



INSTRUCTIVO (parte IV)

Segunda Ronda de Talleres

XVII CUMBRE JUDICIAL IBEROAMERICANA

GRUPO DE TRABAJO

Tecnología de los Poderes Judiciales

4 al 6 de septiembre de 2013

Colombia

II RONDA DE TALLERES

XVII CUMBRE JUDICIAL IBEROAMERICANA

Bogotá -Colombia

Antecedentes

Durante la I Reunión Preparatoria de esta Edición, realizada en Guadalajara - México, se presentó ante los Presidentes y Presidentas de Cortes y Consejos y los Coordinadores y Coordinadoras Nacionales, los proyectos denominados “*Tecnología para el Juez*”, por parte del Poder Judicial de Chile, y el de “*Mapa Tecnológico: hoja de ruta hacia Objetivos Estratégicos*”, por el Poder Judicial de Costa Rica, como continuación al proyecto iniciado en la edición anterior.

En lo que respecta al proyecto de “*Tecnología para el Juez*”, constaba de cinco aspectos centrales, a saber:

- a) Optimización del Expediente Electrónico
- b) Gestión del conocimiento
- c) Archivo Judicial para los Expedientes Electrónicos
- d) Acceso a la Comunidad
- e) Capacitación

Con este proyecto “*Tecnología para el Juez*”, se busca agrupar y compartir elementos tecnológicos que puedan apoyar y volver ms eficiente las labores de los Tribunales en todas sus instancias, así como recopilar y compartir las experiencias logradas, tanto buenas como no tan buenas, al momento de implementar tecnología en este ámbito.

Por su parte el “*Mapa Tecnológico*”, consistía en continuar con la elaboración de los indicadores que permitieran trazar la ruta para la elaboración de dicha herramienta, y a su vez, integrar al proyecto las acciones del grupo e-Justicia y el Programa Tlus de Cumbre Judicial.

Es a partir de lo anterior, que durante la I Reunión Preparatoria, se acuerda concentrar estos proyectos y para ello se definieron los siguientes tres grandes propósitos:

- a) El desarrollo de un sistema integrado para el uso de todos los Poderes Judiciales, que tengan por objeto, concentrar en un solo repositorio documentos de interés de todos los Poderes Judiciales, tanto para el ámbito tecnológico, como para otros temas de importancia de los diferentes grupos de trabajo de las Cumbres, permitiendo acceder a dicha información e una forma inteligente y guiada. Lograr el intercambio de buenas prácticas y experiencias que puedan generar valor a los diferentes Poderes Judiciales, poder discutir sobre temas transversales en tiempo real, entre otros.
- b) Esta herramienta será mantenida por cada país de manera autónoma ya que le permitirá de forma independiente incorporar y actualizar la información que estime pertinente, amparada en el protocolo de uso que se deberá acordar y firmar.
- c) La integración de los Poderes Judiciales a través de una herramienta que facilite el diálogo entre éstos.
- d) Consolidar esta herramienta como un repositorio único de todas las iniciativas referentes a tecnología y otros temas que se generan y se han venido generando en a través de los años en la cumbre.

El grupo se denomina "*Tecnología para los Poderes Judiciales*", integrado por: Chile y Costa Rica, como países co-coordinadores, Argentina, Bolivia, Ecuador, España, Guatemala, Honduras, México, Nicaragua y Paraguay.

En la I Ronda de Talleres, realizada en Antigua – Guatemala, contando con la participación presencial de Chile, Guatemala, Argentina, Bolivia, Ecuador, España, Honduras, México, Nicaragua y Paraguay. Y Costa Rica, vía digital, se dividió el proyecto en cuatro subproyectos, a saber:

1. **Banco de Datos Tecnológicos** que incluye los proyectos Cartera de Proyectos, Brecha Tecnológica, Red de Videoconferencias y Mapa Tecnológico, en el cual trabajarán Costa Rica, Chile, Nicaragua y Paraguay.

2. **Innovación Tecnológica** donde participan Chile, Costa Rica, Honduras y México.
3. **Marco de Referencia para la Cooperación Jurídica Internacional – Telemática**, a cargo de España y Argentina.
4. **Difusión**, integrado por Guatemala, Bolivia y Ecuador

De cara a la II Ronda de Talleres, durante esta sesión de trabajo se acordó levantar la información a través de la matriz desarrollada en la edición anterior de Cumbre Judicial, con algunas modificaciones. Así como la identificación de fuentes de investigación en relación a las tecnologías, procedimientos y mejores prácticas en el mercado de las tecnologías, la recopilación y sistematización de los resultados de la investigación, teniendo como meta obtener los siguientes productos:

1. Disponer de una herramienta informática que permita acceder a información relativa a soluciones aplicadas en el ámbito tecnológico.
2. Propuesta estándar para la implementación del expediente digital, con elementos que son básicos o necesarios que este contenga de una u otra forma, así como la visualización de este.
3. Herramientas y Planes de difusión del ámbito tecnológico (sitio web, publicación o compendio de la cumbre)
4. Marco tecnológico mínimo de estándares que faciliten la cooperación jurídica internacional – telemática, es decir el exhorto electrónico y Video Conferencias para tomar testimonios, entre algunas de las iniciativas.

Es a partir de lo anterior, que cada subgrupo de trabajo, realizó diversas acciones de previo a la segunda ronda de talleres, tal y como se señala seguidamente:

Subgrupo Banco de Datos Tecnológicos

Este subgrupo trabajó de forma virtual en la adecuación de la matriz denominada “Banco de Datos Tecnológico Poderes Judiciales”, con la cual se pretende obtener una visión general en temas específicos, de forma tal que permita conocer hacia donde se orientan las tecnologías, buenas experiencias, errores cometidos y oportunidades de mejora en la implementación de proyectos estratégicos en la aplicación de la tecnología

de la información en la Administración de Justicia.

Se recopiló información basada en diversos criterios generales, con el propósito de recoger las experiencias de cada país respecto de temas comunes a todos, siendo algunos de estos: Equipamiento Tecnológico, Sistemas Informáticos, Servicios, Seguridad y Experiencias. Este documento fue remitido a todos los países que integran el grupo de trabajo, obteniéndose respuestas de: Argentina, Nicaragua, España, Ecuador, Honduras, Chile, Costa Rica y México. Quedando pendiente: Bolivia, Paraguay y Guatemala. (Anexo 1)

Además el Poder Judicial de Chile trabajó en el desarrollo del sistema “*Repositorio Único de Información Tecnológica*”, herramienta que permitirá almacenar la información relativa a las experiencias, proyectos, políticas, personas de contacto, documentos y datos generales relacionados con temas de tecnología de cada Poder Judicial. Pudiendo ser consultada por los Poderes Judiciales de una forma estructurada para conocer las experiencias de los otros países y pudiendo así generar valor. De igual forma dicha herramienta indicará cuál de esos proyectos podrá ser donado entre los países, de forma tal que se logre la cooperación internacional para disminuir los costos de los Poderes Judiciales y replicar las experiencias y las buenas practicas.

Es a partir de esta herramienta y de la matriz de información, donde se podrán obtener los datos para la realización del Mapa Tecnológico, el cual deberá trabajarse de forma coordinada con el grupo del PLIEJ. Con dicho mapa se proyecta conocer el desarrollo tecnológico de los Poderes Judiciales Iberoamericanos de forma bienal a fin de que estos sean un aporte por su expertis para los que así lo requieran.

Por su parte Costa Rica en coordinación con Chile, redactó un borrador del “*Protocolo de Actuación del Sistema Repositorio Único de Información Tecnológica*”, (Anexo 2) con el cual se pretende regular el funcionamiento, organización y operación del sistema desarrollado por Chile.

Subgrupo Innovación Tecnológica

Con respecto a la innovación tecnológica, es de mencionar que se efectuó un encuentro en Santiago de Chile en el mes de julio, cuyo propósito fue conocer sobre los temas de tecnología en los ámbitos de:

1. Innovación tecnológica, es decir, respecto de nuevas herramientas que permitan apoyar la labor en los Juzgados, garantizando una justicia rápida y eficiente.
2. Seguridad Tecnológica, tanto de los sistemas como de la plataforma en si, considerando que la información es de gran valor.
3. Software de justicia, a fin de conocer lo que cada país tiene y su experiencia a este respecto.
4. Diseño de herramientas estadísticas (baremo)

Con la información aquí proveída por los países y los diferentes proveedores es que se espera levantar un documento que recapitule, las herramientas que hay en el mercado y como estas pueden apoyar la labor de los tribunales, así como las experiencias adquiridas en el ámbito tecnológico y documentos de protocolo que aporten a un lineamiento de como operar la plataforma. (Anexo 3, 4, 5 y 6)

Subgrupo Marco de Referencia para la Cooperación Jurídica Internacional – Telemática

En el marco de este proyecto se presentaron dos documentos para ser valorados por el grupo de trabajo:

- **Borrador de Guía de Interoperabilidad y Seguridad de Expediente Electrónico:**
El cual tiene por objeto establecer la estructura y formato técnico del expediente judicial electrónico, así como las especificaciones de los servicios de remisión y puesta disposición.
- **Borrador de Guía de Interoperabilidad**
- **Borrador de Seguridad Informática**
- **Borrador del Documento Judicial Electrónico,** con el cual se establecen los componentes del documento judicial electrónico, así como la estructura y formato técnicos a fin de garantizar su intercambio. En el entendido de que dichos componentes son el Contenido, la Firma Electrónica, y los Metadatos del documento.

Subgrupo Difusión

Los países co-coordinadores del Grupo de Tecnologías de los Poderes Judiciales,

proponen para efectos de difusión, considerar lo propuesto en ediciones anteriores, en el sentido de promover la implementación de la Red de Videoconferencia Iberoamericana, de forma tal que anualmente se agenden actividades donde se impartan charlas, exposiciones, foros, etc., con el fin de compartir experiencias de diversas índoles en relación con las tecnologías de la información en la Administración de Justicia.

Además se sugiere solicitar a la Secretaria Permanente permitan mantener un espacio fijo (una página), en la revista de Cumbre Judicial, para que cada vez que salga una edición se pueda publicar algún tema de interés en la materia. Estos temas serán definidos previamente por el grupo a fin de trabajarlos y poder tener el material necesario al momento de la edición de la revista.

Objetivo General

Durante la II Ronda de Talleres el grupo de trabajo de “Tecnología para los Poderes Judiciales”, tendrá como objetivo general:

- Consolidar los proyectos que se vienen desarrollando en el grupo de trabajo de “Tecnologías para los Poderes Judiciales”, estableciendo las acciones necesarias para lograr su total desarrollo, con el fin de presentar el producto final en la XVII Asamblea Plenaria de Cumbre Judicial a realizarse en Santiago de Chile.

Plan de Trabajo

De acuerdo con el objetivo anterior, las labores a efectuar durante dicha reunión serán las siguientes:

PRIMER DÍA: miércoles 4 de septiembre

De 14:00 a 17:30 horas

Jornada vespertina Hotel Tequendama

Metodología de trabajo: Mesa Plena

Tema	Actividad	Responsable	Hora
Acto Protocolario Grupo de Trabajo	Palabras de bienvenida e inauguración de jornadas de trabajo	Coordinadores de Proyecto Chile: Mauricio Rodríguez Costa Rica: Luis Guillermo Rivas	14:00 – 14:30
Informe encuesta	Análisis de resultados de la encuesta tecnológica aplicada a los países	Chile: Mauricio Rodríguez	14:30 – 15:15
Informe encuentro Chile – V Feria de Tecnología	Informar respecto de las conclusiones logradas en Chile durante el encuentro de informáticos en Santiago de Chile	Chile: Mauricio Rodríguez	15:15 – 16:00
Presentación sistema informático	Se presentará el sistema informático desarrollado por Chile “ <i>Repositorio Único de Información Tecnológica</i> ”	Chile: Mauricio Rodríguez	16:00 – 16:45
Café			16:45 – 17:15
Protocolo	Establecer un documento final como protocolo para el uso del sistema informático	Coordinadores de Proyecto Chile: Mauricio Rodríguez Costa Rica: Luis Guillermo Rivas	17:15 – 19:00

SEGUNDO DÍA: jueves 5 de septiembre

De 09:00 a 17:30 horas

Jornada completa Hotel Tequendama

Metodología de trabajo: Grupos de Trabajo

Grupo	Tema	Hora
Banco de Datos	<ol style="list-style-type: none"> 1. Validación de la metodología de trabajo durante la segunda ronda de talleres. 2. Revisión y avances de las conclusiones y acuerdos de la Primera Ronda de Talleres que se realizó en Guatemala. 3. Revisión de los resultados de la encuesta tecnológica aplicada a los Poderes Judiciales. 4. Elaborar documento de conclusiones del resultado de la encuesta a la luz del objetivo que se proponía con esta. 5. Revisar que otros elementos se debieran levantar, que no se hayan considerado, para un segundo capítulo de la encuesta. 6. Evaluar como extender este sistema como banco de datos de manera transversal a todos los grupos de trabajo. 7. Proponer que este Banco de Datos sea el repositorio único de información para la cumbre 	09:00 – 19:00
Innovación	<ol style="list-style-type: none"> 1. Validación de la metodología de trabajo durante la segunda ronda de talleres. 2. Revisión y avances de las conclusiones y acuerdos de la Primera Ronda de Talleres que se realizó en Guatemala. 3. Análisis de la encuesta y extracción de los proyectos innovadores 4. Interoperabilidad e integración de sistemas, Protocolo de interoperabilidad entre poderes Judiciales. 5. Seguridad informática, documento de buenas prácticas en este ámbito a ser consideradas por los Poderes Judiciales. 6. Evaluar herramientas tecnológicas que faciliten la navegación por el expediente digital 7. Herramientas estadísticas que permitan hacer gestión para los Jueces (Baremo) 8. Investigación de las herramientas de W3C (Web semántica) 	09:00 – 19:00
Difusión	<ol style="list-style-type: none"> 1. Validación de la metodología de trabajo durante la segunda ronda de talleres. 2. Revisión y avances de las conclusiones y acuerdos de la Primera Ronda de Talleres que se realizó en Guatemala. 3. Solicitar una columna en la revista actual de la cumbre, para lo cual debiera prepararse una propuesta con los temas que se estiman publicar. 4. Analizar los alcances de implementar un portal único para los temas de cumbre. 	09:00 – 19:00

Cooperación Jurídica	<ol style="list-style-type: none"> 1. Validación de la metodología de trabajo durante la segunda ronda de talleres. 2. Revisión y avances de las conclusiones y acuerdos de la Primera Ronda de Talleres que se realizó en Guatemala. 3. Revisión y análisis de los documentos elaborados. 4. Software 	09:00 – 19:00
-----------------------------	--	---------------

TERCER DÍA: viernes 6 de septiembre

De 09:00 a 13:00 horas

Jornada diurna Hotel Tequendama

Metodología de trabajo: Mesa Plena

Tema	Actividad	Responsable	Hora
Conclusiones de los grupos de trabajo	Cada grupo expondrá el trabajo realizado y se ira preparando el documento de las conclusiones	Chile: Mauricio Rodríguez Costa Rica: Luis Guillermo Rivas	09:00 – 13:00

Productos Esperados

Concluida la Segunda Ronda de Talleres se espera contar con la aprobación de los siguientes proyectos:

- ✓ Aprobada propuesta de metodología de trabajo entre los Jefes de Informática y el Grupo de tecnología (participación, Video conferencias)
- ✓ Aprobado el Sistema Informático de Repositorio Único de Datos Tecnológicos
- ✓ Propuesta borrador de incorporación de nuevas funcionalidades al Repositorio Único de Datos Tecnológicos
- ✓ Aprobado borrador del Protocolo de administración y uso para el Sistema de Repositorio Único de Datos Tecnológicos.
- ✓ Aprobador borrador de las iniciativas de Innovación Tecnológica
- ✓ Propuesta de mecanismos de difusión a implementar y temas de difundir
- ✓ Definidas las actividades a realizar para la conclusión de los proyectos de cara a la Asamblea Plenaria de Cumbre Judicial

BANCO DE DATOS TECNOLÓGICO PODERES JUDICIALES

Grupo Tecnologías de Información XVII Edición Cumbre Judicial

El presente relevamiento de información tiene como fin obtener los datos básicos para la implementación del **Banco de Datos Tecnológico de los Poderes Judiciales**, el cual permitirá a todos los miembros de Cumbre Judicial tener una visión en temas específicos de hacia dónde se orientan las tecnologías, buenas experiencias, errores cometidos y oportunidades de mejora en la implementación de proyectos estratégicos en la aplicación de la tecnología de la información en la Administración de Justicia.

