMA 3		SISTEMA 4	
Código	Concepto	Código	Concepto	Código	Concepto	Código	Concepto
0301	Lesiones	0201	Lesiones	---	---	---	---
0302	Lesiones cualificadas	0202	Lesiones cualificadas	0802	Lesiones cualificadas	0302	Lesiones cualificadas
0303	Lesiones imprudentes	0203	Lesiones imprudentes	0803	Lesiones imprudentes	0303	Lesiones imprudentes
030301	Lesiones imprudentes – accidente de tráfico	---	---	---	---	---	---
				8515	Desacato		
¿Existen los mismos conceptos? ☑ ¿Se utilizan con los mismos códigos? ☑		¿Existen los mismos conceptos? ☑ ¿Se utilizan con los mismos códigos? ☒		¿Existen los mismos conceptos? ☒ ¿Se utilizan con los mismos códigos? ☒		¿Existen los mismos conceptos? ☒ ¿Se utilizan con los mismos códigos? ☑	

A la vista de este ejemplo, ¿Qué resultado de compatibilidad se establecería para cada sistema?

SISTEMA 1	**Es compatible** porque tiene los mismos conceptos, aunque uno de ellos lo ha desglosado. Además cumple con las mismas características de codificación, que le facilitarán, por ejemplo, los mecanismos de intercambio.
SISTEMA 2	**Es compatible** porque tiene los mismos conceptos, aunque no cumple con las mismas características de codificación. Cuando se comunique con otros sistemas deberá hacerlo con los códigos establecidos por el CGPJ.
SISTEMA 3	**NO es compatible** porque le falta un concepto y añade otro que no es desglose de los previstos en el Test. Además, con los conceptos coincidentes no cumple con las mismas características de codificación, aunque este valor ya es irrelevante.
SISTEMA 4	**NO es compatible** porque le falta un concepto. Sin embargo, con el resto de valores cumple con las mismas características de codificación.

Para la cumplir con la compatibilidad el sistema ha de tener previstos los **Hitos relevantes de la tramitación** definidos en este test. El cuestionario se cumplimentará indicando si existe o no cada hito.

Existe? ☐

En conclusión, tenemos que se considerará un sistema COMPATIBLE si y solo si es capaz de:

- Aceptar y tratar un mensaje de intercambio con la totalidad de datos definidos.
- Enviar un mensaje de intercambio con todos los datos definidos.
- Contemplar todos los conceptos de las tablas de código establecidas en este Test, según los criterios generales fijados en el capítulo V.1.
- Contemplar todos los Hitos de Tramitación establecidos en este Test.
- Contemplar todos los datos referentes a los Alardes.

V - CUESTIONES PARTICULARES DEL TEST

V.1 - CRITERIOS GENERALES SOBRE LAS TABLAS DE CÓDIGOS

Este documento establece unos criterios generales sobre la gestión de las tablas de códigos que intervienen en las itineraciones entre órganos judiciales.

1. Las tablas contendrán un campo codificación y una descripción (concepto).

2. El uso de los códigos y conceptos será obligatorio en las itineraciones entre órganos judiciales.

3. En las aplicaciones de gestión judicial será obligatorio el uso de los conceptos. Será recomendable la utilización de los códigos; de no ser así, la Administración competente deberá desarrollar las tablas de conversión correspondientes.

4. Si una Administración considera necesario desglosar algún concepto en otros más detallados, podrá hacerlo siempre y cuando este desglose se circunscriba al ámbito interno pero no se refleje en las comunicaciones externas. En estas se utilizará el elemento raíz correspondiente.

   Ejemplo:

Código básico	XX
Descripción	'lesiones por violencia de género'
Desglose (opcional)	XX-1 matrimonios XX-2 parejas de hecho

Cuando el expediente correspondiente (asunto, recurso o exhorto) itinere, sólo reflejará: **XX 'lesiones por violencia de género'.**

NOTA: Se recomienda utilizar lo menos posible el desglose y ajustar las tablas internamente a las acordadas.

5. Las tablas residirán en un servicio centralizado del Punto Neutro Judicial (Área de Trabajo), y publicadas y accesibles en Internet dentro el portal del Consejo General del Poder Judicial (www.poderjudicial.es). Se utilizará siempre la última versión. Si alguna Administración entiende que deben modificarse (altas, modificaciones y bajas), deberá proponer el cambio a la Comisión de Informática Judicial del Consejo General del Poder Judicial que las modificará después de las aprobaciones oportunas, cambiará la última versión e informará sobre los cambios al resto de Administraciones para su correspondiente actualización.

V.2 - CODIFICACIÓN DE SERVICIOS COMUNES, UNIDADES ADMINISTRATIVAS Y CUERPOS DE SEGURIDAD

V.2.1 - Servicios comunes y unidades administrativas

El CGPJ, a través del Test de Compatibilidad, fija las reglas y las tablas de códigos para la confección de la codificación de los Servicios Comunes y Unidades Administrativas que las Administraciones Competentes creen.

El Test de Compatibilidad SÍ incorporará el resultado que faciliten las administraciones competentes en una tabla específica separada de la de Unidades Funcionales.

El criterio de codificación para un Servicio Común o Unidad Administrativa es el mismo que para Unidades Funcionales, es decir con el dato **codigoOrgano** de la definición base, donde se señala que es un código de diez caracteres, donde los cinco primeros caracteres señalan la sede (municipio) de acuerdo a la tabla de Municipios, los dos siguientes señalan el tipo de órgano de acuerdo a la tabla de Tipos de Organo, y los tres últimos expresan la particularidad del Servicio Común, como por ejemplo nº, sección, etc.

