INSTRUCTIVO (parte IV)

Segunda Reunión Preparatoria

XVII CUMBRE JUDICIAL IBEROAMERICANA

GRUPO DE TRABAJO

Tecnología de los Poderes Judiciales

4 al 6 de diciembre de 2013

Bolivia

PROTOCOLO DE ACTUACIÓN
Sistema Repositorio Único de Información Tecnológica

XVII CUMBRE JUDICIAL IBEROAMERICANA
SANTIAGO - CHILE

ÍNDICE

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: Los funcionários del Poder Judicial autorizados que haga uso del "*Repositorio Único de Información Tecnológica*"

TICs: Tecnologias de la informacion y la comunicaciones

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 y cualquier información adicional en el ámbito de las TICs, con el propósito de mantener un banco de datos de información único de CJI, 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 mediante un usuario y password debidamente autorizado a través de este Repositorio Único en la Url: https://encuestacumbre.pjud.cl/EncuestaCumbreIberoAmericana/index.php

En el caso que un usuario autorizado se desvincule de la institución, esta ser responsable de notificar la novedad a través del sistema repositorio para dar la baja del sistema.

Cada institución determinará que tipo de información será reservada para el grupo técnico y cual de acceso público.

El sistema permite el ingreso por perfiles de usuario: consulta, administrador, expertos.

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.

Artículo 9 - Derecho al tratamiento de la información

Cada Institución es 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 a los

miembros de la mesa de Tecnología de los Poderes Judiciales y una vez aprobado se remitirá copia a la Secretaría Permanente de la CJI.

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:

Formato: Archivos en PDF **Deseable:** PDF con OCR

Observaciones: Los archivos pueden ser subidos en ZIP

Tamaño Máximo permitido por archivo: 10 Mb

No obstante de acuerdo a los cambios de las tecnologías cualquier cambio con objeto de los formatos será estudiado.

El repositorio de información le asignara un Hash al archivo para asegurar su integridad

Artículo 13 – Sobre base de datos de contactos

Para efectos prácticos cada proyecto o experiencia compartida, contendrá la información actualizada 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 de acuerdo a su perfil de usuario:

1) Incluir, modificar o cambiar el estado de la información relativa a su Institución e incluir comentarios.

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) Dar soporte y mantenimiento evolutivo con el fin de mejorar la herramienta para la implementación del SRUIT.

2) Incluir nuevas funcionalidades aprobadas por el Grupo de trabajo de Tecnología.

3) 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.

4) Establecer el vínculo entre el SRUIT y el sitio oficial de la CJI.

5) Administrar las cuentas de las personas o Instituciones usuarias.

6) En caso de que se transfiera la administración y mantenimiento del SRUIT a otra Institución, deberá hacer entrega de los códigos fuentes, programas, documentación, transferencia de conocimiento 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 la Cumbre Judicial Iberoamericana.

Artículo 18 – Proyecto Piloto

Sin perjuicio de la norma permanente anterior, se implementará el proyecto piloto que integre las distintas disposiciones de este documento, a presentar en la Cumbre XVII Judicial Iberoamericana, conforme ha sido acordado por el grupo de trabajo de Tecnología de Poderes Judiciales durante la segunda ronda de talleres en Bogotá-Colombia.

PODER JUDICIAL
REPUBLICA DE CHILE

REPOSITORIO ÚNICO DE INFORMACIÓN TECNOLÓGICA

Manual de Usuario

Santiago, Noviembre de 2013

Tabla de Contenido

Tabla de Ilustraciones

1 Introducción

El sistema ***Repositorio Único de Información Tecnológica*** es un sistema Web, que permite crear y administrador un repositorio consolidado, sobre información relevante a los distintos países participantes de la Cumbre Judicial Iberoamericana XVII, la cual se llevará a cabo el próximo año 2014.