La información aquí solicitada será compartida en un sitio web de acceso general que facilite la retroalimentación.

1. Equipamiento Tecnológico

I. HARDWARE	
1. ¿Qué Porcentaje de Ministros de la Corte, Jueces y funcionarios cuentan con equipos informáticos?	a) Ministros de Corte % b) Jueces % c) Funcionarios %
2. ¿Qué modalidad utiliza para proveer el equipamiento computacional para los funcionarios?	<input type="checkbox"/> a) Arriendo <input type="checkbox"/> b) Ensamblaje Propio <input type="checkbox"/> c) Compra <input type="checkbox"/> d) Otra
3. ¿Qué nivel de obsolescencia le asigna al equipamiento computacional?	<input type="checkbox"/> a) Entre 3 a 5 años <input type="checkbox"/> b) Superior a 5 años <input type="checkbox"/> c) Otra
4. ¿Cuenta con políticas de respaldo a nivel institucional para la información que manejan directamente en sus equipos los jueces y funcionarios?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO

<p>5. ¿Posee políticas y/o procedimientos para el reemplazo del equipamiento y su término de vida útil? En caso afirmativo, señalar cuáles. Adjuntarlas al documento.</p>	<p><input type="checkbox"/> a) SI</p> <p><input type="checkbox"/> b) NO</p>
<p>6. ¿Qué porcentaje del equipamiento representan los equipos portátiles?</p>	<p>a) Portátiles %</p> <p>b) Smartphone %</p> <p>c) Tablets %</p> <p>d) Otros %</p>

II. CONECTIVIDAD	
<p>1. Actualmente la institución cuenta con una red de datos Institucional.</p> <p>En caso afirmativo indique el porcentaje de Nivel de Cobertura que la misma posee a nivel país.</p>	<p><input type="checkbox"/> a) 0%</p> <p><input type="checkbox"/> b) 25%</p> <p><input type="checkbox"/> c) 50%</p> <p><input type="checkbox"/> d) 75%</p> <p><input type="checkbox"/> e) 100%</p>
<p>2. Disponen de conexión a Internet para todos los funcionarios de la Institución</p>	<p><input type="checkbox"/> a) SI</p> <p><input type="checkbox"/> b) No</p> <p><input type="checkbox"/> c) Parcializado (detallar, por función cargo etc.)</p>
<p>3. ¿Qué herramientas de conectividad se brindan a los Ministros de Corte, jueces y funcionarios?</p>	<p>MINISTROS DE CORTE /JUECES</p> <p><input type="checkbox"/> a) Internet</p> <p><input type="checkbox"/> b) Conexión a la red interna</p> <p><input type="checkbox"/> c) Acceso remoto a la información y a los sistemas de tramitación</p> <p><input type="checkbox"/> d) Correo Institucional</p> <p><input type="checkbox"/> e) Otra alternativa _____</p>

	<p>FUNCIONARIOS</p> <p><input type="checkbox"/> a) Internet</p> <p><input type="checkbox"/> b) Conexión a la red interna</p> <p><input type="checkbox"/> c) Acceso remoto a la información y a los sistemas de tramitación</p> <p><input type="checkbox"/> d) Correo Institucional</p> <p><input type="checkbox"/> e) Otra alternativa _____</p>
<p>4. ¿Posee políticas y/o procedimientos para normar los accesos señalados?</p> <p>En caso afirmativo adjunte material.</p>	<p><input type="checkbox"/> a) SI</p> <p><input type="checkbox"/> b) NO</p>
<p>5. ¿Cuenta con una plataforma de videoconferencia en la Institución?</p>	<p><input type="checkbox"/> a) SI</p> <p><input type="checkbox"/> b) NO</p>
<p>6. ¿Para qué tipo de actividades y con qué cobertura se utiliza la plataforma?</p>	<p><input type="checkbox"/> a) Juicios</p> <p><input type="checkbox"/> b) Reuniones Administrativas</p> <p><input type="checkbox"/> c) Capacitación</p> <p><input type="checkbox"/> d) Cooperación</p> <p><input type="checkbox"/> e) Conferencias / Seminarios</p> <p><input type="checkbox"/> f) Otros</p>
<p>7. ¿Posee protocolos de operación para los procesos judiciales frente a fallas en los enlaces de comunicación</p>	<p><input type="checkbox"/> a) SI</p> <p><input type="checkbox"/> b) NO</p>
<p>8. ¿Los anchos de bandas asignados a los tribunales obedecen a algún tipo de criterio o política?, como por ejemplo:</p>	<p><input type="checkbox"/> a) Velocidad v/s cantidad de usuarios</p> <p><input type="checkbox"/> b) Ancho de banda v/s servicios informáticos</p> <p><input type="checkbox"/> c) Otros</p>
<p>9. ¿Dispone la red de enlaces de respaldo o contingencia en caso de falla del</p>	<p><input type="checkbox"/> a) SI</p>

principal?	<input type="checkbox"/> b) NO
10. ¿Dispone de medidas de contingencia en caso de fallas del enlace principal y respaldo?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
11. ¿Dispone de algún Software de monitoreo de enlaces de comunicaciones que permita alertar eventos y analizar el trafico dentro de los enlaces? En caso afirmativo, adjunte documento.	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
12. ¿Posee actualmente herramientas de optimización de anchos de banda?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
13. ¿Tiene algún estándar de seguridad y certificaciones en el tema de conectividad? De ser Sí, adjunte el documento.	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
14. ¿Cuenta con políticas de confidencialidad respecto al tráfico de información?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
15. ¿Cuenta con herramientas de encriptación de datos?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO

III. Almacenamiento de Datos

1. ¿Cuenta la Institución con Data Center?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
2. Dicho centro de procesamiento de datos es:	<input type="checkbox"/> a) Propio

	<input type="checkbox"/> b) Externo
3. ¿Cuenta actualmente la Institución con un centro de procesamiento de datos alternativo? En caso afirmativo, señalar que servicios posee replicado.	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
4. ¿Utiliza motor de base de datos? De ser afirmativo:	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO Indique si es: <input type="checkbox"/> a) Licenciado <input type="checkbox"/> b) Código Abierto Especifique el/los motores de BD utilizados: Oracle. _____
5. ¿Qué tipo de tecnología de procesamiento utiliza para las bases de datos?	<input type="checkbox"/> a) Tecnología X86 <input type="checkbox"/> b) SPARC <input type="checkbox"/> c) RISC <input type="checkbox"/> d) ITANIUM <input type="checkbox"/> e) OTRA. Indique:
6. Señale el tamaño de gigabytes y descripción de cada una de las 5 bases de datos principales que gestiona	
7. Señale la cantidad de usuarios por cada una de las 5 bases de datos señaladas en el punto anterior	
8. ¿Posee normativas o procedimientos referentes a las políticas de administración y roles de la administración de las bases de datos? En caso afirmativo, adjunte material.	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
9. ¿Posee normativas o procedimientos para respaldo, su periodicidad y vigencia de datos almacenados en bases de datos? En caso afirmativo,	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO

adjunte material.	
10. ¿Dispone de herramientas de software para monitorear el rendimiento del motor de bases de datos? En caso afirmativo, indique.	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO <hr/>

IV. Virtualización	
1. ¿Cuenta con herramientas de virtualización dentro de la plataforma tecnológica?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
2. ¿Que tiene virtualizado y en qué proporción? Favor indicar	<input type="checkbox"/> a) Equipos de escritorio <input type="checkbox"/> b) Equipos virtualizado <input type="checkbox"/> c) Equipos servidores <input type="checkbox"/> d) Equipos de comunicación <input type="checkbox"/> e) Otros. Indique: _____ <hr/>
3. ¿Posee políticas de Virtualización y Consolidación, respaldo y alta disponibilidad del equipamiento tecnológico virtualizado? De ser positivo, adjunto documento	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO

2. Sistemas Informáticos

V. Sistemas Judiciales	
1. ¿Cuenta la Institución con sistemas informáticos para el Registro, Control, Gestión y/o tramitación de causas?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
2. ¿Qué porcentaje del total de tribunales utiliza sistemas informáticos para la tramitación de causas?	<input type="checkbox"/> a) 0% <input type="checkbox"/> b) 25%

	<input type="checkbox"/> c) 50% <input type="checkbox"/> d) 75% <input type="checkbox"/> e) 100%
3. ¿Se utilizan sistemas informáticos para la tramitación íntegra de las causas como un mecanismo de respaldo, seguimiento y/o apoyo a la tramitación en papel?	<input type="checkbox"/> a) Si <input type="checkbox"/> b) No
4. Describa cómo es la relación actual entre ambas formas de registro (digital y papel).	<input type="checkbox"/> a) Electrónica <input type="checkbox"/> b) Mixta <input type="checkbox"/> c) Otra
5. ¿La tramitación electrónica o expediente electrónico es optativo u obligatorio?	<input type="checkbox"/> a) Optativo <input type="checkbox"/> b) Obligatorio <input type="checkbox"/> c) Otra
6. ¿Se utiliza la firma electrónica en las resoluciones de los expedientes electrónicos?	<input type="checkbox"/> a) Si <input type="checkbox"/> b) No
7. ¿Se encuentra estandarizado el formato de documentos digitales que se utilizan dentro de la organización? En caso afirmativo, indicar que formatos se utilizan.	<input type="checkbox"/> a) Si <input type="checkbox"/> b) No
8. ¿Qué tipo de firma se utiliza?	<input type="checkbox"/> a) Firma mediante certificado digital <input type="checkbox"/> b) Firma electrónica bajo autenticación <input type="checkbox"/> c) Otro tipo. Especificar
9. ¿Cuenta la Institución con registro de audio de audiencias u otros trámites?	<input type="checkbox"/> a) SI

En caso afirmativo señale brevemente el procedimiento y para que tipos de tribunales se utiliza.	<input type="checkbox"/> b) NO
10. ¿Cuál es el porcentaje de implementación en la Institución del expediente electrónico? Adjunte material explicando en qué consiste el expediente electrónico que se utiliza, como funciona y que opciones de visualización tienen los usuarios, tanto internos como externos, manuales de usuario o las rutas de acceso para poder observarlos directamente en línea.	<input type="checkbox"/> a) 0% <input type="checkbox"/> b) 25% <input type="checkbox"/> c) 50% <input type="checkbox"/> d) 75% <input type="checkbox"/> e) 100%

VI. Sistemas Jurisprudenciales

1. ¿Dispone la Institución con sistemas informáticos para la Gestión Documental?	<input type="checkbox"/> a) Jurisprudencia <input type="checkbox"/> b) Doctrina <input type="checkbox"/> c) Legislación <input type="checkbox"/> d) Otros documentos
2. ¿Los sistemas de gestión jurídica documental como tiene sus procesos de registro y gestión?	<input type="checkbox"/> a) Electrónica <input type="checkbox"/> b) Mixta <input type="checkbox"/> c) Otra
3. ¿Los sistemas de gestión jurídica documental están integrados con los sistemas de gestión de causas?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
4. ¿Existen herramientas mediante las cuales la Institución haga Gestión del Conocimiento? En caso afirmativo describa su funcionamiento y alcance.	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
5. ¿Existen sistemas de información de Tesauro Jurídico vinculados a los	<input checked="" type="checkbox"/> a) SI <input type="checkbox"/> b) NO

sistemas de Gestión Jurídica Documental?	
6. ¿Dispone la Institución algún buscador electrónico de información interna, particularmente para el conocimiento e intercambio de sentencias, criterios, legislación entre los Ministros de la Corte, Jueces y funcionarios?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO

VII. Sistemas Administrativos	
1. ¿Cuenta con sistemas informáticos de gestión administrativa?	<input type="checkbox"/> a) Gestión Administrativa <input type="checkbox"/> b) Gestión Recurso Humano <input type="checkbox"/> c) Gestión Financiera <input type="checkbox"/> d) Gestión de Adquisiciones <input type="checkbox"/> e) Gestión de Inventarios <input type="checkbox"/> F) Otros. Indicar E-learning

VIII. Sistemas de Archivo Judicial para Expedientes Electrónicos y Audiencias Orales	
1. ¿Existe en la Institución un organismo especializado que se encargue de la función de archivar y resguardar los expedientes judiciales	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
2. ¿Existe algún procedimiento que se esté utilizando para archivar causas digitales terminadas o estas se mantienen en las mismas bases de datos que los expedientes en tramitación? En caso de existir adjunte documento explicando.	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
3. ¿De qué forma se están archivando las audiencias orales grabadas tanto para procesos activos como para procesos terminados? Si existe algún	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO

procedimiento favor adjuntarlo	
4. ¿Qué alternativas de acceso tienen actualmente los usuarios al momento de querer consultar un expediente digital de una causa terminada, o bien un audio y/o video de una grabación de una audiencia oral?	