En la tabla de Tipos de Órganos, para los Servicios Comunes se contemplan los siguientes tipos

00 = Servicio Común Procesal
01 = Unidad Administrativa
02 = Servicio Común Procesal de Órganos Centrales
03 = Unidad Administrativa de Órganos Centrales

Las Administraciones competentes organizarán los Servicios Comunes Procesales previstos en la Ley Orgánica del Poder Judicial así como aquéllos que autorice el Consejo General del Poder Judicial, y los codificarán con tres restricciones:

1. Deberán respetar el tipo de órgano (00, 01, 02, 03).
2. Deberán asignar a cada Servicio Común Procesal o Unidad Administrativa tantos códigos de la tabla de especialidades como le correspondan. El campo especialidad pasará a ser obligatoria. Se agrupan por un dígito prefijo de la siguiente forma:

0 = Especialidades comunes (Jurisdicción)

1 = Especialidades propias de Órganos Judiciales

2 = Especialidades propias de Servicios Comunes

3 = Especialidades propias de Unidades Administrativas

4 = Especialidades propias de Fiscalías

5 = Especialidades propias de Otras Unidades

3. No podrán repetir codificaciones dentro de la misma Sede (municipio).

El Test incorpora un documento xml específico para su codificación, separado del de Órganos Judiciales. De forma similar a lo que se contempla para Juzgados de Paz. Opcionalmente se podrá indicar a qué órganos judiciales atiende el servicio común creado.

Un ejemplo de codificación sería:

```
<unidadFuncional>
	<codigo>2807900001</codigo>
	<denominacion>SERVICIO COMUN PROCESAL EJEMPLO DE MADRID</denominacion>
	<!-- Sus especialidades -->
	<especialidades>
		<especialidad>003</especialidad>
		<especialidad>299</especialidad>
	</especialidades>
	<!--
		Opcionalmente, unidades a las que da servicio
	<servicio>
		<unidadFuncional>2807945001</unidadFuncional>
		<unidadFuncional>2807945002</unidadFuncional>
	</servicio>
	-->
	</unidadFuncional>
```

Con estas restricciones, cada Administración podrá utilizar como quiera los tres últimos caracteres de los diez necesarios para codificar una unidad funcional, porque cuando se realice una itineración a un Servicio Común Procesal o Unidad Administrativa se hará atendiendo a la especialidad del servicio o unidad.

V.2.2 - Cuerpos de seguridad

Se recomienda que el Ministerio de Justicia y las Administraciones competentes codifiquen las distintas Fuerzas de Seguridad siguiendo las dos restricciones siguientes:

1. Deberán respetar el tipo de órgano (91).
2. No podrán repetir codificaciones dentro de la misma Sede (municipio).

Y de esta forma mantener la siguiente recomendación:

1. Los 5 primeros carcteres señalan la Sede (municipio)
2. Los 2 siguientes caracteres serán siempre 91 de acuerdo a la restricción 1.
3. El siguiente carácter (letras y números) para expresar los distintos Cuerpos de Seguridad del Estado como por ejemplo:
   1 = Policia Nacional
   2 = Guardia Civil
   3 = Mossos d'Esquadra
   4 = Ertzaintza
   5 = Policia Foral
   6 = Policia Judicial
   7 = Policia Municipal, Local o Guardia Urbana
   8 = Registro Central de Detenidos
4. Y los 2 últimos caracteres (letras y números) para identificar las distintas Unidades respetando la restricción 2 de evitar códigos duplicados.

Ejemplos orientativos

08019 91 4 00 Cuerpo de Seguridad Mossos d'Esquadra
08019 91 4 37 Mossos d'Esquadra. Barcelonès – Barcelona – Les Corts
08172 91 4 64 Mossos d'Esquadra. Maresme - Premià de Mar
08172 91 7 00 Policia Municipal de Premià de Mar

V.3 - CRITERIOS DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN AL SERVICIO DE LA ADMINISTRACIÓN DE JUSTICIA

El Pleno del Consejo General del Poder Judicial, en su sesión de 13 de septiembre de 2007, ha adoptado el siguiente acuerdo: *«Aprobar el documento denominado "Criterios generales de seguridad en los sistemas de información al servicio de la Administración de Justicia", que se incorporará como Anexo al "Test de Compatibilidad de los Sistemas Informáticos de Gestión Procesal", aprobado por el Pleno en su sesión celebrada el 12 de abril de 2007.»*

V.3.1 - ANTECEDENTES

La sensibilidad de la información jurisdiccional y la creciente importancia de los sistemas de información en la tramitación de los procedimientos judiciales son dos elementos que inciden en la relevancia de la seguridad de la información.

El Consejo General del Poder Judicial es consciente de la importancia de la seguridad en los sistemas de información al servicio de la Administración de Justicia, y en particular en lo relativo a los aspectos relacionados con el cumplimiento de la Ley Orgánica de Protección de Datos y el Reglamento de Medidas de Seguridad.

El Código de Conducta para usuarios de equipos y sistemas informáticos al servicio de la Administración de Justicia (Instrucción 2/2003, de 26 de febrero, BOE de 10 de marzo de 2003) y la realización de auditorías de seguridad en los sistemas de información al servicio de la Administración

de Justicia (aprobada por el Pleno en sesión celebrada el 23 de julio de 2003), son algunas de las iniciativas abordadas y que reflejan esta importancia. Trabajo e iniciativas que han permitido concluir con la creación y declaración de los Ficheros de carácter personal dependientes de los Órganos Judiciales, efectuada por Acuerdo del Pleno del Consejo General del Poder Judicial de 20 de septiembre de 2006 (BOE de 12 de octubre de 2006).