Este sistema permitirá recopilar información, en el ámbito de las tecnologías de la información, referente a las siguientes categorías:

- Equipamiento tecnológico: Esta categoría aborda preguntas al equipamiento tecnológico, esto es tanto en Hardware como Software del encuestado. Además se incorpora información relacionada a la arquitectura física y de sistemas de cada país/federación que responde el cuestionario.

- Sistemas Informáticos: Esta categoría aborda preguntas relativas a los sistemas de información que comprenden o están implementados en cada país/federación encuestada. Es importante considerar que la información consultada establece una diferencia entre sistemas jurisdiccionales y sistemas administrativos, siendo estos últimos aquellos sistemas de apoyo que son transversales a la administración de justicia.

- Servicios: Esta categoría permite consulta en dos grupos, uno Interno y Otro externo, respecto de los servicios que la plataforma informática o los sistemas de información proveen a la administración de justicia en el país/federación encuestado.

- Seguridad: Esta categoría consulta al país/federación encuestado información básica pero muy relevante respecto de los aspectos de seguridad considerados en el establecimiento de su plataforma tecnológica y sistemas de información.

- Organizacional: Esta categoría tiene por objetivo recopilar información respecto de cuál es el rol, posición organizacional y características básicas con la que cuenta la entidad responsable de la plataforma tecnológica y sistemas de información.

- Experiencias: Finalmente este ítem pretender revelar las mejores experiencias observadas en el país/federación encuestado respecto de la implementación de las tecnologías de la información en la Administración de Justicia.

Sin embargo, el sistema ***Repositorio Único de Información Tecnológica*** no es sólo una encuesta o un repositorio de preguntas, sino que tiene por objetivo la administración documental asociada a los ítems que son encuestados, así como también tiene como razón ser un sitio o foro de ideas a ser compartidas en la Cumbre Judicial.

En las siguientes secciones de este manual se describen todas las funcionalidades que entrega el sistema.

2 Manual de Usuario

2.1 Ingreso al Sistema.

A continuación se detallan las opciones relacionadas con el ingreso a la aplicación por parte de un usuario.

2.1.1 Pantalla Principal

http://encuestacumbre.pjud.cl/EncuestaCumbreIberoAmericana

Ilustración 1 Ingreso al Sistema

- Pantalla de Ingreso: En esta pantalla se solicita el usuario y clave proporcionado para ingresar al sistema. Una vez ingresados usuario y clave se presentará el Home o Pantalla de Bienvenida, la cual tiene la siguiente estructura:

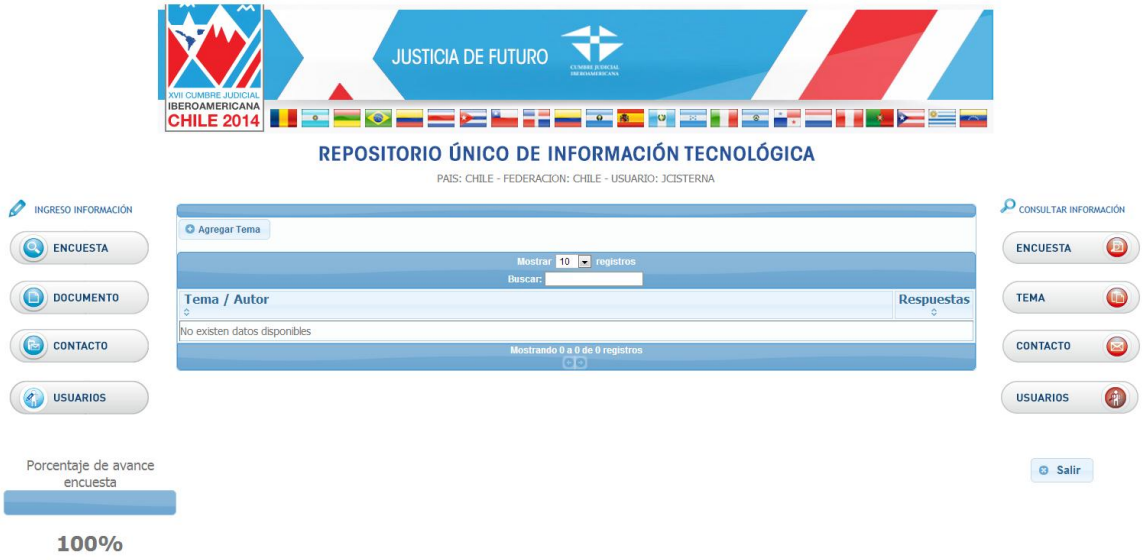


Ilustración 2 Home de Aplicación

Los ítems o funcionalidades disponibles se encuentran separadas por Rol del usuario autenticado, esto es, existen los siguientes roles de aplicación:

- Perfil Administrador Global: permite ingresar documentos y encuestas, crear usuarios y agregar contactos.
- Perfil Administrador País: permite ingresar encuesta y documentos a su País/Federación.
- Perfil Consulta: permite consultar la encuesta ingresada por el administrador de su Federación/País.
- Perfil Documentador: Permite ingresar documentos a su Federación/País.

A continuación se describen las funcionalidades disponibles a través de las distintas opciones del menú.

2.2 Encuesta

La siguiente imagen muestra el botón "Encuesta", el cual está disponible en la sección izquierda del Home, siendo la primera opción que verá cualquier usuario.

Ilustración 3 Menú Encuesta

La opción de Encuesta permite responder la encuesta según las categorías:

- Equipamiento Tecnológico
- Sistemas Informáticos
- Servicios
- Seguridad
- Organizacional
- Experiencias

Al presionar la opción Encuesta se despliega la siguiente pantalla:

Ilustración 4 Pantalla de Ingreso Encuesta

Al seleccionar cualquier de los ítems, se desplegará un listado de preguntas asociadas a él.

Ilustración 5 - Sección de Respuestas

La encuesta puede ser respondida en forma parcial grabando cada pregunta con el botón Guardar.

Cabe destacar, que cada pregunta permite el ingreso de documentación asociada o relacionada al ítem que se está contestando. En la sección 2.3 Documento, se describe como adjuntar documentación.

En la sección izquierda se ve un abanico donde se despliegan las categorías Equipamiento Tecnológico, Sistemas Informáticos, Servicios, Seguridad, Organizacional, Experiencias.

2.3 Documento

La opción documento, visible como segunda opción al costado izquierdo del menú principal, permite asociar documentos en forma general al repositorio. Al presionar el botón Documento (visible en la siguiente figura); se accederá a las funcionalidades descritas a continuación:

Ilustración 6 - Botón Documento

Las funcionalidades del ***Menú Documento***, permiten tanto buscar, como adjuntar documentación global al repositorio.

La pantalla principal del ***Menú Documento*** se muestra en la siguiente imagen:

Ilustración 7 - Menú Documento

La primera sección del menú documento, permite realizar una búsqueda sobre los documentos que el usuario ha subido al repositorio, utilizando los siguientes criterios:

- País.
- Federación (si corresponde).
- Idioma.
- Fecha Documento.
- Título (título del documento).
- Tema
- Sub-Tema
- Autor
- Síntesis

El campo Federación solo aplica para aquellos países que son federados, en los otros países se desplegará un nombre de Federación con el mismo nombre del País.