3. Servicios

IX. Servicios Internos	
1. ¿Cuentan con Intranet Institucional?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
2. ¿Qué servicios se publican en dicha página?	
3. ¿Qué metodologías de capacitación está utilizando la Institución en la actualidad? Detalle todas aquellas que involucran el uso de tecnologías de la información y las comunicaciones (TICs)	
4. ¿La Institución hace uso de metodologías de capacitación como E-Learning o B-Learning? Señale en qué tipo de cursos.	<input type="checkbox"/> a) E-Learning <input type="checkbox"/> b) B-Learning

X. Servicios Externos	
1. ¿Los usuarios pueden consultar el estado de las causas que se encuentran en tramitación en línea? Señale si hay alguna distinción por procedimiento, instancia o territorio	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
2. ¿Existen mecanismos de tramitación en línea a través de los cuales los usuarios puedan realizar presentaciones a los tribunales directamente utilizando Internet?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO

<p>En caso afirmativo, señale en qué consisten para qué tipo de causas y trámites se encuentra permitido y cuáles son los requisitos que debe cumplir el usuario para hacer uso del servicio</p>	
<p>3. ¿Se han implementado mecanismos de notificación alternativos, como correo electrónico o mensajería de texto? En caso afirmativo, señale su funcionamiento y casos en que aplica.</p>	<p><input type="checkbox"/> a) SI <input type="checkbox"/> b) NO</p>
<p>4. ¿Existen interconexiones con otros organismos u instituciones, que permitan el intercambio de información que disminuyan la cantidad de trámites al ciudadano o agilicen los procesos?</p> <p>Si es así con qué organismos se encuentra funcionando. Señale algunos ejemplos o adjunte información al respecto.</p>	<p><input type="checkbox"/> a) SI <input type="checkbox"/> b) NO -</p>
<p>5. ¿Se hace uso de redes sociales para brindar información y promover el acercamiento con los usuarios? Señale cuáles son esas experiencias</p>	<p><input type="checkbox"/> a) SI <input type="checkbox"/> b) NO</p>

4. Seguridad

<p>1. ¿Cuenta con políticas, estándares de seguridad y certificaciones? En caso afirmativo adjunte material.</p>	<p><input type="checkbox"/> a) SI <input type="checkbox"/> b) NO</p>
<p>2. ¿Cuenta con procedimientos estandarizados referente al resguardo y seguridad de la plataforma tecnológica? (servidores, equipos de almacenamiento y de comunicación). En caso afirmativo adjunte material.</p>	<p><input type="checkbox"/> a) SI <input type="checkbox"/> b) NO</p>
<p>3. ¿Posee la Institución servicios estandarizados y certificados? En caso</p>	<p><input type="checkbox"/> a) SI</p>

afirmativo adjunte el material.	<input type="checkbox"/> b) NO
4. ¿Qué medios de difusión emplea para informar de las políticas de seguridad dentro de la organización?	

5. Organizacional

1. ¿Cuál es el nivel en la estructura organizacional que ocupa el área de tecnología?	<input type="checkbox"/> a) Dirección <input type="checkbox"/> b) Departamento <input type="checkbox"/> c) Unidad <input type="checkbox"/> d) Otra. Indique: _____
2. ¿Cuántas personas en total laboran en el área de tecnología?	65 profesionales aprox. - Jefes de Depto. y Área - Jefes de Proyectos - Coordinadores Técnicos - Técnicos Jurídicos - Asesores Informáticos
3. ¿Cuentan con presupuesto específico para las TICS?	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO
4. ¿Cuenta con Plan Estratégico de Tecnologías de Información? En caso afirmativo adjunte el material.	<input type="checkbox"/> a) SI <input type="checkbox"/> b) NO

6. Experiencias

1. Mencione cinco experiencias exitosas vividas por ustedes en cuanto a mejorar los servicios de justicia. De ser necesario aporte documentación al	
---	--

respecto	
2. Mencione cinco experiencias negativas vividas por ustedes en cuanto a la aplicación de la tecnología en el mejoramiento de la Administración de Justicia. De ser necesario aporte documentación al respecto	
3. Mencione cinco oportunidades de mejora o recomendaciones que ustedes darían para la implementación de la tecnología en los procesos judiciales	

PROTOCOLO DE ACTUACIÓN
Sistema Repositorio Único de Información Tecnológica

XVII CUMBRE JUDICIAL IBEROAMERICANA
SANTIAGO - CHILE

ÍNDICE

CAPÍTULO I: DISPOSICIONES GENERALES	2
Artículo 1 –Objeto y Ámbito de aplicación	2
Artículo 2 –Ámbito de aplicación	2
Artículo 3- Definiciones y Abreviaturas	2
CAPÍTULO II: SISTEMA REPOSITORIO ÚNICO DE INFORMACIÓN TECNOLÓGICA.....	3
Artículo 4 - Sobre el Sistema Repositorio Único de Información Tecnológica.....	3
Artículo 5 - Acceso a la información.....	3
Artículo 6 - Uso y Difusión de la Información.....	3
Artículo 7 - Administración y mantenimiento del sistema.....	3
Artículo 8 - Responsabilidad en cuanto a la información publicada	4
Artículo 9 - Derecho al tratamiento de la información	4
Artículo 10 – Módulos del Sistema.....	4
Artículo 11 - Solicitud de requerimientos.....	4
CAPÍTULO III: SOBRE LA INFORMACIÓN	5
Artículo 12 - Requisitos para la presentación de los documentos.....	5
Artículo 13 – Sobre base de datos de contactos	5
CAPÍTULO IV: FUNCIONES	5
Artículo 14 - Función de las Instituciones que son fuentes de información	5
Artículo 15 - Función de la Institución administradora del SRUIT.....	6
CAPÍTULO V: DISPOSICIONES FINALES	7
Artículo 16 - Disposiciones supletorias.	7
Artículo 17 - Publicación y Vigencia	7

CAPÍTULO I: DISPOSICIONES GENERALES

Artículo 1 –Objeto y Ámbito de aplicación

El presente protocolo regula el funcionamiento, organización y operación del “*Repositorio Único de Información Tecnológica*”, para el tratamiento de toda aquella información legítima, que de forma voluntaria compartan los países miembros que integran la Cumbre Judicial Iberoamericana (CJI), en el marco de la cooperación técnica internacional. Las entidades y personas autorizadas que utilicen el sistema y la información que por él transita deberán respetar las disposiciones del presente protocolo.

Artículo 2 –Ámbito de aplicación

Éste Protocolo será de aplicación a todas aquellas personas e Instituciones, en adelante “usuarios”, que hacen uso del “*Repositorio Único de Información Tecnológica*”, proporcionado por la Cumbre Judicial Iberoamericana.

Artículo 3- Definiciones y Abreviaturas

Para los efectos de aplicación del presente protocolo, el significado de algunos términos y abreviaturas es el siguiente:

CJI: Cumbre Judicial Iberoamericana

SRUIT: Sistema Repositorio Único de Información Tecnológica

Administrador del Sistema: Institución autorizada por la Cumbre Judicial Iberoamericana, para administrar y dar mantenimiento al sistema de “*Repositorio Único de Información Tecnológica*”.

Usuarios: Toda persona o Institución que haga uso del “*Repositorio Único de Información Tecnológica*”

CAPÍTULO II: SISTEMA REPOSITORIO ÚNICO DE INFORMACIÓN TECNOLÓGICA

Artículo 4 - Sobre el Sistema Repositorio Único de Información Tecnológica

El Sistema Repositorio Único de Información Tecnológica, almacena toda aquella información relativa a proyectos, experiencias – positivas y negativas-, productos, que se han desarrollado en la Administración de Justicia por los diversos Poderes Judiciales Iberoamericanos, con la cual se pretende mantener un banco de datos de información único, el cual podrá ser utilizado por cualquier Institución, como guía para el desarrollo de sus proyectos, como una forma de cooperación internacional en procura de optimizar los recursos institucionales de la región Iberoamericana.

Artículo 5 - Acceso a la información

La información será accedida a través de un programa desarrollado para ese fin, en el cual las personas podrán

Artículo 6 - Uso y Difusión de la Información

La información publicada en este sistema, es propiedad de cada Poder Judicial, quienes autorizan su uso y difusión, de forma legítima, en resguardo de los derechos fundamentales, a través del sitio web y herramienta destinado para ese fin por la CJI.

Artículo 7 - Administración y mantenimiento del sistema

El SRUIT, será administrado por el Poder Judicial autorizado por la CJI para cumplir con dicha labor, quienes serán los responsables de brindar el acceso, mantenimiento y resguardo a la información, de forma adecuada.

Artículo 8 - Responsabilidad en cuanto a la información publicada

Cada Institución será responsable del contenido de la información publicada para cada una de ellas. Otorgando los derechos de publicación de forma expresa al subir o remitir la información al Administrador del Sistema para su difusión.

Artículo 9 - Derecho al tratamiento de la información

Cada Institución dueña de la información publicitada, tendrá derecho a modificarla o eliminarla del SRUIT, según lo considere pertinente.

Artículo 10 – Módulos del Sistema

El SRUIT podrá contener módulos especiales que permitan la interacción de los datos o personas, tal como encuestas, foros de discusión, chats, entre otros, que faciliten la comunicación y dinamismo entre las diversas Instituciones.

Artículo 11 - Solicitud de requerimientos

En caso de estimarse oportuno incluir nuevos requerimientos al SRUIT, en procura de mejorar su funcionamiento y/o efectividad, las sugerencias pueden ser remitidas al Administrador del Sistema con copia a la Secretaría Permanente de la CJI, quienes valoraran la viabilidad de dicha petición.

CAPÍTULO III: SOBRE LA INFORMACIÓN

Artículo 12 - Requisitos para la presentación de los documentos

El SRUIT ofrece la posibilidad de incluir información documental, no obstante, con el fin de optimizar el uso de la herramienta, es necesario que la información incorporada cumpla con los siguientes requisitos: xxxxxxxxxxxxxx

Artículo 13 – Sobre base de datos de contactos

Para efectos prácticos cada proyecto o experiencia compartida, contendrá la información de las personas relacionadas con cada proyecto. De igual forma se mantendrá una base de datos unificada de contactos técnicos de todos los países, donde se autoriza la publicación de la información necesaria para establecer la comunicación.

CAPÍTULO IV: FUNCIONES

Artículo 14 - Función de las Instituciones que son fuentes de información

Todo Poder Judicial o Institución que cuente con acceso al SRUIT, tendrá como funciones:

- 1) Incluir, modificar o excluir información relativa a su Institución
- 2) Ser responsable de la publicación incorporada por su Institución mediante el usuario y clave proporcionada.
- 3) Velar porque la información publicitada sea legítima, veraz, pertinente y actualizada

- 4) Promover a nivel interno de cada Institución el uso de esta herramienta
- 5) Comunicar al Administrador del Sistema y/o a la CJI, cualquier inconveniente, anomalía, mejora o buena práctica que beneficie el mejoramiento del SRUIT.

Artículo 15 - Función de la Institución administradora del SRUIT

El Poder Judicial o Institución a cargo de la administración y mantenimiento del SRUIT, deberá:

- 1) Actualizar, dar mantenimiento y mejorar la herramienta para la implementación del SRUIT.
- 2) Tener disponible la herramienta para ser accedida de forma permanente. En caso de requerir un tiempo para mantenimiento, hacer la advertencia de que se está desarrollando dicha actividad.
- 3) Establecer el vínculo entre el SRUIT y el sitio oficial de la CJI.
- 4) Administrar las cuentas de las personas o Instituciones usuarias.
- 5) Realizar el análisis y desarrollo de aquellos requerimientos que se consideren oportunos para mejorar el SRUIT.
- 6) En caso de que se transfiera la administración y mantenimiento del SRUIT a otra Institución, deberá hacer entrega de los códigos fuentes, programas, y aquellos necesarios para dar sostenibilidad a este sistema.

CAPÍTULO V: DISPOSICIONES FINALES

Artículo 16 - Disposiciones supletorias.

En lo no expresamente establecido en el presente Protocolo, se regirá por lo dispuesto por la Asamblea Plenaria o los órganos competentes de la Cumbre Judicial Iberoamericana.

Artículo 17 - Publicación y Vigencia

El presente Protocolo rige a partir de su aprobación en xxxxxxxxxxxxxxxxxxxxxxxxx.



**Grupo Tecnologías de Información
XVII Edición Cumbre Judicial**

BORRADOR DE GUÍA DE INTEROPERABILIDAD Y SEGURIDAD
DE EXPEDIENTE JUDICIAL ELECTRÓNICO



Introducción

Con el fin de mejorar y agilizar la cooperación jurídica internacional, se deben establecer marcos de referencia de estándares que contengan determinados elementos básicos que permitan la interoperabilidad y compatibilidad entre los diferentes países para compartir información, por ejemplo en causas de derecho internacional.

En ese contexto, se requerirá analizar la posibilidad de estandarizar la estructura de los expedientes, de forma tal que permita su tratamiento informático como una estructura de información; es decir, el desarrollo de prototipos con miras a generar un traspaso de los expedientes en los temas de cooperación y asistencia internacional, como se ha señalado, en que, los países de Iberoamérica tengan una plataforma común que pueda emplearse en los diversos requerimientos posibles (ejemplo de cartas rogatorias, exhortos, exequátur, extradiciones o traspaso de sentencias para el cumplimiento en otro país de sentencias impuestas a nacionales).

En definitiva, y como objetivo básico del proyecto se señala que el proyecto permitirá, incluso, redefinir los tratados existentes, a través de una cooperación directa entre jueces, con resguardos mínimos sustanciales y procesales.

En ese marco de referencia es que deben establecerse los estándares y formatos tecnológicos básicos que contengan la información necesaria.

Objeto.

La Guía de Interoperabilidad y Seguridad del Expediente Judicial Electrónico tiene por objeto establecer la estructura y formato técnicos del expediente judicial electrónico, así como las especificaciones de los servicios de remisión y puesta a disposición.

El expediente judicial electrónico se define como el conjunto de documentos electrónicos asociados a un procedimiento judicial.



Expediente judicial electrónico

OBJETIVO

Como complemento del objetivo anterior, es necesario fijar los estándares necesarios para construir un expediente judicial electrónico que sea compatible para todos los sistemas de gestión procesal de los países Iberoamericanos.

El conjunto de estándares no limitará las necesidades de cada país, más bien establecerá unos mínimos comunes que todos los expedientes deberán incorporar para permitir la interoperabilidad.

Se establecen las siguientes definiciones:

Documentos electrónicos: entendidos como objetos digitales administrativos de cada una de las actuaciones administrativas que integran el expediente que contienen la información objeto (contenido y firma) y los datos asociados a ésta (metadatos). En el caso de intercambios entre organizaciones y con el ciudadano, estos documentos han de cumplir las características de estructura y formato establecidas por el marco de referencia para la cooperación jurídica internacional telemática Iberoamericana.

Los documentos electrónicos pueden incluirse en un expediente electrónico de diferentes formas:

- a. Directamente como elementos independientes.
- b. Dentro de una carpeta, entendida ésta como una agrupación de documentos electrónicos creada por un motivo funcional.
- c. Como parte de un sub-expediente electrónico, entendido éste como un expediente electrónico anidado dentro de otro, y que, como tal, sigue la estructura y consideraciones definidas en este marco.

La inclusión de un sub-expediente puede deberse a la existencia de expedientes vinculados al expediente que lo contiene o, a la generación de una vista del propio expediente.

El contenido y características de un expediente vinculado evolucionarán conforme al procedimiento con el que se corresponde dicho sub-expediente, independientemente de su vinculación a otro, reflejándose dichos cambios en el expediente que lo contiene.



Índice electrónico: objeto digital que contiene la identificación sustancial de los documentos electrónicos que componen el expediente, a efectos de preservar la integridad del mismo.