En esa línea, la colaboración de las Administraciones Públicas competentes en la provisión de recursos y medios materiales (a las que se reconoce, en el citado acuerdo de 20 de septiembre de 2006, la cualidad de Encargados del tratamiento, al ser los responsables de los centros de tratamiento, locales, equipos, sistemas, programas, así como del personal técnico que interviene en el tratamiento) y de los usuarios (entendidos como todos los profesionales que prestan sus servicios en los órganos judiciales) es indispensable, dado que constituyen una parte clave en el nivel de seguridad y protección de la información.

El Consejo General del Poder Judicial, al amparo de lo dispuesto en los artículos 230.5 de la Ley Orgánica del Poder Judicial, 97.1 y 102.1 del Reglamento núm. 1/2005, de 15 de septiembre, de los Aspectos Accesorios de las Actuaciones Judiciales, ha elaborado este documento que incluye un conjunto de medidas que permitan mejorar y/o homogeneizar (cuando proceda) el nivel de seguridad existente sobre los sistemas de gestión procesal. En este sentido, no debe ser interpretado como una lista exhaustiva sino como un marco de referencia (o modelo de seguridad) asociado a los requerimientos fundamentales relativos a la seguridad de estos sistemas, cuyo desarrollo, ejecución e implantación corresponde a las Administraciones Públicas competentes en la dotación de medios materiales, en su respectivo ámbito territorial. En atención a las

peculiaridades y necesidades propias del Tribunal Supremo, dichas labores deberán ser llevadas a cabo por el Ministerio de Justicia en coordinación con el Gabinete Técnico de Información y Documentación del citado Alto Tribunal.

V.3.2 - CRITERIOS BÁSICOS DE SEGURIDAD

MARCO NORMATIVO

Con carácter general, las tareas realizadas por las Administraciones Públicas competentes en la provisión de recursos y medios materiales en lo relativo a la gestión de la infraestructura tecnológica y sistemas de información al servicio de la Administración de Justicia, estarán basadas en un Documento de seguridad, de obligado cumplimiento para el personal con acceso a los datos de carácter personal de los Sistemas de Información de Gestión Procesal, que describirá las medidas de seguridad (organizativas y técnicas) puestas en marcha por las mencionadas Administraciones Públicas. El Documento de seguridad, adecuadamente formalizado e implantado, contendrá los aspectos contemplados en los artículos 8.2 y 15 del Reglamento de Medidas de Seguridad.

Además, las Administraciones Públicas competentes elaborarán (y ejecutarán) un Plan de acción detallado de las medidas a adoptar para dar cumplimiento al expresado Documento de seguridad, así como las que permitan asegurar la ejecución de los criterios técnicos y organizativos que se señalan a continuación.

Una copia de dicho Documento de Seguridad y del Plan de acción serán remitidos a la Comisión de Informática Judicial del Consejo General del Poder Judicial.

MEDIDAS TÉCNICAS

Configuración de infraestructura tecnológica

- Los servidores en los que se ubiquen los sistemas de gestión procesal deberán prevenir riesgos asociados a accesos no autorizados derivados de la existencia de aplicaciones y/o sistemas no relacionados con aspectos jurisdiccionales (por ejemplo: sistemas de información soporte a las áreas, departamentos o consejerías de educación, agricultura,...). Para ello implantarán las medidas y medios tecnológicos necesarios para garantizar la independencia, unicidad y protección de los datos.
- Las plataformas tecnológicas soporte a los sistemas de gestión procesal (lo que también incluye sistemas operativos y bases de datos y, cuando proceda, configuraciones en puestos clientes) estarán configuradas de acuerdo a guías y estándares de securización adecuadamente formalizadas y actualizadas. La posibilidad de realizar cambios sobre esta configuración estará restringida, previa aprobación, a un reducido número de usuarios (personal técnico especializado). Existirá un registro de cambios (que incluye la instalación de parches u otro tipo de soluciones facilitadas por el proveedor).
- Con carácter general, existirá una separación efectiva entre los entornos de desarrollo y producción.

Identificación y autenticación

Los sistemas de información (y software de base) dispondrán de mecanismos de identificación y autenticación que prevengan los accesos no autorizados basados en la existencia de un identificador unívoco de usuario y contraseña, o mediante la utilización de certificado digital o algún otro mecanismo de protección suficientemente probado, dado el

estado de la tecnología en cada momento y las características de la información a proteger.

- En el caso de sistemas de identificación basados en usuario y contraseña, la creación de un nuevo usuario se realizará atendiendo al procedimiento establecido y previa autorización del responsable competente. La asignación de contraseña inicial será aleatoria y, en cualquier caso, pre-expirada. Los sistemas permitirán asociar períodos de validez a los identificadores de usuario de forma que fuera de ese rango de fechas el sistema prevenga la autenticación a través de dicho identificador.
- Las contraseñas de los usuarios generales (es decir, sin privilegios especiales asociados a tareas de administración) deberán satisfacer, al menos, los siguientes criterios:
    - Calidad. La contraseña tendrá, al menos, una longitud mínima. Adicionalmente, deberá evaluarse la posibilidad de exigir reglas adicionales de complejidad en base al grado de madurez de los controles de seguridad implantados.
    - Cambio periódico. Los usuarios deberán cambiar periódicamente sus contraseñas (por ejemplo, cada tres meses). Existirá un histórico de contraseñas que prevenga la re-utilización de la contraseña anterior. En cualquier caso, los sistemas permitirán el cambio autónomo de contraseña por parte de los usuarios aún cuando no sea como consecuencia del cambio periódico previsto.