Una vez realizada la búsqueda, se desplegará una lista de documentos que cumplen los criterios del filtro seleccionado, tal como se aprecia en la siguiente figura:

Ilustración 8 - Búsqueda de Documentos Propios

En la esquina superior derecha, es posible observar un botón son la siguiente descripción “Agregar Nuevo Documento”:

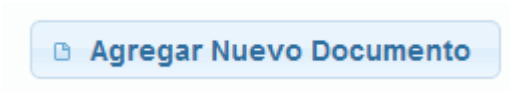


Ilustración 9 - Botón Agregar Nuevo Documento

Al presionar esta opción, se desplegará el siguiente formulario:

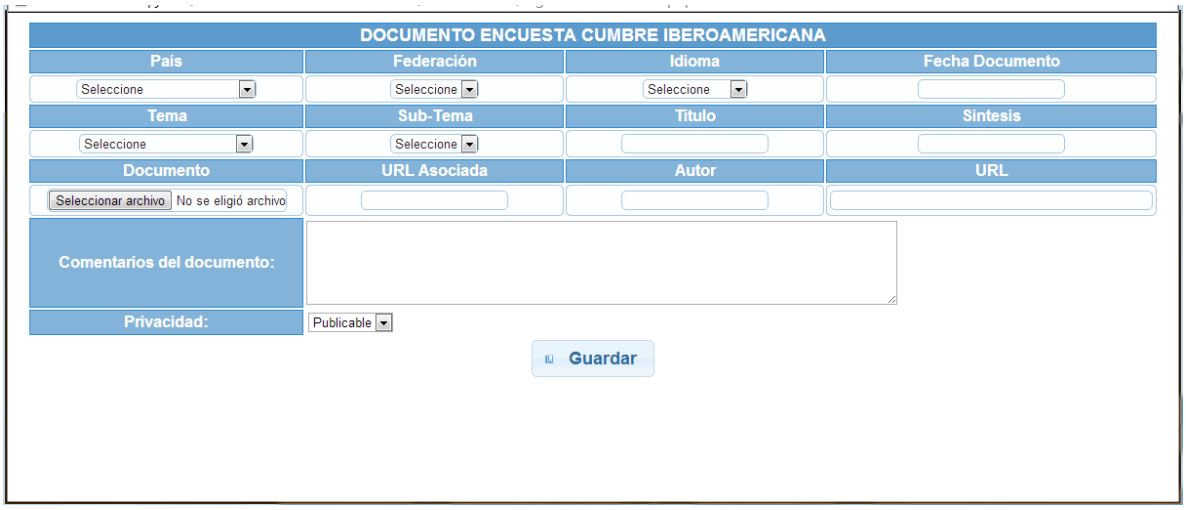


Ilustración 10 - Agregar Nuevo Documento

Esta opción permitirá el ingreso de meta-data asociada al documento y a su vez adjuntar el archivo físico que se quiere subir al **Repositorio de Único de Información Tecnológica.**

2.4 Contacto

Otra funcionalidad que se encuentra disponible en la sección izquierda del Menú, es el administrador de contactos.

Ilustración 11 - Menú Contacto

Al seleccionar esta opción, se desplegará una pantalla como la siguiente:

Ilustración 12 - Administrador de Contactos

El administrador de contactos cuenta también con un menú de ingreso y con un formulario de búsqueda. Éste último permite la búsqueda de contactos por los siguientes criterios:

- Nombres / Apellido Paterno / Apellido Materno / Cargo / País/Federación

Una vez seleccionados los criterios de búsqueda se desplegará una lista resultante como la siguiente:

Ilustración 13 - Buscador de Contactos

Por lo demás, es posible crear contactos mediante la opción “Agregar Nuevo Contacto”:

Ilustración 14 - Botón Agregar Nuevo Contacto

Al seleccionar esta opción, se desplegará un formulario de registro de contacto, como el que se visualiza en la siguiente imagen:

Ilustración 15 - Formulario Nuevo Contacto

2.5 Usuarios

La siguiente funcionalidad disponible en la sección izquierda del menú es la administración de usuarios del sistema. Solo el usuario con el Rol Administrador Global puede acceder a la administración de usuarios. Esta administración permite tanto la búsqueda como registro de nuevos usuarios. Este menú está disponible en el botón que se muestra en la siguiente imagen:

Ilustración 16 - Menú Usuarios

La ventana principal de la administración de usuarios permitirá ver una pantalla como la que se aprecia en la siguiente figura:

Ilustración 17 - Administración de usuarios

El administrador de usuarios permite realizar tanto búsqueda como registro de nuevos usuarios del sistema. El buscador permite búsquedas utilizando los siguientes criterios:

- Username/Nombre/Apellido Paterno/Apellido Materno/ País-Federación

El listado de los usuarios resultantes de una búsqueda se aprecia como en la siguiente imagen:

Ilustración 18 - Buscador de Usuarios

Por otra parte la opción de Agregar Nuevo Usuario, desplegará un formulario como el siguiente:

Ilustración 19 - Formulario Nuevo Usuario

Una vez registrados los nuevos datos y seleccionada la opción Grabar, el usuario quedará registrado en la aplicación.

2.6 Encuesta

La opción o menú Encuesta, corresponde a la primera opción de consulta sobre la información disponible en el **Repositorio Único de Información Tecnológica.** Para acceder a esta funcionalidad se debe utilizar el siguiente botón:

Ilustración 20 - Menú Encuesta Consulta

Esta opción permite la visualización de los resultados de la información registrada en el sistema, tanto en forma individual por País/Federación o en forma global. Al seleccionar Encuesta, se desplegará una ventana como la siguiente:

Ilustración 21 - Resultados Encuesta

La primera sección despliega un listado de los usuarios que han respondido la encuesta y a través de la imagen  , será posible desplegar la encuesta completa con los datos que fueron registrados. Al dar click sobre esta imagen, se desplegará una ventana como la siguiente:

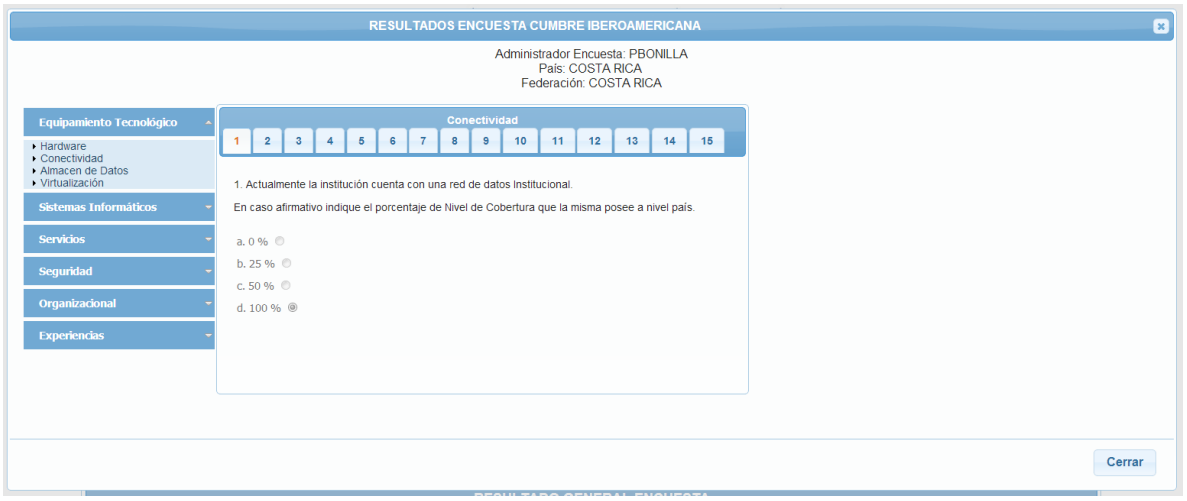


Ilustración 22 - Resultados de Encuesta

Por otra parte, en la parte inferior de la pantalla, se podrá leer el mensaje “Resultado General Encuesta”; este resultado permitirá visualizar gráficos globales con toda la información ingresada al sistema por los distintos Países/Federaciones.