El contenido del índice del expediente puede variar según las necesidades de cada organización, la cual puede diseñar diferentes patrones que se ajusten a las actividades y diferentes tipos de procedimientos que desarrolla. También es conveniente utilizar este patrón del índice para definir qué documentos deben integrar un determinado tipo de expediente.

Firma del expediente: conjunto de datos de identificación que sirve para la validación del contenido y la estructura de un expediente, a los efectos de garantizar su autenticidad e integridad, pudiendo abarcar, además de la información propia del índice, otra de carácter procedimental particular de cada organización.

La firma del expediente es por tanto una firma electrónica de la organización responsable del expediente.

La firma del expediente se aplica a su índice electrónico, avalando la integridad de dicho índice y, por extensión, del contenido del expediente electrónico.

Deberá acordarse la normativa común aplicable a las firmas digitales.

Dado que la firma del expediente es la firma del índice electrónico, que es a su vez un documento electrónico, ésta debe cumplir lo establecido a tal efecto en las especificaciones del documento electrónico.

Metadatos del expediente: conjunto de datos que proporcionan contexto al contenido, estructura y firma del expediente, contribuyendo al valor probatorio de éste a lo largo del tiempo. Además, los metadatos del expediente pueden incluir particularidades procedimentales de cara a facilitar su gestión.

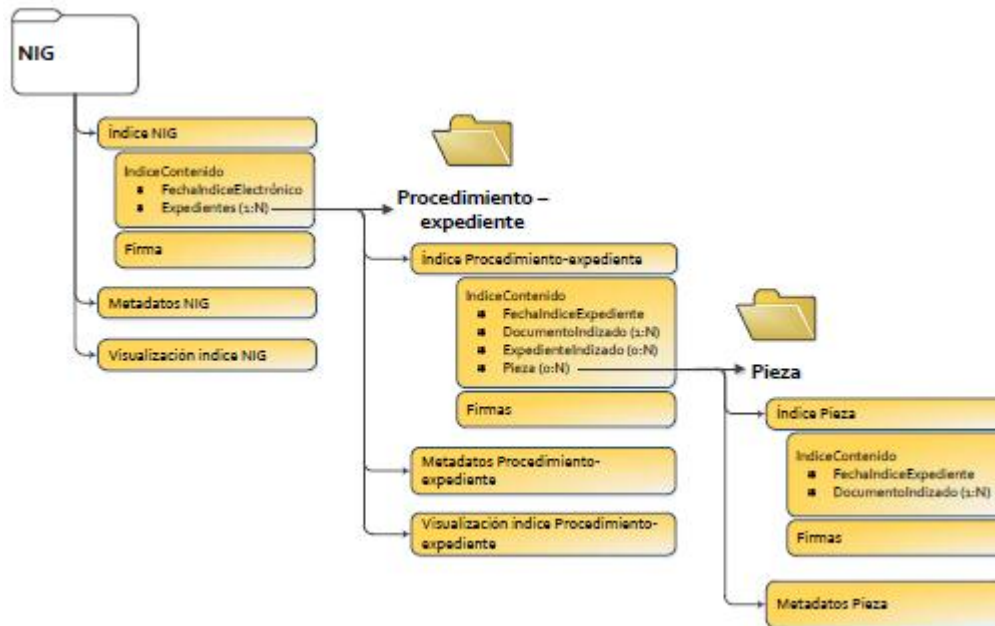
Número de identificación General NIG Para la unívoca identificación de un expediente o de un grupo de expedientes a lo largo de toda su vida procesal, independientemente del lugar en el que se encuentre o del país iberoamericano por el que esté itinerando, se considera necesario crear un Número de Identificación General (NIG) único, que deje rastro de su movimiento y gestión. Este NIG deberá ser acordado por todos los países y se intentará que coincida en la medida de lo posible con los números identificativos internos ya creados.

Los componentes de la capa técnica NIG son:

- a) Procedimientos/expedientes judiciales electrónicos, que tendrán la estructura definida en el Anexo I.
- b) Índice electrónico que garantizará su integridad. Recogerá el conjunto de procedimientos/expedientes judiciales electrónicos

asociados a un NIG.

- c) Firma del índice electrónico mediante sello del órgano judicial actuante.



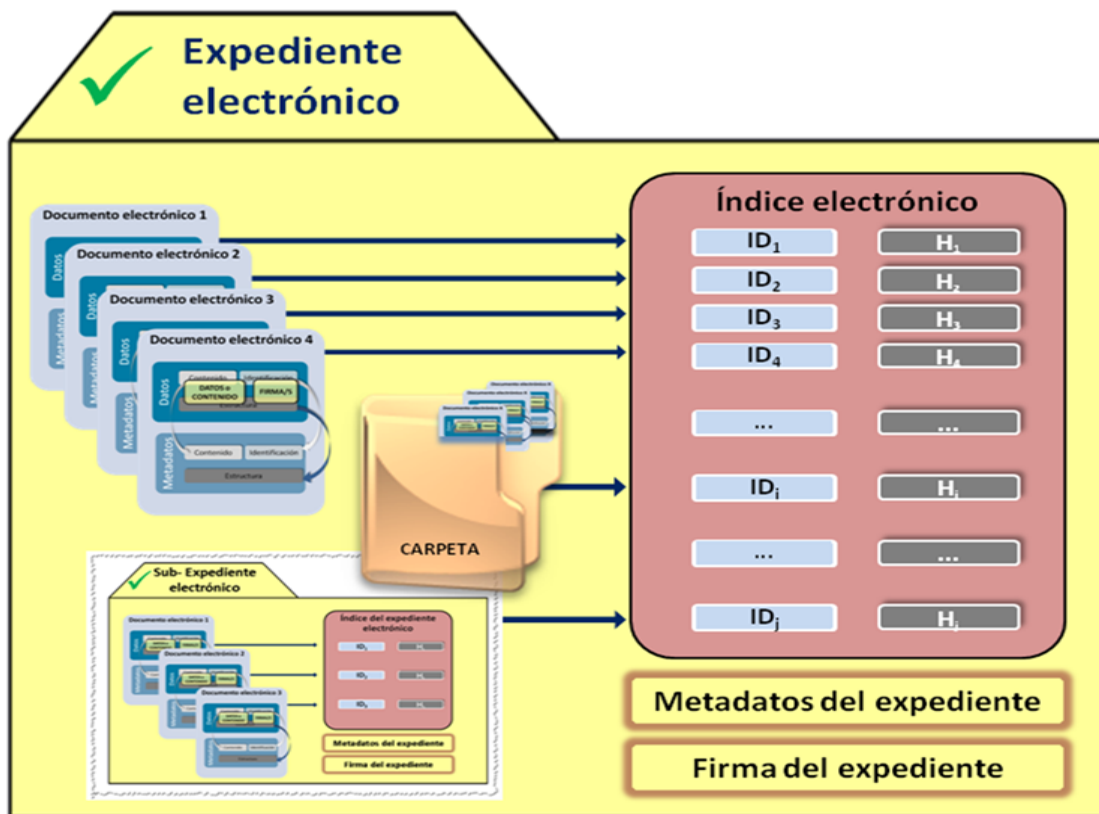
Para que la guía contemple el máximo número de posibilidades que pueden llegar a producirse en los diferentes países iberoamericanos y situaciones procesales, se puede ‘empaquetar’ para su envío, bajo el ‘paraguas’ de un NIG, un procedimiento –expediente electrónico, o varios de ellos relacionados con el mismo asunto. Y cada procedimiento-expediente electrónico, puede tener a su vez: documentos, otros expedientes electrónicos, y piezas separadas (las piezas separadas con tramitaciones especiales relacionadas con el expediente principal)

Componentes del procedimiento - expediente judicial electrónico.

1. Los componentes de un expediente judicial electrónico son:
 - a) El conjunto de *documentos electrónicos* correspondientes a un procedimiento judicial, que cumplirán con las características de estructura y formato establecidos en la Guía de Interoperabilidad y Seguridad del Documento Judicial Electrónico (ver Guía Documento Judicial Electrónico). Los documentos electrónicos podrán incluirse

en el expediente judicial electrónico, bien directamente como elementos propios del mismo o bien como parte de otro expediente, ya sea judicial o administrativo, anidado en el primero o como parte de una pieza.

- b) Índice electrónico, que garantizará la integridad del expediente judicial electrónico y permitirá su recuperación siempre que sea preciso.
Recogerá el conjunto de documentos electrónicos asociados al expediente en un momento dado y, si es el caso, su disposición en expedientes anidados o en piezas.
- c) Firma del índice electrónico mediante sello del tribunal actuante que se realizará mediante el sistema de firma.
- d) Metadatos del expediente judicial electrónico.



ID_x : ID del Objeto electrónico X
H_x: Huella digital del Objeto electrónico X

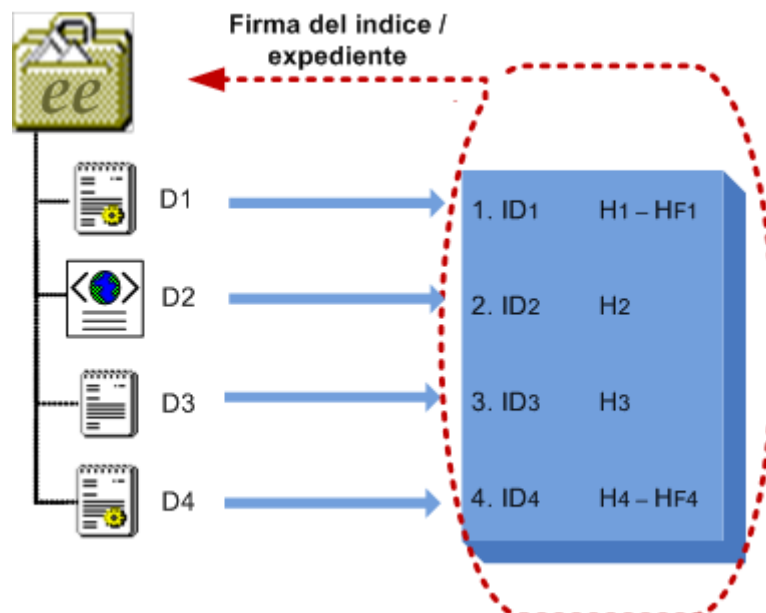
Componentes de la pieza.

Por su naturaleza, si es necesario la pieza se creará dentro de un expediente judicial electrónico. Los componentes de la pieza serán los mismos que los del expediente judicial electrónico excepto la posibilidad de incluir expedientes electrónicos, judiciales o administrativos, anidados o piezas.

No todos los países contemplan la posibilidad de crear piezas separadas, pero todos deben admitir un envío procedente de otro país con piezas o tramitaciones procesales asociadas a un expediente pero independientes de este.

Componente del índice electrónico del procedimiento- expediente digital

El contenido del índice del expediente puede variar según las necesidades de cada organización, la cual puede diseñar diferentes patrones que se ajusten a las actividades y diferentes tipos de procedimientos que desarrolla. También es conveniente utilizar este patrón del índice para definir qué documentos deben integrar un determinado tipo de expediente



Metadatos.

Los metadatos mínimos obligatorios de la capa técnica NIG, del expediente judicial electrónico y de la pieza:

- a) Serán los definidos en el anexo I.
- b) Se asociarán en cada caso para su remisión o puesta a disposición.
- c) Durante la tramitación procesal del expediente judicial electrónico o pieza, los metadatos no serán modificados salvo en supuestos de error material, omisión, aclaración o rectificación de datos o resoluciones o cuando obedezca al contenido de resolución judicial. Se exceptúan aquellos metadatos que, por su propio contenido o definición, son susceptibles de actualización conforme se tramita el procedimiento. Deberá garantizarse el debido acceso a dichas modificaciones, control de su realización, momento y registro del cambio.

Se podrán asignar metadatos complementarios para atender a necesidades de descripción específicas.

Estos metadatos complementarios se aplicarán, en su caso, de acuerdo con la Guía de Interoperabilidad y Seguridad de Política de Gestión de Documentos Electrónicos.

Intercambio de expedientes judiciales electrónicos.

El intercambio de expedientes judiciales electrónicos, a los efectos de remisión y puesta a disposición, se realizará mediante el envío en primer lugar de todo o parte de la estructura definida en el Anexo II. Tras este intercambio, se enviarán cada uno de los documentos electrónicos que componen el todo o parte del expediente que se remite, en el orden indicado en el índice y atendiendo a lo establecido en la Guía de Interoperabilidad y Seguridad del Documento Judicial Electrónico o en la Norma Técnica de Interoperabilidad de Documento Electrónico, en función de la naturaleza del documento.

Cuando la naturaleza o la extensión de los documentos o elementos que forman parte del expediente judicial no permitan o dificulten notablemente su inclusión en una de las estructuras establecidas, se incorporará al expediente judicial electrónico un documento judicial electrónico en el que se especifique cuáles son estos documentos o elementos.



Grupo Tecnologías de Información XVII Edición Cumbre Judicial

El índice electrónico de la capa técnica NIG objeto de intercambio reflejará, al menos:

- a) La fecha de generación del índice.
- b) Los procedimientos/expedientes judiciales electrónicos de los que se compone.

El índice electrónico de los expedientes judiciales electrónicos objeto de intercambio reflejará, al menos:

- a) La fecha de generación del índice.
- b) Para cada documento electrónico, su identificador, su huella digital, la función resumen utilizada para su obtención, que atenderá a lo establecido en la Norma Técnica de Interoperabilidad de catálogo de estándares, la fecha de incorporación al expediente judicial electrónico, el orden del documento dentro del mismo y la tipología respecto del carácter electrónico o digitalización del documento.
- c) Si es el caso, la disposición de los documentos en expedientes judiciales electrónicos o expedientes administrativos electrónicos anidados y/o piezas.

En caso de remisión o puesta a disposición de los expedientes judiciales electrónicos, la verificación de la autenticidad e integridad de un expediente judicial electrónico se llevará a cabo bajo la responsabilidad del órgano judicial transferidor en el momento en que dicha transferencia se produzca.