  En cualquier caso, las contraseñas se almacenarán en las aplicaciones y sistemas, de forma encriptada.

  Los usuarios con privilegios de administración considerarán mecanismos adicionales de seguridad y protección, en relación a las claves, para prevenir accesos no autorizados a través de sus identificadores.

- Los sistemas de gestión procesal y la infraestructura tecnológica soporte dispondrán de mecanismos de bloqueo de los usuarios. En particular, considerarán al menos las siguientes casuísticas:
    - Bloqueo automático por intentos reiterados de acceso fallidos (por ejemplo: 6 intentos).
    - Bloqueo automático asociado a intentos de acceso fuera del intervalo de fechas de validez de un identificador de usuario.
    - Bloqueo manual por parte del Administrador.

  Se recomienda el bloqueo automático por no acceso en un determinado período de tiempo (por ejemplo: tres meses) con objeto de regularizar las cuentas activas en el órgano judicial.

  El desbloqueo de un determinado identificador se realizará, con carácter general, de forma manual por parte del personal autorizado al efecto.
- No se permitirá, con carácter general, el acceso a los sistemas a través de usuarios genéricos. Esto incluye, sin limitarse a, aquellos que, por defecto, son creados en el proceso de instalación de los sistemas y aplicaciones. En cualquier caso, deberá asignarse un responsable de aquellos usuarios genéricos que se estimen necesarios.
- En el caso de sistemas basados en identificación digital, solo se podrán utilizar certificados digitales autorizados por la Administración competente. Las aplicaciones deberán consultar las listas de certificados revocados correspondientes antes de permitir el acceso.
- Igualmente podrán ser utilizados sistemas biométricos como método de identificación y autentificación.

Control de acceso

- Perfiles y roles. El acceso a los sistemas de información de gestión procesal estará basado, habitualmente, en perfiles y roles. Estos

mecanismos determinarán, en base a las necesidades autorizadas de los usuarios, dos aspectos fundamentales:

- Las especialidades (de las previstas por el sistema de información) a las que podrán acceder (con frecuencia basado en puntos de menú)
- Los datos a los que deberán tener acceso. Para ello permitirá, sin perjuicio de las capacidades de búsqueda y explotación de la información, segmentar los usuarios en base a criterios organizativos como los órganos judiciales, secciones, etc. a las que están adscritos. Será posible aplicar mecanismos adicionales de protección basados en expedientes o asuntos concretos (por ejemplo, a través de listas de control de acceso)

Con relación a las sustituciones, los sistemas de información tenderán a considerar el principio de herencia. En particular, se pretende que sea posible asociar (y revocar) a un sustituto los asuntos en los que participara el sustituido.

- Bloqueo por inactividad. Tras un período de inactividad (por ejemplo: 30 minutos) se activará un mecanismo de bloqueo que evite la suplantación del usuario en momentos en los que su equipo no esté atendido.
- Con carácter general, los privilegios de administración en los propios equipos de los usuarios estarán restringidos. Es decir, se prevendrá la instalación de software no autorizado en los equipos de los usuarios por parte de los mismos.

Registro de accesos

- Los accesos a los expedientes o asuntos mantendrán un registro que incluya, al menos, la identificación del usuario, la fecha y hora en la

que se realizó el acceso, el tipo de acceso y si ha sido autorizado o denegado.

- Se definirán pistas de auditoría y seguimiento de actividad en los sistemas operativos y gestores de bases de datos. El seguimiento estará, especialmente, orientado a las tareas de administración del sistema. La configuración del sistema prevendrá la eliminación y/o desactivación de estos logs.

Redes y comunicaciones

- La red en la que se ubiquen sistemas y a la que accedan los usuarios de los sistemas de información al servicio de la Administración de Justicia estará protegida de accesos no autorizados.
- El acceso a otras redes estará protegido a través de cortafuegos (firewalls) u otro tipo de mecanismos que aseguren en las comunicaciones a través de las redes locales un nivel de protección suficiente frente a las amenazas de terceros. Este apartado también incluye la existencia y actualización periódica de mecanismos de protección frente a virus u otros códigos maliciosos. Los dispositivos de red (como encaminadores – routers -) también estarán adecuadamente securizados y protegidos.
- La conectividad remota ("teletrabajo") a través de redes públicas de datos estará adecuadamente protegida, en línea con las soluciones tecnológicas de seguridad existentes en cada momento.
- Igualmente, la conectividad a través de redes inalámbricas requerirá la configuración (con los mecanismos actualmente disponibles o los que puedan existir en el futuro) segura de la misma.
- La administración de forma remota de los equipos y servidores, en caso de ser necesaria, se realizará mediante canales seguros.