Grupo Tecnologías de Información XVII Edición Cumbre Judicial

ANEXO I. METADATOS DEL EXPEDIENTE JUDICIAL ELECTRÓNICO

NIG

NIG						
Metadato	Descripción/Condiciones de uso	Cardinalidad	Tipo	Esquema de valores	Ejemplo	Observaciones
IndiceNIG	Contenido del índice del NIG	1				
MetadatosNIG	Metadatos mínimos obligatorios del NIG	1				
VisualizacionIndice	Elemento para incluir una visualización alternativa de la información del NIG, como podría ser el índice o el contenido completo de los documentos que lo componen	0				

INDICE DEL NIG

Metadato	Descripción/Condiciones de uso	Cardinalidad	Tipo	Esquema de valores	Ejemplo	Observaciones
IndiceContenidoNIG	Contenido del índice del NIG	1				
FechaIndiceNIG	Fecha en la que se firma el índice del NIG (conjunto de procedimiento(s) y expediente(s) judicial(es) electrónico(s)) que deberá ser actualizada como mínimo ante un intercambio de al menos un procedimiento/expediente que compone dicho NIG o ante el cierre del último procedimiento/expediente en activo que componen el NIG.	1	TimeStamp	Formato ISO 8601 Ejemplo: AAAA-MM-DD HHMMSS	<2011-03-12 10:32:15>	
Procedimientos_Espedientes	Listado de las referencias de todos los Procedimientos/Expedientes que forman parte de un NIG	1N		<CodigoProcedimiento>: Código entrante de la tabla Tipos de Tramitación del Test de Compatibilidad del CGPJ, 3 caracteres <NumeroProcedimiento>: Secuencial, 7 caracteres <AñoProcedimiento>: Año del procedimiento (Formato: 9999), 4 caracteres	<MON6:<00000088><2010>	
Firmas	Existirá, al menos, una firma del contenido del índice del expediente judicial electrónico					
Firma						
TipoFirma	Indica el tipo de firma electrónica que firma electrónicamente el índice NIG a efectos de garantizar la integridad del expediente judicial electrónico. En caso de firma con certificado, indica el formato de la firma.	1N	Cadena de caracteres	CSV y formatos de firma electrónica definidos en la Ley 18/2011, Codificación: -TF01 - CSV -TF02 - XAdES Internally detached signature -TF03 - XAdES Enveloped signature -TF04 - CAAdES detached/explicit signature -TF05 - CAAdES attached/implicit signature -TF06 - PAdES	<TF02>	
ContenidoFirma						
CSV						
ValorCSV	[Sólo en caso de firma CSV] Valor del CSV	1N	Cadena de caracteres	String		
RegulacionGeneracionCSV	[Sólo en caso de firma CSV] Referencia a la Orden, Resolución o documento que define la creación del CSV correspondiente	1N	Cadena de caracteres	Si AGE: Referencia BOE/BOE-A-YYYY-XXXX; En otro caso, referencia correspondiente.		
FirmaConCertificado						
FirmaBase64	Firma en formato base64	1		base64Binary		
ds:Signature	Estandar http://www.w3.org/2000/09/xmldsig	1		Estandar http://www.w3.org/2000/09/xmldsig		
ReferenciaFirma	Referencia interna al fichero firma, por ejemplo a fichero contenido en caso de firmas attached	1		Cadena de caracteres		



Grupo Tecnologías de Información XVII Edición Cumbre Judicial

METADATOS MÍNIMOS DEL NIG

Metadato	Descripción/Condiciones de uso	Cardinalidad	Tipo	Esquema de valores	Ejemplo	Observaciones
VersionGIS	Identificador normalizado de la versión de la Guía de Interoperabilidad y Seguridad del Expediente Judicial Electrónico	1	URI			
Intencionadamente en blanco						
NIG	Número de Identificación General	1	Cadena de caracteres (19 caracteres)			
Jurisdiccion	Orden jurisdiccional (civil, penal, contencioso o social) al que corresponde el NIG por razón de la materia	1	Cadena de caracteres		<g>	
FechaInicio	Fecha en la que se recibe en la Oficina Judicial (Decanato o Servicio Común) el escrito iniciador del primer procedimiento/expediente del conjunto de procedimientos/expedientes que conforman el NIG. En los casos en los que el primer procedimiento/expediente se inicie de oficio por el Órgano Judicial será la fecha de la primera resolución	1	Fecha/hora	Formato ISO 8601 Ejemplo: AAAA-MM-DD HH:MM:SS	<2011-03-12 10:32:15>	
FechaArchivo	Fecha de archivo del último procedimiento/expediente activo del conjunto de procedimientos/expedientes que conforman el NIG	1	Fecha/hora	Formato ISO 8601 Ejemplo: AAAA-MM-DD HH:MM:SS	<2011-03-12 10:32:15>	Codificación establecida en el hito del TC (1240) correspondiente a la fecha de archivo del último procedimiento/expediente activo del NIG



Grupo Tecnologías de Información XVII Edición Cumbre Judicial

INDICE DEL PROCEDIMIENTO/EXPEDIENTE JUDICIAL ELECTRÓNICO

Metadato	Descripción/Condiciones de uso	Cardinalidad	Tipo	Esquema de valores	Ejemplo	Observaciones
IndiceContenido	Contenido del índice del Procedimiento/Expediente Judicial Electrónico	1				
FechaIndiceProcedimientoExpediente	Fecha en la que se firma el índice del procedimiento/expediente que deberá ser actualizada como mínimo ante un intercambio o cierre del procedimiento/expediente	1	Timestamp	Formato ISO 8601 Ejemplo: AAAA-MM-DD HH:MM:SS	<2011-03-12 10:32:15>	
DocumentoIndizado	Documentos incluidos en el Procedimiento/Expediente	1..N				
IdentificadorDocumento	Código con carácter normalizado y único para la identificación del documento	1	Cadena de caracteres			
ValorHuella	La huella de un documento electrónico se obtiene de la aplicación de una función resumen al fichero de contenido de dicho documento o bien concatenando las huellas de todos los ficheros que lo componen (en caso de documentos con más de un fichero de contenido), pudiendo incluir a su vez la huella del fichero de la firma electrónica de cada uno de ellos, cuando éstas se almacenan en ficheros independientes	1	Cadena de caracteres			
FuncionResumen	Función resumen utilizada para la generación de la huella digital del documento	1	Cadena de caracteres			
TipologiaElectronica	Tipología al respecto del carácter electrónico o digitalización del documento	1	Cadena de caracteres	0- Electrónico 1- Digitalizado 2- No digitalizable	<0>	
FechaCaptura	La fecha de acceso del documento al procedimiento/expediente	1	Fecha/hora	Formato ISO 8601 Ejemplo: AAAA-MM-DD HH:MM:SS	<2011-03-12 10:32:15>	
OrdenDocumentoProcedimientoExpediente	El orden del documento judicial electrónico dentro del procedimiento/expediente	1	Cadena de caracteres	String[S]	<000007>	
ProcedimientoExpedienteIndizado	Listado de cada uno de los procedimientos/expedientes que forman parte de este procedimiento/expediente	1..N		Índice procedimiento/expediente Metadatos procedimiento/expediente Visualización		Ver pestañas Índice Proc_Expediente y Metadatos Proc_Expediente para los metadatos y esquema de valores
Pieza	Listado de cada una de las piezas que forman parte de este procedimiento/expediente	1..N		Índice pieza Metadatos pieza Visualización		Ver pestañas Índice Pieza y Metadatos Pieza para los metadatos y esquema de valores
ExpedienteAdministrado	Listado de cada uno de los expedientes administrativos que forman parte de este procedimiento/expediente	1..N		Índice expediente administrativo Metadatos expediente administrativo Visualización		Ver NTI de Expediente Electrónico
Firmas						
TipoFirma	Indica el tipo de firma electrónica que firma al índice del procedimiento/expediente judicial electrónico a efectos de garantizar la integridad del mismo. En caso de firma con certificado, indica el formato de la firma	1..N	Cadena de caracteres	CSV y formatos de firma electrónica definidos en la Ley 18/2011. Codificación: -T01- CSV -T02- XAdES Internally detached signature -T03- XAdES Enveloped signature -T04- CAdES detached/implicit signature -T05- CAdES attached/implicit signature -T06- PAdES		
ContenidoFirma						
ValorCSV	[Sólo en caso de firma CSV] Valor del CSV	1..N	Cadena de caracteres	N/A		
RegulacionGeneracionCSV	[Sólo en caso de firma CSV] Referencia a la Orden, Resolución o documento que define la creación del CSV correspondiente	1..N	Cadena de caracteres	SI AEE: Referencia BOE-BOE-A-YYYY-XXXXX En otro caso, referencia correspondiente		
FirmaConCertificado						
FirmaBase64	Firma en formato base64	1		base64Binary		
dsSignature	Estándar http://www.w3.org/2000/09/xmldsig#	1		Estándar http://www.w3.org/2000/09/xmldsig#		
ReferenciaFirma	Referencia interna al fichero firma, por ejemplo a fichero contenido en caso de firmas attached	1		Cadena de caracteres		

EJEMPLO DE METADATOS DEL PROCEDIMIENTO/EXPEDIENTE JUDICIAL ELECTRÓNICO

Metadato	Descripción/Condiciones de uso	Cardinalidad	Tipo	Esquema de valores	Ejemplo	Observaciones
VersionGIS	Identificador normalizado de la versión de la Guía de Interoperabilidad y Seguridad del Expediente Judicial Electrónico	1	URI			
ORG	Número de Identificación General	1	Cadena de caracteres (15 caracteres)	Codificación establecida por el CPJ	<090942120100501021>	<Código de municipio>: Codificación extraída de la tabla Municipios del Test de Compatibilidad del CPJ (longitud: 5 caracteres). <Tipo de órgano>: Codificación extraída de la tabla Tipos de Órgano del Test de Compatibilidad del CPJ (longitud: 2 caracteres). <Orden jurisdiccional>: Codificación extraída de la tabla Jurisdicciones del Test de Compatibilidad del CPJ (longitud: 1 carácter). <Año>: Año de la fecha de captura del documento (longitud: 4 caracteres). <Número secuencial>: Número secuencial del documento producido dentro del órgano judicial (longitud: 7 caracteres).
OrganoJudicial	Identificador normalizado del Órgano Judicial titular del Procedimiento/Expediente	1	Cadena de caracteres	Código alfanumérico único para cada órgano judicial extraído del grupo de tablas Unidades Funcionales del Test de Compatibilidad del CPJ	<090942001>	
FechaProcedimientoExpediente	Conjunto de fechas relevantes dentro del Procedimiento/Expediente	1				
FechaPresentacion	Fecha en la que se recibe en la Oficina Judicial (Decanato o Servicio Común) el escrito iniciador del Procedimiento/Expediente	1	Fecha/hora	Formato ISO 8601 Ejemplo: AAAA-MM-DD HH:MM:SS	<2011-03-12 10:32:15>	
FechaRegistro	Fecha de registro en Decanato o Servicio Común. Fecha en la que el escrito iniciador del Procedimiento/Expediente queda registrado en la Unidad Funcional receptora competente para tal actuación (Decanato o Servicio Común)	0	Fecha/hora	Formato ISO 8601 Ejemplo: AAAA-MM-DD HH:MM:SS	<2011-03-12 10:32:15>	
FechaResolucionIniciadora	Fecha de la primera resolución dictada por el Órgano Judicial. Fecha en la que se dicta la primera resolución judicial o del Secretario Judicial en dicho Procedimiento/Expediente	1	Fecha/hora	Formato ISO 8601 Ejemplo: AAAA-MM-DD HH:MM:SS	<2011-03-12 10:32:15>	
FechaUltimaResolucion	Fecha de la última resolución dictada por el Órgano Judicial. Fecha en la que se dicta la última resolución judicial o del Secretario Judicial en dicho Procedimiento/Expediente	1	Fecha/hora	Formato ISO 8601 Ejemplo: AAAA-MM-DD HH:MM:SS	<2011-03-12 10:32:15>	
IdentificadorProcedimiento	Este elemento permite la trazabilidad del procedimiento dentro del Órgano Judicial, registrando los cambios que se puedan producir en el número de dicho Procedimiento	1:N				El identificador del procedimiento se encuentra compuesto por: <Código Procedimiento> (8 dígitos) <Número Procedimiento> (7 dígitos) <Año Procedimiento> (4 dígitos)
CodigoProcedimiento	Código del Procedimiento	1	Cadena de caracteres	Código extraído de la tabla Tipos de Tramitación del Test de Compatibilidad del CPJ	<MON>	3 caracteres
NumeroProcedimiento	Número del Procedimiento	1	Cadena de caracteres	Secuencial	<0000088>	7 caracteres
AñoProcedimiento	Año del Procedimiento	1	Cadena de caracteres	Año del procedimiento (Formato: yyyy)	<2011>	4 caracteres
Situación	Situación del Procedimiento/Expediente en el momento del intercambio	1	Cadena de caracteres	TE01 - Activo TE02 - No Activo	<TE01>	
Intervinientes	Intervinientes en el procedimiento/expediente	0				El elemento Intervinientes será siempre obligatorio, salvo en casos excepcionales (Ej. Auxilio Judicial)
Parte	Partes intervinientes en el procedimiento/expediente	1:N				
DatosPersona	Condición de la parte interviniente cuando no sea Ministerio Fiscal: persona física, persona jurídica o ente sin personalidad	1				
Persona	Condición de la parte interviniente cuando no sea Ministerio Fiscal: persona física, persona jurídica o ente sin personalidad	1				
Personald	Identificación de persona	1				
Tipoidentificacion	Tipo de identificador de persona, persona jurídica o ente sin personalidad jurídica	1	Cadena de caracteres	Código extraído de la tabla Tipos de Identificación del Test de Compatibilidad del CPJ	<D>	
Identificacion	Identificador dependiente del valor del tipo de identificación seleccionado	1	Cadena de caracteres	String	<123456782>	
PersonaFisica	Datos de la persona física	1				
Nombre	Nombre	1	Cadena de caracteres	String	<Alberto>	
PrimerApellido	Primer apellido	1	Cadena de caracteres	String	<López>	
SegundoApellido	Segundo apellido	0	Cadena de caracteres	String	<Pérez>	
Nacionalidad	Nacionalidad de la persona	1	Cadena de caracteres	Código extraído de la tabla Países y Nacionalidades (ISO 3166) del Test de Compatibilidad del CPJ	<ES>	
Sexo	Sexo de la persona	1	Cadena de caracteres	Código extraído de la tabla Tipos de Sexo del Test de Compatibilidad del CPJ	<M>	
Personajuridica	Datos de la persona jurídica	1				
NombreEntidad	Nombre de la entidad	1	Cadena de caracteres	String	<NombreEntidad S.A.>	



Grupo Tecnologías de Información

XVII Edición Cumbre Judicial

EnteSinPersonalidadJuridica	Datos de la persona jurídica	1				
NombreEntidad	Nombre de la entidad	1	Cadena de caracteres	String	<NombreEntidad>	
Representacion						
	Información de representación procesal y defensa	0/N				
RepresentanteColegado	Información de representante en caso de ser un profesional colegiado contemplado por tipo de representación	1				
Colegio	Identificación del Colegio Profesional en el que está inscrito	1	Cadena de caracteres	Código extraído de la tabla Colegios Profesionales del Text de Compatibilidad del (COP)	<AD1059>	
Representanteld	Nº de colegiado según el Colegio Profesional	1	Cadena de caracteres	String	<11230>	
Personald	Identificación como persona física	0	Cadena de caracteres	String	<N>	
Nombre	Nombre	1	Cadena de caracteres	String	<Juan>	
PrimerApellido	Primer apellido	1	Cadena de caracteres	String	<Espinola>	
SegundoApellido	Segundo apellido	0	Cadena de caracteres	String	<Gómez>	
RepresentanteAdmon						
	Información de representante en caso de ser un profesional de la Administración contemplado por tipo de representación	1				
Personald	Identificación como persona física o jurídica. Ver los metadatos del tipo complejo Personald	1	Cadena de caracteres	<Tipoidentificacion> + <Identificacion>	<N> + <123456782>	
Nombre	Nombre de pila	0	Cadena de caracteres	String	<Luis>	
PrimerApellido	Primer apellido	0	Cadena de caracteres	String	<González>	
SegundoApellido	Segundo apellido	0	Cadena de caracteres	String	<Gutiérrez>	
RepresentanteLegal						
	Información de representante en caso de no ser ninguno de los anteriores casos	1				
Personald	Identificación de persona. Ver los metadatos del tipo complejo Personald	1	Cadena de caracteres	<Tipoidentificacion> + <Identificacion>	<N> + <123456782>	
PersonaFisica	Datos de la persona física. Ver los metadatos del tipo complejo PersonaFisica	1	Cadena de caracteres	<Nombre> + <PrimerApellido> + <SegundoApellido> + <Nacionalidad> + <Sexo>	<liberto> + <López> + <Pérez> + <ES> + <M>	
PersonaJuridica	Datos de la persona jurídica. Ver los metadatos del tipo complejo PersonaJuridica	1	Cadena de caracteres	<Nombre de la entidad>	<NombreEntidad S.A.>	

ÍNDICE DE LA PIEZA

INDICE PIEZA						
Metadato	Descripción/Condiciones de uso	Cardinalidad	Tipo	Esquema de valores	Ejemplo	Observaciones
IndiceContenidoPieza	Contenido del índice de la pieza	1				
FechaIndicePieza	Fecha en la que se firma el índice de la pieza perteniente a un procedimiento/expediente, que deberá ser actualizada como mínimo ante un intercambio o cierre de la totalidad de la pieza	1	TimeStamp	Formato ISO 8601 Ejemplo: AAAA-MM-DD HH:MM:SS	<2011-03-12 10:32:15>	
DocumentoIncluido	Documentos incluidos en la pieza	1..N				
IdentificadorDocumento	Código con carácter normalizado y único para la identificación del documento	1	Cadena de caracteres			
ValorHuella	La huella de un documento electrónico se obtiene de la aplicación de una función resumen al fichero de contenido de dicho documento o bien concatenando las huellas de todos los ficheros que lo componen (en caso de documentos con más de un fichero de contenido), pudiendo incluir a su vez la huella del fichero de la firma electrónica de cada uno de ellos, cuando éstas se almacenan en ficheros independientes.	1	Cadena de caracteres			
FuncionResumen	Función resumen utilizada para la generación de la huella digital del documento	1	Cadena de caracteres			
TipologiaElectronica	Tipología al respecto del carácter electrónico o digitalización del documento	1	Cadena de caracteres	0 - Electrónico 1 - Digitalizado - No digitalizable	<0>	
FechaCreacion	La fecha de creación o incorporación del documento judicial electrónico a la pieza (resolución iniciadora de la pieza)	1	Fecha/hora	Formato ISO 8601 Ejemplo: AAAA-MM-DD HH:MM:SS	<2011-03-12 10:32:15>	
OrdenDocumentoPieza	El orden del documento dentro de la pieza	1	Cadena de caracteres	String[6]	<000001>	
Firmas						
Firma						
TipoFirma	Indica el tipo de firma electrónica que firma electrónicamente el índice NIG a efectos de garantizar la integridad del expediente judicial electrónico. En caso de firma con certificado, indica el formato de la firma	1..N	Cadena de caracteres	CSV y formatos de firma electrónica definidos en la Ley 13/2011. Codificación: -TF01 - CSV -TF02 - XAdES Internally detached signature -TF03 - XAdES Enveloped signature -TF04 - CAdES detached/explicit signature -TF05 - CAdES attached/implicit signature -TF06 - PAdES	<TF03>	
ContenidoFirma						
CSV						
ValorCSV	Sólo en caso de firma CSV Valor del CSV	1..N	Cadena de caracteres	String		
RegulacionGeneracionCSV	Sólo en caso de firma CSV Referencia a la Orden, Resolución o documento que define la creación del CSV correspondiente	1..N	Cadena de caracteres	3 ADE. Referencia BOE/BOE-A-YYYY-XXXXX En otro caso, referencia correspondiente.		
FirmaConCertificado						
FirmaBase64	Firma en formato base64	1		base64Binary		
ds:Signature	Estandar http://www.w3.org/2000/09/mxdsig	1		Estandar http://www.w3.org/2000/09/mxdsig		
ReferenciaFirma	Referencia interna al fichero firma, por ejemplo a fichero contenido en caso de firmas attached	1		Cadena de caracteres		



Grupo Tecnologías de Información XVII Edición Cumbre Judicial

EJEMPLO DE METADATOS DE LA PIEZA

Metadato	Descripción/Condiciones de uso	Cardinalidad	Tipo	Esquema de valores	Ejemplo	Observaciones
VersionGIS	Identificador normalizado de la versión de la Guía de Interoperabilidad y Seguridad del Expediente Judicial Electrónico	1	URI	N/A		
NIG	Número de Identificación General	1	Cadena de caracteres		<0905942120100501021>	
OrganoJudicial	Identificador normalizado del Órgano Judicial titular de la pieza	1	Cadena de caracteres	Código alfanumérico único para cada órgano judicial extraído del grupo de tablas Unidades Funcionales, del Test de Compatibilidad del CGPJ	<0905942001>	
FechaPieza	Conjunto de fechas relevantes dentro de la	1				
FechaResolucionIniciadora	Fecha de la primera resolución dictada por el Órgano Judicial. Fecha en la que se dicta la primera resolución judicial o del Secretario Judicial en dicha pieza	1	Fecha/hora	Formato ISO 8601 Ejemplo: AAAA-MM-DD HH:MM:SS	<2011-03-12 10:32:15>	
FechaUltimaResolucion	Fecha de la última resolución dictada por el Órgano Judicial. Fecha en la que se dicta la última resolución judicial o del Secretario Judicial en dicha pieza	1	Fecha/hora	Formato ISO 8601 Ejemplo: AAAA-MM-DD HH:MM:SS	<2011-03-12 10:32:15>	
IdentificadorProcedimiento_Pieza	Este elemento permite mantener la trazabilidad de la pieza dentro del Órgano Judicial, permitiendo registrar los cambios que se puedan producir en el número de dicha pieza	1:N				El Procedimiento se encuentra compuesto por : <codigoProcedimiento>(3 dígitos) <numeroProcedimiento>(7 dígitos) <añoProcedimiento>(4 dígitos) La pieza se encuentra compuesta por : <codigoPieza>(3 dígitos) <numeroPieza>(7 dígitos) <añoPieza>(4 dígitos) <subindicePieza>(7 dígitos)
CodigoProcedimiento	Código del Procedimiento	1	Cadena de caracteres	Código extraído de la tabla Tipos de Tramitación del Test de Compatibilidad del CGPJ	<MON>	3 caracteres
NumeroProcedimiento	Número del Procedimiento	1	Cadena de caracteres	Secuencial	<0000088>	7 caracteres
AnioProcedimiento	Año del Procedimiento	1	Cadena de caracteres	Año del procedimiento (Formato: yyyy)	<2010>	4 caracteres
CodigoPieza	Código de la pieza	1	Cadena de caracteres	Esquema de valores normalizado según el test de compatibilidad del CGPJ		3 caracteres. Codificación en proceso de definición por parte del CGPJ
NumeroPieza	Número de la pieza	1	Cadena de caracteres	Secuencial	<0000021>	7 caracteres. Codificación en proceso de definición por parte del CGPJ
AnioPieza	Año de la pieza	1	Cadena de caracteres	Año de la pieza (Formato: yyyy)	<2010>	4 caracteres. Codificación en proceso de definición por parte del CGPJ
SubindicePieza	Subíndice que identifica la pieza dentro del procedimiento/legado	1	Cadena de caracteres	Secuencial	<0000001>	7 caracteres. Codificación en proceso de definición por parte del CGPJ
Situación	Situación de la Pieza en el momento del intercambio	1	Cadena de caracteres	TE01 - Activo TE02 - No Activo	<TE01>	
Intervinientes	Datos de las distintas partes intervinientes en la pieza	0				El elemento Intervinientes será siempre obligatorio, salvo en casos excepcionales (Ej: Auxilio judicial)
Parte	Datos de las distintas partes intervinientes en la pieza	1:N				
DatosPersona	Condición de la parte interviniente cuando no sea Ministerio Fiscal: persona física, persona jurídica o ente sin personalidad	1				
Persona	Condición de la parte interviniente cuando no sea Ministerio Fiscal: persona física, persona jurídica o ente sin personalidad	1				
Personald	Identificación de persona	1				
Tipoidentificacion	Tipo de identificador de persona, persona jurídica o ente sin personalidad jurídica	1	Cadena de caracteres	Código extraído de la tabla Tipos de Identificación del Test de Compatibilidad del CGPJ	<0>	
Identificacion	Identificador dependiendo del valor del tipo de identificación seleccionado	1	Cadena de caracteres	Esquema de valores normalizado según el test de compatibilidad del CGPJ	<123456782>	
Personafisica	Datos de la persona física	1				
Nombre	Nombre	1	Cadena de caracteres	String	<Alberto>	
PrimerApellido	Primer apellido	1	Cadena de caracteres	String	<Lopez>	
SegundoApellido	Segundo apellido	0	Cadena de caracteres	String	<Perez>	
Nacionalidad	Nacionalidad de la persona	1	Cadena de caracteres	Código extraído de la tabla Países y Nacionalidades (ISO 3166) del Test de Compatibilidad del CGPJ	<ES>	
Sexo	Sexo de la persona	1	Cadena de caracteres	Código extraído de la tabla Tipos de Sexo del Test de Compatibilidad del CGPJ	<M>	
Personajuridica	Datos de la persona jurídica	1				
NombreEntidad	Nombre de la entidad	1	Cadena de caracteres	String	<NombreEntidad S.A.>	
EnteSinPersonalidadJuridica	Datos de la persona jurídica	1				
NombreEntidad	Nombre de la entidad	1	Cadena de caracteres	String	<NombreEntidad>	

Representación	Información de representación procesal y defensa	D/N				
RepresentanteColegiado	Información de representante en caso de ser un profesional colegiado contemplado por tipo de representación	1				
Colegio	Identificación del Colegio Profesional en el que está inscrito	1	Cadena de caracteres	Código extraído de la tabla Colegios Profesionales del Test de Compatibilidad del CGPJ	<A01059>	
RepresentanteId	Nº de colegiado según el Colegio Profesional	1	Cadena de caracteres	String	<11230>	
Personald	Identificación como persona física	0	Cadena de caracteres	<Tipoidentificación> + <Identificación>	<0> + <123456782>	
Nombre	Nombre	1	Cadena de caracteres	String	<Alberto>	
PrimerApellido	Primer apellido	1	Cadena de caracteres	String	<Lopez>	
SegundoApellido	Segundo apellido	0	Cadena de caracteres	String	<Perez>	
RepresentanteAdmon	Información de representante en caso de ser un profesional de la Administración contemplado por tipo de representación	1				
Personald	Identificación como persona física o jurídica. Ver los metadatos del tipo complejo Personald	1	Cadena de caracteres	<Tipoidentificación> + <Identificación>	<0> + <123456782>	
Nombre	Nombre de pila	0	Cadena de caracteres	String	<Alberto>	
PrimerApellido	Primer apellido	0	Cadena de caracteres	String	<Lopez>	
SegundoApellido	Segundo apellido	0	Cadena de caracteres	String	<Perez>	
RepresentanteLegal	Información de representante en caso de no ser ninguno de los anteriores casos	1				
Personald	Identificación de persona. Ver los metadatos del tipo complejo Personald	1	Cadena de caracteres	<Tipoidentificación> + <Identificación>	<0> + <123456782>	
Personafisica	Datos de la persona física. Ver los metadatos del tipo complejo Personafisica	1	Cadena de caracteres	<Nombre> + <PrimerApellido> + <SegundoApellido> + <Nacionalidad> + <Sexo>	<Alberto> + <Lopez> + <Perez> + <ES> + <0>	
Personajuridica	Datos de la persona jurídica. Ver los metadatos del tipo complejo Personajuridica	1	Cadena de caracteres	<Nombre de la entidad>	<NombreEntidad S.A.>	

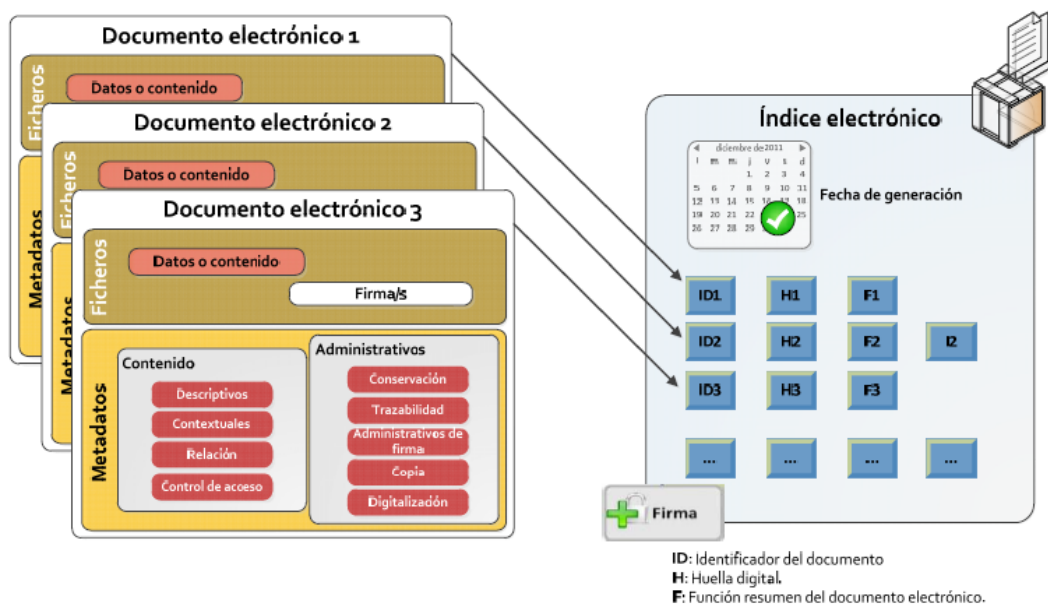


**Grupo Tecnologías de Información
XVII Edición Cumbre Judicial**

**BORRADOR DE GUÍA DE INTEROPERABILIDAD Y SEGURIDAD
DE DOCUMENTO JUDICIAL ELECTRÓNICO**

Objeto.

La Guía de Interoperabilidad y Seguridad del Documento Judicial Electrónico tiene por objeto establecer los componentes del documento judicial electrónico, así como la estructura y formato técnicos a fin de garantizar su intercambio.



Componentes del documento judicial electrónico.

Los componentes de un documento judicial electrónico son:

- Contenido, entendido como conjunto de datos o información del documento.
- Firma electrónica reconocida de acuerdo con lo que establece la sección segunda, capítulo II, Título III.
- Metadatos del documento judicial electrónico.