MEDIDAS ORGANIZATIVAS

Organización de seguridad

- Las funciones y responsabilidades asociadas a la administración y explotación de los sistemas y, en particular, a la gestión de la seguridad de la información estarán formalmente aprobadas y asignadas a personas concretas. Estas funciones pueden incluir, sin limitarse a:
    - Mantenimiento y actualización del marco normativo.
    - Instalación y configuración segura de sistemas.
    - Elaboración de informes asociados al análisis de logs.
    - Monitorización y resolución de incidencias.
    - Formación y concienciación de usuarios
    - Seguimiento de accesos en sistemas operativos y gestores de bases de datos y, en términos generales, accesos en tareas de administración de sistemas.
    - Seguimiento de los servicios contratados en lo que afecte a la administración y explotación de sistemas de gestión procesal.
    - Realización de copias de respaldo

Ubicación física de los servidores y equipos

- La ubicación física de los servidores y dispositivos de comunicaciones (electrónica de red, firewalls,...) prevendrá el acceso no autorizado y se realizará atendiendo a un análisis de riesgos. En particular, el acceso estará restringido de forma efectiva (por ejemplo, a través de puertas cerradas con llave) a personal autorizado. Existirá, por lo tanto, un registro de estos accesos.
- Medidas de protección medioambiental. Las salas en las que se ubiquen los servidores tendrán sistemas de detección y extinción de incendios. La temperatura de la sala estará en los rangos de operación definidos por los fabricantes (habitualmente a través de sistemas de aire acondicionado). Por último, en caso de riesgo de

daños por agua (tuberías, instalaciones aéreas de aire acondicionado refrigeradas por agua, ...) existirán sistemas que mitiguen o prevengan los daños en los equipos y servidores.

- Garantía de suministro eléctrico. Existirán mecanismos que aseguren el suministro eléctrico no sólo a los servidores en los que se ubiquen los sistemas de gestión procesal sino también a los diferentes elementos necesarios para asegurar la conectividad de los usuarios a los servicios críticos.
- Como orientación general y en la medida que resulte posible, los equipos de los usuarios no estarán ubicados en zonas de paso o distribución.

Formación y concienciación de usuarios

- Se desarrollarán mecanismos de formación y concienciación específicamente orientados a la seguridad de la información (complementarios a los que el Consejo General del Poder Judicial pudiera arbitrar). Habitualmente estarán basados en cursos presenciales y/o a través de e-learning, y tendrán carácter periódico. Entre las áreas que pueden incluir figuran:
    - Conocimiento del marco normativo en lo que sea relevante a la operativa de los diferentes usuarios.
    - Funciones y responsabilidades de los usuarios.
    - Confidencialidad y privacidad de las contraseñas (u otros mecanismos de autenticación)
    - Criterios de conservación y almacenamiento de los ficheros generados por los usuarios (incluyendo la eliminación de los ficheros temporales)
    - Políticas de bloqueo de pantalla y puesto de trabajo despejado de papeles y soportes con información sensible.
    - Condiciones de trabajo fuera de las oficinas habituales.

Seguimiento de accesos

- Revisiones periódicas de usuarios autorizados. Periódicamente (por ejemplo, cada tres meses) se realizará, por parte de los usuarios competentes, una revisión de los usuarios autorizados para identificar usuarios con acceso indebido potencial a los sistemas. A tal efecto, los sistemas permitirán obtener los usuarios activos en los sistemas para poder contrastar dicha lista con los usuarios autorizados e identificar excepciones.
- Registro de usuarios con privilegios de administración. Existirá un registro de usuarios con privilegios de administración (asociados a tareas habituales de mantenimiento y explotación de sistemas o como consecuencia de accesos de emergencia de usuarios de desarrollo a producción). Este registro incluirá el identificador autorizado, el período de validez, el responsable de la autorización y las tareas a realizar por el mismo. Este registro podrá servir como fuente de contraste con el log de los sistemas.

  El Consejo General del Poder Judicial considera este apartado especialmente relevante por los riesgos de seguridad inherentes a la función de administración de sistemas y por la constatación que, en ocasiones, estas tareas son realizadas por personal externo (por ejemplo, adscrito a empresas privadas con las que la Administración Pública tiene suscrito un contrato) en el que el índice de rotación puede ser elevado.

  El mantenimiento actualizado de este registro (conjuntamente con la trazabilidad de las acciones realizadas por estos usuarios) debería permitir un seguimiento más efectivo de las tareas que se realizan.

  El registro de usuarios con privilegios de administración estará a disposición de la Comisión de Informática Judicial.

Copias de respaldo

- Se realizarán copias de respaldo, en base a los procedimientos formalizados y de acuerdo a un calendario previsto, que aseguren, en caso de ser necesario, la recuperación de la información anterior a producirse la incidencia. El calendario determinará el período de retención y los controles asociados a la rotación de los soportes.
- Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en el que se encuentren los equipos y servidores (con medidas de restricción de acceso suficientes). El traslado se realizará preservando la confidencialidad de la información.

Contratos de prestación de servicios.

- Las Administraciones Públicas competentes en la provisión de recursos y medios materiales mantendrán un registro actualizado de las organizaciones prestadoras de servicios que pudieran tener acceso a información de gestión procesal. En este sentido, estarán identificados para cada organización las funciones asociadas, las personas con acceso, ...

- Las Administraciones Públicas arbitrarán mecanismos de seguimiento y control de las empresas o entidades que prestan asistencias técnicas de forma que sea posible conseguir un nivel asimilable de control a la realización interna de las funciones. Los sistemas de seguimiento y control pueden estar basados en estándares, como por ejemplo ITIL. En cualquier caso, las cláusulas contractuales considerarán acuerdos de confidencialidad que prevalecerán aún cuando haya finalizado el contrato.

Procesamiento paralelo por parte del usuario final

- Las Administraciones Públicas arbitrarán mecanismos que permitan el mantenimiento y actualización de las aplicaciones asociadas a la gestión procesal. Asimismo, existirán registros de incidencias o de solicitudes de mantenimientos evolutivos y se realizará un seguimiento de la resolución y/o cierre de las mismas.
- Por otra parte, se restringirán los privilegios de instalación de programas diferentes a los previstos en las maquetas de equipos ofimáticos definidas. Estas aplicaciones podrán ser instaladas exclusivamente por los administradores autorizados, que en todo momento seguirán las normas señaladas en el Documento de seguridad. Eventualmente, se realizará un seguimiento para identificar software no corporativo instalado en los equipos de usuario. Las excepciones que se identifiquen y el análisis de las mismas permitirán arbitrar las medidas de sensibilización y concienciación aplicables. En todo momento los datos gestionados con las herramientas ofimáticas o aplicaciones distintas a las previstas, seguirán los mismos criterios de seguridad, que los establecidos para las aplicaciones corporativas. En ningún caso se crearán ficheros de carácter personal distintos a los declarados atendiendo a los requerimientos de la Ley Orgánica de Protección de Datos.
- Los sistemas de gestión procesal dispondrán de mecanismos de seguimiento de la frecuencia de acceso de los diferentes identificadores de usuario al sistema. Es decir, permitirán identificar usuarios que no han accedido durante un determinado período de tiempo al sistema de gestión procesal.

Revisiones periódicas

- Al menos cada dos años se revisará el grado de implantación del modelo de seguridad sobre los sistemas de información e

infraestructura tecnológica al servicio de la Administración de Justicia y el nivel de madurez de los controles. El análisis tendrá un alcance completo y, como consecuencia del mismo, se derivará además del diagnóstico, un seguimiento de las acciones previstas asociadas a la mejora continua en el nivel de seguridad y control. Además, cuando proceda, incluirá propuestas asociadas a la resolución de los aspectos susceptibles de mejora.

SECRETARIO JUDICIAL

El Secretario Judicial, en el marco de las competencias contempladas en el artículo 454 de la Ley Orgánica del Poder Judicial, velará por la observancia en las oficinas judiciales de los criterios generales de seguridad establecidos en el presente documento.

RESPONSABLES DE SEGURIDAD

Las Administración Pública competente, en su respectivo ámbito territorial, designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el correspondiente Documento de seguridad.

Dicha designación será comunicada a la Comisión de Informática Judicial del Consejo General del Poder Judicial.

AUDITORÍA

Los Sistemas de Información al servicio de la Administración de Justiciase someterán a una auditoría que verifique el cumplimiento del presente documento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos cada dos años.

Corresponde al Consejo General del Poder Judicial o a la Administración Pública competente, cuando así lo haya manifestado, la práctica y ejecución de la citada auditoría.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente documento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará sus conclusiones a la Comisión de Informática Judicial, así como a la Administración Pública competente, a fin de que se adopten las medidas correctoras adecuadas

Los informes de auditoría quedarán a disposición de la Agencia de Protección de Datos.

PLAZOS DE EJECUCIÓN

Las Administraciones Públicas competentes deberán adoptar las medidas que a continuación se relacionan en los plazos especificados:

Comunicar a la Comisión de Informática Judicial la designación del Responsable de Seguridad, así como de la confección del registro de organizaciones prestadoras de servicios, en Diciembre de 2007.

Enviar a la Comisión de informática Judicial el Documento de Seguridad así como el denominado Plan de acción, en Enero de 2008.

Llevar a cabo la Auditoria de seguridad reseñada en el presente documento, durante el primer trimestre de 2009.

V.4 - GUÍA DE LECTURA DE LOS CUESTIONARIOS.

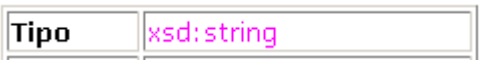
V.4.1 - Cuestionarios de Especificaciones de información e intercambio.

El lector debe conocer que estos cuestionarios son el resultado de una transformación XSL de los documentos de especificación XML-Schema de los intercambios. Por ello se mantienen en los cuestionarios ciertos conceptos y términos que a continuación describimos.

El Anexo I presenta las definiciones de datos comunes referenciadas en las definiciones en los siguientes anexos. Los datos definidos en este anexo se presentan con los siguientes conceptos y descripciones:

(simpleType)

Especifica un dato, como por ejemplo **materia** o **codigoOrgano**, su formato y dominio de valores mediante definiciones de longitud, expresión regular, enumerado discreto de valores y/o referencia a tabla de valores variable definida en un documento XML externo. En su especificación toman significado los siguientes atributos utilizados que lo definen:



Tipo de datos básico XML-Schema de entre xsd:string o xsd:base64Binary. El primero corresponde a una cadena de texto sin codificar, mientras que el segundo corresponde a la codificación en Base64 de un contenido en binario como puede ser un documento de Microsoft Word.

Formato	\d{5}\d\d([A-Z]|\d){3}

Expresión regular[2] que actuando como un patrón define tanto la longitud como la sintaxis del dato.

En la imagen ejemplo anterior, la expresión regular expresa un valor compuesto de 7 números *\d{5}\d\d* y 3 caracteres formados por letras mayúsculas o números *([A-Z]|\d){3}*, ya que:

\d expresa un dígito del 0 al 9

\d{5} expresa la repetición 5 veces del elemento anterior, en este caso significar 5 dígitos.

( ) agrupa una subexpresión para establecer precedencias

[ ] expresa un rango de valores

[A-Z] expresa el rango de valores de la letra A a la Z

| expresa opcionalidad

([A-Z] | \d) expresa una letra de la A a la Z o un dígito

Valor	H	Hombre
Valor	M	Mujer

Valor concreto que puede tomar el dato. Cuando el dato presenta un enumerado extenso y variable no se utiliza éste atributo, y en su lugar aparece una referencia al documento XML que define todo el dominio o enumerado de valores, como podemos ver en el siguiente

Enumerado de códigos también disponible en sexos.xml

Longitud máxima	11

[2] Lenguaje informático normalizado relacionado con la teoría de lenguajes formales y autómatas

Longitud máxima en caracteres del dato.