El documento electrónico que incluya la fecha electrónica y tenga incorporada la firma electrónica, de conformidad con lo dispuesto en las leyes procesales de cada país, tendrá la consideración de documento público.

Firma del documento judicial electrónico.

Los documentos judiciales electrónicos, tendrán siempre asociada, al menos, una firma electrónica de acuerdo con lo establecido en la Administración de Justicia y el resto de la normativa aplicable.

Metadatos del documento judicial electrónico.

1. Los metadatos mínimos obligatorios del documento judicial electrónico:
 - a) Serán los definidos en el anexo I.
 - b) Estarán presentes en cualquier proceso de intercambio de documentos judiciales electrónicos dentro de la Administración de Justicia o con otras Administraciones y organismos públicos.
 - c) Los documentos judiciales electrónicos, deberán tener asociados metadatos que permitan su identificación, localización y contextualización en el marco del órgano, función o procedimiento al que corresponde.

- d) Durante la tramitación del expediente judicial electrónico, los metadatos del documento judicial electrónico no serán modificados salvo en supuestos de error material, omisión, aclaración o rectificación de datos o resoluciones o cuando obedezca al contenido de resolución judicial. Se exceptúan aquellos metadatos que, por su propio contenido o definición, son susceptibles de actualización conforme se tramita el procedimiento. Deberá garantizarse el debido acceso a dichas modificaciones, control de su realización, momento y registro del cambio.
2. Se podrán asignar metadatos complementarios para atender a necesidades de descripción específicas. Estos metadatos complementarios se aplicarán, en su caso, de acuerdo con la Guía de Interoperabilidad y Seguridad de Política de Gestión de Documentos Electrónicos.
 3. Cada País podrá implementar aquellos metadatos de los documentos judiciales electrónicos para su tratamiento y gestión a nivel interno. Además, garantizará la disponibilidad e integridad de los metadatos de sus documentos judiciales electrónicos, manteniendo de manera permanente las relaciones entre el documento y sus metadatos.

Formato de documentos judiciales electrónicos.

1. Los ficheros de contenido de los documentos judiciales electrónicos se ajustarán a los formatos establecidos para este tipo de ficheros en los catálogos de estándares que se acuerden entre los países Iberoamericanos.
2. La elección del formato se realizará conforme a la naturaleza de la información a tratar primando la finalidad para la cual fue definido cada formato.
3. Se podrán utilizar otros formatos cuando existan particularidades que lo justifiquen o sea necesario.

ANEXOS

ANEXO I

EJEMPLO DE METADATOS OBLIGATORIOS DEL DOCUMENTO JUDICIAL ELECTRÓNICO

Metadato	Descripción/Condiciones de uso	Cardinalidad	Tipo	Esquema de valores	Ejemplo	Observaciones
ContenidoDocumentoJudicial						
IdentoXML	Contenido en formato XML. En caso de datos XML, cuya codificación ofiera de la de esta estructura, tal se incluirá una cláusula CDATA.		Cadena de caracteres			
ValorBinario	Contenido en base64		Cadena de caracteres			
ReferenciaFichero	Referencia interna al fichero de contenido		Cadena de caracteres			
NombreFormato	El formato del fichero de contenido del documento electrónico atenderá a lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares	1	Cadena de caracteres	Extrajo de la NTI de Catálogo de estándares	<DOC>	
MetadatosDocumentoJudicial						
VersionGIS	Identificador normalizado de la versión de la Guía de Interoperabilidad y Seguridad del Documento Judicial Electrónico conforme a la cual se estructura el documento judicial electrónico	1	URI			
IdentificadorIntercambio	Código con carácter normalizado y único para la identificación del documento electrónico	1	Cadena de caracteres (24 caracteres)	<Código de población> + <Tipo de órgano> + <Orden jurisdiccional> + <Número secuencial> + <Año>	<18003> + <13> + <1> + <00000000000000000000> + <2011>	Codificación del identificador del documento: <Código de población> Codificación extraída de la tabla Municipios del Test de Compatibilidad del CSJF (longitud: 5 caracteres). <Tipo de órgano> Codificación extraída de la tabla Tipos de Órgano del Test de Compatibilidad del CSJF (longitud: 2 caracteres). <Orden jurisdiccional> Codificación extraída de la tabla Jurisdicciones del Test de Compatibilidad del CSJF (longitud: 1 carácter). <Número secuencial> Número secuencial del documento producido dentro del órgano judicial (longitud: 12 caracteres). <Año> Año de la fecha de captura del documento (longitud: 4 caracteres).
NIJ	Número de identificación General	1	Cadena de caracteres (19 caracteres)	Codificación establecida por el CSJF	<090942120100501021>	<Código de municipio> Codificación extraída de la tabla Municipios del Test de Compatibilidad del CSJF (longitud: 5 caracteres). <Tipo de órgano> Codificación extraída de la tabla Tipos de Órgano del Test de Compatibilidad del CSJF (longitud: 2 caracteres). <Orden jurisdiccional> Codificación extraída de la tabla Jurisdicciones del Test de Compatibilidad del CSJF (longitud: 1 carácter). <Año> Año de la fecha de captura del documento (longitud: 4 caracteres). <Número secuencial> Número secuencial del documento producido dentro del órgano judicial (longitud: 7 caracteres).
UnidadProductora		1	Cadena de caracteres			
UnidadTitular		1	Cadena de caracteres			
CódigoJurisdicción	Código de la jurisdicción a la que pertenece el documento	1	Cadena de caracteres		<2>	
CódigoEspecialidad	Código de la especialidad a la que pertenece el documento	1	Cadena de caracteres		<13>	
Procedimiento_Pieza	Procedimiento o pieza al que está asociado el documento. Está compuesto por el código de procedimiento, el número de procedimiento y el año del procedimiento, o si el documento pertenece a una pieza el código de la pieza, el número de la pieza, el año de la pieza y el subíndice de la pieza					
CódigoProcedimiento	Código del procedimiento	1	Cadena de caracteres		<M00>	3 caracteres
NúmeroProcedimiento	Número del procedimiento	1	Cadena de caracteres	Secuencial	<0000001>	7 caracteres
AñoProcedimiento	Año del procedimiento	1	Cadena de caracteres	Año del procedimiento (Formato: yyyy)	<2011>	4 caracteres
CódigoPieza	Código de la pieza	0	Cadena de caracteres			
NúmeroPieza	Número de la pieza	0	Cadena de caracteres	Secuencial	<0000002>	7 caracteres
AñoPieza	Año de la pieza	0	Cadena de caracteres	Año de la pieza (Formato: yyyy)	<2011>	4 caracteres
SubíndicePieza	Subíndice que identifica la pieza dentro del procedimiento	0	Cadena de caracteres			
ÓrganoJudicial	Órgano judicial que está conociendo del procedimiento judicial electrónico	1	Cadena de caracteres		<001437920>	

TipologíaElectronica	Tipología al respecto del carácter electrónico o digitalización del documento	1	Cadena de caracteres	0- Electrónico 1- Digitalizado 2- No digitalizable	<1>	
FechaCapturaDocumento		1	Fecha/hora	Formato: AAAAMMDDTHH:MM:SS <ISO 8601>	<2011-03-12 10:32:15>	
FechaCreacionDocumento	Fecha en la que se creó el documento	0	Fecha/hora	Formato ISO 8601 Ejemplo: AAAAMMDD HH:MM:SS	<2011-03-12 10:32:15>	
IdiomaDocumento	Idioma en el que está redactado el documento	0	Cadena de caracteres	Código extraído de la tabla de idiomas del estándar ISO 639-1	<124>	
OrigenCiudadanoAdministracionOrigenJudicial	Indica la condición particular o profesional del emisor del documento	1	Cadena de caracteres	T001 - Interventista T002 - Abogado T003 - Procurador T004 - Administración T005 - Órgano Judicial T006 - Médico Forense T007 - Ministerio Fiscal T008 - Fuerzas y Cuerpos de Seguridad del Estado T009 - Graduado Social	<T002>	
NaturalezaDocumento	Indica la naturaleza del documento. Si es copia, este metadato indica también si se ha realizado una digitalización o conversión de formato en el proceso de generación: - Original - Copia electrónica auténtica con cambio de formato (Ley 18/2011 Art. 28.1) - Copia electrónica auténtica de documento papel (Ley 18/2011 art. 28.2 y 30.3) - Copia electrónica auténtica parcial - Otros: LEC	1	Cadena de caracteres	E01 - Original E02 - Copia electrónica auténtica con cambio de formato E03 - Copia electrónica auténtica de documento papel E04 - Imagen electrónica aportada por el ciudadano E05 - Copia electrónica parcial auténtica E09 - Otros.	<E01>	
IdentificadorDocumentoOrigen	Identificador normalizado del documento origen al que corresponde la copia	0	Cadena de caracteres			
SecretoActuacion	Indica si se ha accedido al secreto de las actuaciones en el documento judicial electrónico. Dato obligatorio para discriminar en caso de secreto parcial o total, si el documento referido está afectado por el mismo	1	Boolean	0- No 1- Sí	<0>	
CircunstanciasEspeciales	Indica si en el documento existen circunstancias especiales tales como: causa con preso, violencia de género, etc	0/N	Cadena de caracteres	TCE01 - Causa con preso TCE02 - Violencia de género TCE03 - Testigo protegido TCE04 - Agente encubierto	<TCE01>	
TipoDocumental	Tipología de documentos	1	Cadena de caracteres	Mapa documental judicial español		
NombreFormato	Formato lógico del fichero de contenido del documento judicial electrónico	1	Cadena de caracteres	Valor extraído de la lista de formatos admitidos para documentos judiciales electrónicos definidos en la Norma Técnica de Interoperabilidad de Catálogo de estándares	<DOC>	
OrdenDocumentoProcedimientoExpediente	Posición del documento judicial electrónico dentro del procedimiento/expediente a juicio	1	Cadena de caracteres	String[5]	<000009>	
MetadatosDocumentoENI		0				
VersionENI	Identificador normalizado de la versión de la Norma Técnica de Interoperabilidad del Documento Electrónico	1	URI			
Identificador	Identificador normalizado del documento	1	Cadena de caracteres	ES_<Organismo>_<AAAA>_<ID_especifico> <ES_E00010207_2010_MPR0000000000000000000010207>	<Organismo> 4 caracteres <AAAA> 4 caracteres <ID_especifico> 30 caracteres	
Organo	Identificador normalizado de la administración generadora del documento o que realiza la captura del mismo	1/N	Cadena de caracteres	Código alfanumérico único para cada Organismo/Jurisdicción extraído del Directorio Común gestionado por el MPTAP	<E00010207>	
FechaCaptura	Fecha de alta del documento en el sistema de gestión documental	1	Fecha/hora	Formato ISO 8601 Ejemplo: AAAAMMDD HH:MM:SS	<2011-03-12 10:32:15>	
Origen	Indica si el contenido del documento fue creado por el ciudadano o por una administración	1	Boolean	0 - Ciudadano 1 - Administración	<0>	
EstadoElaboracion	Indica la naturaleza del documento. Si es copia, este metadato indica también si se ha realizado una digitalización o conversión de formato en el proceso de generación	1	Cadena de caracteres	<ValorEstadoElaboracion> <E01> <E02> <E03> <E04> <E05> <E09> <IdentificadorDocumentoOrigen>	E01 - Original (Ley 11/2007 Art. 30) E02 - Copia electrónica auténtica con cambio de formato (Ley 11/2007 Art. 30.1) E03 - Copia electrónica auténtica de documento papel (Ley 11/2007 Art. 30.2 y 30.3) E04 - Copia electrónica auténtica de documento electrónico E09 - Otros	
TipoDocumental	Descripción del tipo documental del documento	1	Cadena de caracteres	- T001 - Resolución. - T002 - Acuerdo. - T003 - Contrato. - T004 - Convenio. - T005 - Declaración. /Documentos de transmisión/ - T006 - Comunicación. - T007 - Notificación. - T008 - Publicación. - T009 - Acta de recibo. /Documentos de constancia/ - T010 - Acta. - T011 - Certificado. - T012 - Origenia. /Documentos de juicio/ - T013 - Informe. /Documentos de ciudadano/ - T014 - Solicitudes. - T015 - Denuncia. - T016 - Alegación. - T017 - Recursos. - T018 - Comunicación ciudadano. - T019 - Factura. - T020 - Otros inscritados. /Otros/ - T099 - Otros.	<T002>	
Firma	Exibirá, si menos, una firma del contenido del índice del documento judicial electrónico					
Firma	Indica el tipo de firma electrónica que firma electrónicamente el índice NIG a efectos de garantizar la integridad del expediente judicial electrónico. En caso de firma con certificado, indica el formato de la firma	1/N	Cadena de caracteres	CSV y formatos de firma electrónica señalados en la Ley 18/2011. Codificación: - T001 - CSV - T002 - iMDEInternally detached signature - T003 - iMDE Enveloped signature - T004 - CAdES detached/implicit signature - T005 - CAdES detached/implicit signature - T006 - iMDE	<T002>	
ContenidoFirma						
ValorCSV	Sólo en caso de firma CSV	1/N	Cadena de caracteres	String		
RegulacionGeneracionCSV	Sólo en caso de firma CSV	1/N	Cadena de caracteres	Si AGE Referencia BOE/A/YYY-XXXXX en otro caso, referencia correspondiente		
FirmaConCertificado						
FirmaBase64	Firma en formato base64	1		base64Binary		
esSignature	Estándar http://www.w3.org/2000/09/xmldsig	1		Estándar		
ReferenciaFirma	Referencia interna al fichero firma, por ejemplo a fichero contenido en caso de firmas attached.	1		http://www.w3.org/2000/09/xmldsig Cadena de caracteres		

CONCLUSIONES QUINTA FERIA DE JUSTICIA Y TECNOLOGIA

Diferentes han sido las necesidades que han impulsado a las instituciones del sistema de justicia a modernizarse en cuanto al uso de herramientas tecnológicas de la información y comunicación; mejorar el acceso a la justicia; lograr un acercamiento a la comunidad a través del acceso a la información legal, tanto respecto de las leyes, de los tribunales y del funcionamiento de la institución en general como a las causas propiamente tal; facilitar y hacer más efectiva la tramitación de causas; y, en general, mejorar la organización del trabajo y transparencia de la información, entre otras.

I. INTEROPERABILIDAD E INTEGRACIÓN DE SISTEMAS

Cómo se aborda la interoperabilidad e integración desde las siguientes perspectivas:

- Diversidad de plataformas / Lenguajes/Protocolos
- Gobernabilidad de Servicios / Evolución de servicios e implementación de SOA.
- Cómo se identifica qué tipo de herramientas (Bus de Servicios u otros) son necesarios y cómo se justifica su inversión.
- Ventajas Tecnológicas
- Alternativas de Mercado, herramientas abiertas vs herramientas licenciadas.