(complexType)

Especifica información compuesta por uno o varios datos. Es decir por varios *(simpleType)* u otros *(complexType).* Así por ejemplo, **direccionNacional** se trata de una información compuesta para definir una dirección postal en el estado español, que se conforma por **tipoVia**, un **nombreVia**, una **poblacionProvincia** y un **codigoPostal**, y opcionalmente con **numeroVia** y **piso**, siendo en éste caso todos ellos *(simpleType)*.

En su especificación toman significado los siguientes atributos:

Nombre

Nombre del elemento que conforma la estructura de datos.

Descripcion

Descripción del elemento

Definición

Nombre del *(simpleType)* u otro *(complexType)* que lo define, pudiendo darse el caso de que sea directamente un tipo directo XML-Schema (resaltado en color), como por ejemplo xsd:string

La ocurrencia de un elemento dentro de la composición de datos *(complexType)* es obligatoria (*minOccurs="1")* u opcional[3] (*minOccurs="0"*) y de ocurrencia única (*maxOccurs="1")* o múltiple (*maxOccurs="unbounded")*. Los elementos obligatorios presentan

[3] Obligatoriedad y opcionalidad a efectos de intercambio. Es decir, desde el punto de vista de envío y aceptación del mensaje. El sistema, internamente, ha de tener previstos todos los datos.

su nombre en negrita, mientras que los opcionales en cursiva. La ocurrencia única no tiene representación especifica ya que por defecto todos los elementos son de ocurrencia única, en cambio los elementos de ocurrencia múltiple se presentan con un carácter asterisco ***** al final del nombre.

También se produce una situación de elección (*choice*) como podemos ver en el siguiente ejemplo:

domicilio (complexType)

Información de contacto de una persona física o jurídica

Nombre	Descripcion	Definición
domicilioId	Identificación del domicilio de una persona. Es un número de domicilio por persona	numeroOrden
Obligatorio entre		
direccionNacional	Direccion en el territorio nacional	direccionNacional
direccionExtranjero	Direccion en el extranjero	direccionExtranjero
*telefono**	Telefono de contacto	xsd:string

En el ejemplo tenemos que un domicilio se define con un **domicilioId** obligatorio, y también con un dato obligatorio entre direccionNacional y direccionExtranjero; cosa que por otra parte es lógica ya que un domicilio sin dirección carecer de sentido, y por otra parte las características para un dirección en España y en el extranjero no son las mismas. Así por ejemplo el código postal en España tiene un formato y longitud de acuerdo a Correos, que no tiene por qué coincidir con los códigos postales de otros países.

Los anexos de Intercambio de Información posteriores presentan el mismo formato e interpretación que a continuación explicamos. Se tata de los cuestionarios de:

- Solicitud de cooperación jurisdiccional (Anexo III.1)
- Devolución cooperación jurisdiccional (Anexo III.2)
- Envío de recurso interpuesto (Anexo IV.1)

- Devolución recurso (Anexo IV.2)
- Envío asunto completo (Anexo V.1)
- Envío a CENDOJ (Anexo VI.1)
- Alardes (Anexo VII)

La parte izquierda presenta las especificaciones con los atributos Nombre, Descripción y Definición de igual forma que la descrita anteriormente, mientras que en la parte derecha se encuentra la información de cuestionario.

Ejemplo:

envioAsunto (complexType)

Información que una Unidad Funcional debe enviar a otra cuando se produce una remisión de asunto completo, ya sea por cuestiones de incompetencia, de elevación para consulta, por primer conocimiento, etc.

Nombre	Descripcion	Definición	Existe?
unidadFuncionalOrigen	Unidad Funcional que remite o eleva el expediente completo a otra Unidad	codigoOrgano	☐
nig	Identificación del asunto que se remite	nig	☐
tipoTramitacion	Tipo de Tramitación mediante el que se está tramitando el expediente actual	tipoTramitacion	☐
numeroProcedimiento	Nº de procedimiento o de registro general en caso de no existir procedimiento mediante el que se está tramitando el expediente	numeroProcedimiento	☐
refAcontecimiento	Referencia del acontecimiento que da origen a esta remisión.	refAcontecimiento	☐
	Resolución por la que se eleva o remite		

Vemos en la parte izquierda las columnas Nombre, Descripción y Definición de *(complexType)* con el mismo significado y presentación definido anteriormente. Así pues en el ejemplo tenemos que **unidadFuncionalOrigen** se trata de un dato obligatorio de acuerdo a la definición "codigoOrgano"; mientras que *refAcontecimiento* se trata de un dato opcional de acuerdo la definición de igual nombre.

En la parte derecha está las casillas de cuestionario donde poder señalar si es el sistema puede enviar/recibir el dato con las mismas características

de formato y dominio de valores que los definidos en el tipo simple (*simpleType*) de datos correspondiente.

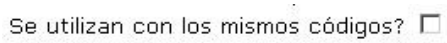
También al inicio del formulario, como vemos en el siguiente ejemplo, está la casilla relativa a la capacidad de enviar y recibir la información de acuerdo a las especificaciones de intercambio, y la casilla RESULTADO DEL TEST, para recoger el resultado general del cuestionario.