Conclusiones:

En los Poderes Judiciales de los diferentes países pertenecientes a la Cumbre, se ha implementado la interoperabilidad entre diferentes plataformas desde los años 2000, con organismos relacionados, de manera un tanto artesanal, es decir, con los recursos con que se contaban en su momento, de acuerdo a los intereses o la problemática que se requería abordar, utilizando intercambio de archivos o de procesos batch hasta desarrollo de web service, siendo estos los más recientes.

Hoy se ha visto la clara necesidad de dar un paso más adelante para implementar la interoperabilidad de manera ordenada y cumpliendo con los estándares necesarios, siendo esta una visión país. Entendiendo que la interoperabilidad facilita el poder atender las solicitudes que se le hacen a las instituciones, reduciendo los tiempos de

respuesta de manera más eficiente, optimizando los recursos al utilizar un solo canal, al atender muchas consultas a la vez y de la misma manera, con un mismo protocolo y con las mismas reglas de negocio.

Sin la interoperabilidad los procesos son más tediosos, el margen de error es mayor y poco controlable, se evidencia una vez ocurre y los planes de acción se van a dar de manera correctiva y no preventiva.

La interoperabilidad tiene 2 ámbitos: infraestructura tecnológica y los catálogos o protocolos.

En la interoperabilidad uno de los hitos relevantes es establecer los dueños de la información, es decir donde nace, donde surge la información, quien la genera realmente, donde es su origen y quien tiene la información, lo cual se debe definir de manera previa, luego se debe establecer quién va a mantener dicha información.

En Principio cada país es el dueño de su información y de la manera en que la disponibiliza.

La información que se está entregando se debe indicar si es información oficial o si es meramente referencial, cuando se puede distribuir y a quien se le puede distribuir.

La entrega de información se debe ofrecer oficialmente, pero no debe generar responsabilidad.

Debe existir un registro de cada pregunta y cada respuesta para poder establecer cuando se ha modificado la información, es decir, cuando se ha modificado efectivamente y no de manera referencial.

Los estados de la información debe propender a que sea: Original, actualizada y verificada.

Se define un catálogo, se pone a disposición de los posibles proveedores y se consolida.

Un catálogo se puede definir en aproximadamente 6 meses.

Una plataforma de interoperabilidad se puede implementar la infraestructura unos 3 meses.

La interoperabilidad permite que la información de la que se dispone pueda ser inserta en cualquier sistema que lo reciba.

El marco de la interoperabilidad debe estar enfocado a mejorar los procesos jurídicos. El implementar una plataforma de interoperabilidad es un tema gobierno actualmente, pero ello no limita a que una organización se prepare dando el primer paso con la definición de su protocolo y diccionario de información.

II. SEGURIDAD INFORMÁTICA

La seguridad informática cada vez toma un peso más relevante en los aspectos tecnológicos y es por ello que se hace deseable abordar los siguientes temas:

- La seguridad de las plataformas y los sistemas y sus protocolos
- Que estructura de seguridad implementar y como identificar las herramientas adecuadas
- Administración unificada de usuarios
- Firma Electrónica Avanzada y garantía de la veracidad de los documentos en el largo plazo

Conclusiones:

Dos elementos a considerar cuando hablamos de seguridad de la información:

1. El acceso a la información.
2. La modificación o alteración de la información.
3. Se debe establecer un protocolo de seguridad a seguir como lineamiento.

La seguridad tiene un papel relevante en los procesos de interoperabilidad ya que en este proceso lo relevante es que se está compartiendo información de las bases de datos.

Para el reconocimiento de las personas hay 3 elementos a considerar:

1. Como Identificar,
2. Como autenticar,
3. La autorización (roles y perfiles asociados).

La tendencia en las organizaciones es a 0 en cuanto a los especialistas en la seguridad, si bien se puede invertir en plataformas de seguridad, no todas las organizaciones cuentan con un grupo de especialistas en seguridad que apoye la plataforma tecnológica implementada, que asegure aplicaciones que cumpla con los estándares de seguridad, que monitoree las posibles vulnerabilidades que se tengan en la organización.

Los 3 elementos relevantes y que son un eslabón de la seguridad:

1. Tecnologías, securizar la plataforma y Software
2. Procesos, establecer y difundir los procesos de seguridad
3. Personas, capacitarlos y comprometerlos y responsabilizarlos

En la ingeniería social es donde más inseguridad existe.

La seguridad no debe estar orientada solo a la calle, debe estar orientada también al interior de las organizaciones, se debe educar a los funcionarios respecto de los responsables que cada uno de ellos es en la información que está manejando y a la que tiene acceso.

Una problemática actual es identificar quienes han tenido acceso a la información que tenemos en las diferentes BD, la práctica es almacenar o dejar registro de acciones cuando esta obedece a una transacción, pero por las consultas no siempre se almacena información, ya que se convierte en algo muy costoso, si no se cuenta con

un protocolo adecuado de cuánto tiempo es prudente almacenar este tipo de información, por ejemplo.

El mecanismo y la tendencia es ir a un monitoreo 7 por 24 del acceso a las Bases de datos de manera indiscriminada, es decir no solo por transacciones, sino por consultas, por la sensibilidad de la información, especialmente respecto de aquella que tiene carácter de reservada.

Las organizaciones deben poder reaccionar a tiempo y de manera eficiente frente a ataques a su información, porque recordemos que lo que almacenamos es información, muy sensible.

Cuando hablamos sobre seguridad de la información, se debe pensar siempre en el antes, durante y después, es decir poder detectar el riesgo, identificar el riesgo, reaccionar ante el riesgo.

III. SOFTWARE

Hoy se tiene experiencia en aplicaciones para elaborar y conformar un expediente de manera electrónica y se hace necesario revisar:

- Consecuencias que ha traído la implementación del expediente digital a nivel tecnológico.
- Uso de sistemas open source
- El desarrollo propio de sistemas
- ERP para instituciones públicas
- Plataformas de Inteligencia de negocio
- Firma Electrónica Avanzada (Auto certificadores – empresa certificadora)

Conclusiones:

Lo primero que se persiguió con el expediente electrónico fue concentrarlo en un solo punto con acceso múltiple, desde diferentes partes a través de una Base de Datos que

contuviera todos los documentos propios de la causa, se logró suprimir el papel y fundir la información en un documento digital, siendo luego lo más importante, el poder extraer hitos del mismo que ayuden a hacer gestión.

Pasar del papel al expediente digital es un cambio que ha requerido mucho apoyo, hace parte de lo que se denomina como la gestión del cambio, impulsando el uso de las herramientas como nuevo elemento de trabajo.

Hoy todos los poderes judiciales cuentan, de alguna manera con una especie de expediente digital, en su mayoría elaborado a la medida y los que no van en vía a ello. Hay elementos como las notas (post it) que se podrían incorporar en el expediente para que los funcionarios o jueces pudieran enriquecer el documento con alcances o notas propias de ellos y que posteriormente sirvan como referencias.

Luego de la implementación del expediente digital se hace indispensable extraer la información contenida, de manera ordenada y con alguna lógica que permita hacer gestión, es entonces cuando surge la necesidad de plataformas de inteligencia de negocios, como elemento de gestión, el cual debe ayudar a tomar decisiones, a evaluar comportamientos y levantar alertas y/o tendencias.

Con respecto a la supresión de datos para que no sea manual, debe hacerse a través de plantillas que permitan identificar los datos que son susceptibles o sensibles y que no deben ser publicados.

Se carece de elementos que permitan medir la eficiencia de tener el expediente digital tales como, reducción de tiempos en los procesos, la calidad de la atención de servicios, los procesos deben ser optimizados para luego sistematizarlos.

Debemos adelantarnos entregando soluciones de innovación, este es el gran reto de las TI de las organizaciones.

El área de TI debe ser el socio estratégico de la organización.

Hoy no existe un solo modelo de expediente digital entre todos los países, es recomendable evaluar los elementos indispensables del expediente y poder ver que es lo mínimo que un expediente digital debiera tener, para que exista en todos.

Hoy por hoy si bien los software no pudiesen ser compatibles, lo que se debe revisar es que información es equivalente e intercambiable.

IV. PLATAFORMA TECNOLÓGICA E INNOVACIÓN

La evolución permanente de la tecnología hace que este ámbito sea muy diferente entre el ayer y el hoy y las tendencias van cambiando rápidamente y hoy se plantean nuevas soluciones que ameritan ser evaluadas:

- La plataforma debe ser centralizada, descentralizada o un mix.
- Se debe tener un data center o contratar los servicios de almacenamiento y procesamiento de datos (que hay que considerar para evaluar estas alternativas)
- La nube virtual ¿Qué llevar a la nube? ¿Cómo securizarla?
- Enlaces y Red 4G

Conclusiones:

Los Poderes Judiciales cuentan todos de alguna forma en menor o mayor escala con centros de datos y hoy, de acuerdo a la realidad de cada organización se debe evaluar si seguir adquiriendo maquinas o adquirir servicios de procesamiento de datos.

El concepto de la nube virtual si bien es bastante novedoso, no todos los organismos lo tienen incorporado, pero es claro que la nube debe ser ajustada a las necesidades de la organización y de acuerdo a ella su incorporación, se plantea que inicialmente la nube puede ser un mix transitorio, es decir, ir traspasando servicios a la nube de a poco, hasta alcanzar el estándar que la organización pretende o se a propuesto como meta y para ello se deben evaluar algunos criterios tales como:

1. Revisar el estado de madurez del TI de la organización
2. Revisar qué información es la que se puede y debe subir a la nube, que condiciones debe cumplir en cuanto a peso vs autopista por la que va a transitar.
3. Revisar quién va a tener acceso a la nube
4. Revisar que usabilidad que se le va a dar a la nube

Lo mas recomendable para incursionar es partir con una nube hibrida, es decir, servicios internos y externos en ella.



Con respecto a la plataforma tecnológica hoy por hoy hay tantas alternativas y todas ellas validas, de acuerdo a las características de cada negocio, donde lo más importante es evaluar las necesidades y ver qué solución cubre con mayor cobertura esas necesidades.

Se hace necesario estar evaluando el mercado permanentemente, ya que su cambio es constante y acelerado, lo que hoy puede ser la mejor solución, probablemente mañana ya no lo sea.

Video Conferencia

Fecha: martes 23 de julio 2013

Horario: 9:00 a 10:00 hora Chile

Participantes:

1. Giovanna Pinto, Perú.
2. Rafael Ramirez, Costa Rica.
3. Cesar Arambillete, Uruguay.
4. Julia Centurión, Paraguay.
5. Damián Rosero, Ecuador.
6. Juan José Garcia, México.
7. Roberto Rubín, Bolivia.
8. Víctor Pacheco, El Salvador.
9. Félix Bajandas, Puerto Rico.
10. Mauricio Rodrigo, Chile.
11. Ana María Martínez, Chile

CONCLUSIONES:

I. Interoperabilidad e Integración de Sistemas

a. Alcances

La interoperabilidad es un tema que a todos los participantes les parece importante y por ello se hace necesario pensar en una arquitectura orientada a servicios y con un convenio de colaboración.

b. Compromisos

- i. Cada País informará sobre la situación de cada uno en esta materia, es decir su experiencia en la interconexión con otros países, de contar con convenios enviarlos como referencia para tomarlos como referencia.
- ii. De existir la interoperabilidad Gobierno en el país, enviará las normas gobierno de su país.
- iii. Se trabajará en la elaboración de un manual de interoperabilidad jurisdiccional entre países cumbre.

c. Equipo de Trabajo

País	Representante
Costa Rica	Rafael Ramirez
Puerto Rico	Félix Bajandas
El Salvador	Víctor Pacheco
Chile	Mauricio Rodriguez
Ecuador	Damián Rosero

II. Seguridad Informática

a. Alcance

La seguridad es un hito importante en los servicios informáticos y es por ello que se hace indispensable abordarlo entre los diferentes países a fin de enriquecerse de las experiencias que en este ámbito se han tenido a lo largo del tiempo.

Considerando que la seguridad en cuanto a la seguridad de la información el usuario de esta tiene un papel protagónico.

b. Compromisos

- i. Compartir las experiencias de seguridad de cada país, considerando aquellos eventos en que se han visto vulnerados.
- ii. Establecer un protocolo respecto de la protección de datos, a fin de que estos no se accesen de manera arbitraria y no puedan ser modificados por quien no corresponda.
- iii. Levantar un documento que contenga todas aquellas buenas prácticas que puedan garantizar la alta disponibilidad de la plataforma.
- iv. Firma Electrónica avanzada, evaluar cuál es la postura de cada país, como país, en cuanto al concepto de firma electrónica avanzada, para considerar la implementación de esta en el expediente digital para todos los documentos que se generen en los tribunales.

c. Equipo de Trabajo

País	Representante
Uruguay	Cesar Arambillete
Ecuador	Damián Rosero
México	Juan José Garcia
Bolivia	Roberto Rubín

III. Software

a. Alcance

El expediente digital por el papel protagónico que tiene en este proceso debe ser potenciado para que sea de fácil uso y manejo por los

b. Compromisos

- i. El expediente digital es una herramienta indispensable en el proceso jurisdiccional y se hace indispensable establecer elementos comunes y esenciales como contenido de este de manera transversal en todos los países, con el fin de unificarlos de manera general, por lo tanto se elaborará un documento que defina el expediente y los elementos mínimos que este debe contener.
- ii. Investigar alternativas para mejorar la navegación del expediente digital indicando las ventajas y desventajas que pudiese tener.
- iii. Definir un proceso de almacenamiento de las causas históricas e investigar alternativas tecnológicas que soporten el almacenado histórico.
- iv. Generar un repositorio de herramientas tecnológicas (SW) cuyo contenido sea una especie de librería de componentes utilizables, debidamente documentados, para procesos como las notificaciones, la Firma Electrónica Avanzada, la incompetencia, las interconexiones, entre otros.
- v. Se deberán coordinar con el equipo de trabajo TIUS para considerar los proyectos que allí se vieron.

c. Equipo de Trabajo

País	Representante
Perú	Giovanna Pinto
Paraguay	Julia Centurión
Costa Rica	Rafael Ramirez
Puerto Rico	Félix Bajandas
El Salvador	Víctor Pacheco
Bolivia	Roberto Rubín

IV. Plataforma Tecnológica e Innovación

a. Alcance

En cuanto a la plataforma tecnológica esta amerita ser evaluada constantemente de acuerdo a las tendencias del mercado y a las necesidades de cada una de las instituciones, de acuerdo a la cantidad de usuarios, a la cantidad de información y a la cantidad de transacciones según el tamaño.

b. Compromisos

- i. Elaboración de un documento con políticas y procedimientos que apunten a garantizar una alta disponibilidad en los servicios que se entregan tanto a los usuarios como a la misma comunidad.
- ii. Revisar las tecnologías que puedan ser sustentables en el tiempo para poder garantizar el servicio que se está entregando.

c. Equipo de Trabajo

País	Representante
Ecuador	Damián Rosero
Puerto Rico	Félix Bajandas
Paraguay	Julia Centurión
Chile	Mauricio Rodriguez



Los equipos de trabajo deberán nombrar un coordinador y deberán trabajar para presentar avances en la próxima reunión que se estará realizando el día 6 de agosto del presente.