V.4.2 - Cuestionario de codificación.

El cuestionario de codificación presenta la relación de tablas de códigos utilizados en los mensajes de Intercambios o composición de códigos compuestos (como es el caso del código de órgano).

En cada tabla hay un enlace a la lista de valores completa. A continuación se presentan las casillas del cuestionario donde:

- para señalar que el sistema contempla todos los conceptos de la tabla de valores, pudiendo desglosar los que desea. Si añade nuevos conceptos o le falta alguno, el sistemas no será compatible.



- para señalar que se utilizan con los mismo códigos definidos en el Test.

V.4.3 - Cuestionario de hitos relevantes en la tramitación

El cuestionario de hitos presenta la relación de fechas relevantes en la tramitación de los procedimientos o expedientes que los sistemas informáticos de gestión procesal deben proporcionar. Ejemplo:

Anexo X. Hitos procesales

RESULTADO DEL TEST ☐

F01	Fecha de registro		Existe ? ☐
F02	Fecha de la primera resolución dictada por el órgano judicial		Existe ? ☐
F03	Fecha de la resolución que declara conclusos los autos, a la espera de que se dicte la resolución definitiva	Órganos unipersonales	Existe ? ☐
F04	Fecha de pendiente de señalamiento para votación y fallo	Órganos colegiados	Existe ? ☐

En este cuestionario se indica la clase de hito, el ámbito jurisdiccional donde es aplicable (si está en blanco, es aplicable a todos) y la casilla

Existe ? ☐

En esta etapa de revisión del test únicamente se indicará, a través de esta casilla, si el sistema puede proporcionar esta fecha, con el formato *fechaSimple*. No se evalúa la capacidad de envío al CGPJ.

V.4.4 - Cuestionario de Alardes

El formato e interpretación de estos formularios es el mismo que los descritos anteriormente para el intercambio de información.

En el caso concreto de los alardes hay que resaltar su particular estructura. De una unidad funcional se ha de poder obtener, obligatoriamente, la siguiente información:

alardeType (complexType)

Un Alarde tiene que incluir la relación de Asuntos y Escritos pendientes, y un resumen global de los mismos.

Nombre	Descripcion	Definición	Existe?
unidadFuncional	Juzgado o Tribunal al que corresponde el alarde.	codigoOrgano	☐
asuntos	Relación de Asuntos pendientes. Incluyendo Recursos, Exhortos, Ejecuciones y Piezas.	alardeAsuntosType	☐
escritos	Relación de Escritos pendientes.	alardeEscritosType	☐
resumen	Resumen global de Asuntos y Escritos pendientes según el Juzgado o Tribunal al que corresponde el alarde.	alardeResumenType	☐

La relación de asuntos y escritos está conformada por una serie de datos definidos con la misma metodología vista hasta ahora.

alardeAsuntoType (complexType)

La información por asunto pendiente es la siguiente:

Nombre	Descripcion	Definición	Existe?
nig	NIG del asunto	nig	☐
jurisdiccion	Jurisdicción. En los órganos mixtos permitirá determinar si es del orden civil o penal	jurisdiccion	☐
tipoTramitacion	Tipo de Tramitación	tipoTramitacion	☐
numeroProcedimiento	Nº de procedimiento o de registro general en caso de no existir procedimiento.	numeroProcedimiento	☐
materia	Materia	materia	☐
situacion	Situación Procesal 1 = En la Oficina 2 = Pendiente exclusivamente de sentencia o de dictar resolución de fondo 3 = Recurso pendiente de elevar 4 = Recurso devuelto		☐

alardeEscritoType (complexType)

La información por escrito pendiente es la siguiente:

Nombre	Descripcion	Definición	Existe?
tipoTramitacion	Tipo de Tramitación al que hace referencia	tipoTramitacion	☐
numeroProcedimiento	Nº de procedimiento o de registro general en caso de no existir procedimiento al que hace referencia	numeroProcedimiento	☐
objeto	Objeto del escrito	xsd:string	☐
fechaPresentacion	Fecha de presentación	fechaSimple	☐

El resumen global solcitado en el alarde está individualizado según el tipo de órgano. Por ejemplo, si la unidad funcional es una sección mixta de la Audiencia Provincial, se deberá obtener el formulario T37.

alardeResumenType (complexType)

Resumen global según el tipo de Tribunal o Juzgado.

Nombre	Descripcion	Definición	Existe?
Obligatorio entre			☐
T37-1	AUDIENCIA PROVINCIAL (SECCION CIVIL)	T37-1Type	☐
T37-2	AUDIENCIA PROVINCIAL (SECCION PENAL)	T37-2Type	☐
T37	AUDIENCIA PROVINCIAL (SECCION MIXTA)	T37Type	☐

T37Type (complexType)

Resumen de la AUDIENCIA PROVINCIAL (SECCION MIXTA)

Nombre	Descripcion	Definición	Existe?
C2	Apelaciones contra Sentencias dictadas en Procedimientos Abreviados	xsd:integer	☐
C3	Apelaciones de Juicios de Faltas	xsd:integer	☐
C17	Despachos Penales de Auxilio Judicial	xsd:integer	☐
C28	Ejecutorias Pendientes	xsd:integer	☐

xsd:integer → Se obtendrá el número total (sumarizado) de cada concepto.

Al inicio del formulario está la casilla relativa a la capacidad de obtener la información requerida, y la del resultado general del cuestionario.

Anexo XII. Alardes

Capacidad de obtener esta información de acuerdo a las especificaciones ? ☐

RESULTADO DEL TEST

☐