La pantalla de visualización de resultados de encuesta es como la siguiente:

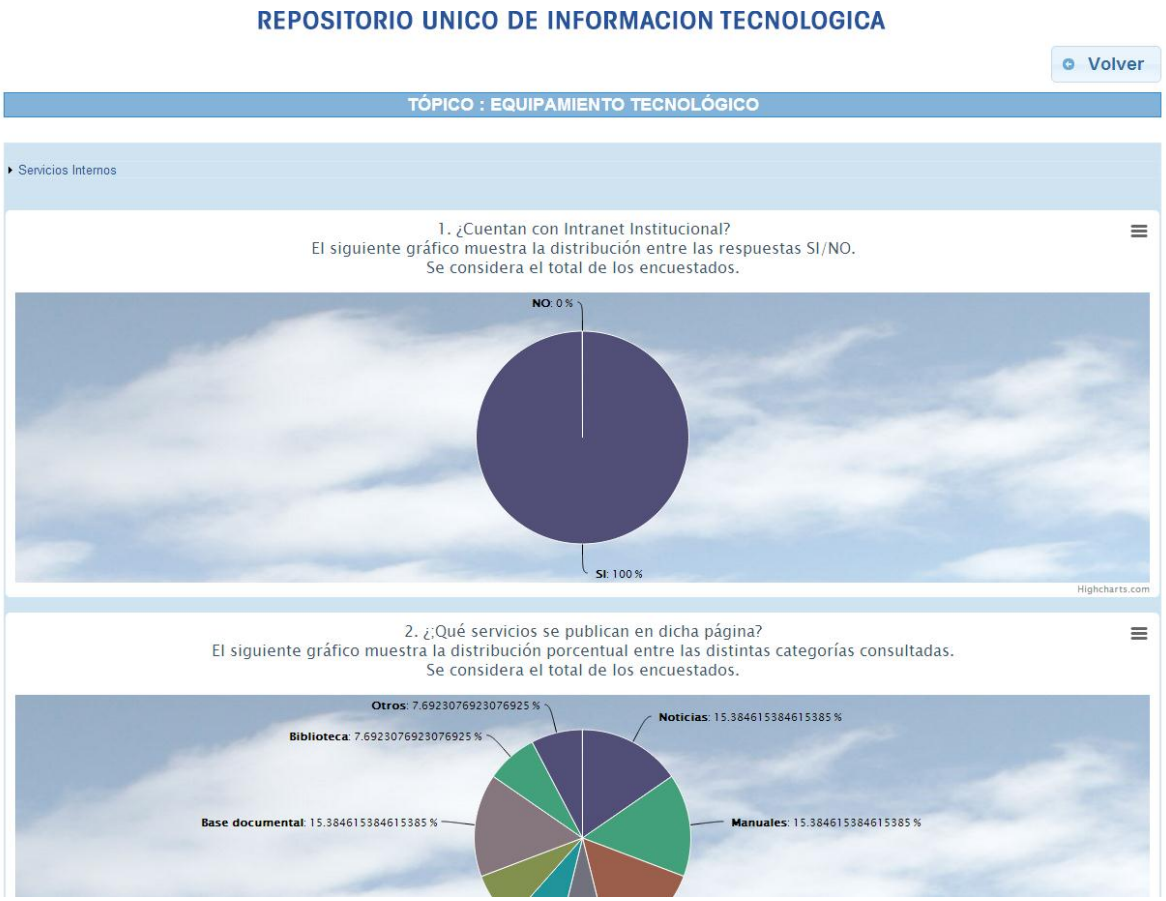


Ilustración 23 - Gráficos Globales Resultado Encuesta

Los gráficos desplegados variarán de acuerdo a la pregunta y sección elegida para su visualización.

2.7 Tema

La siguiente opción tiene relación con una búsqueda o disposición que entrega el **Repositorio Único de Información Tecnológica**, para buscar sobre todos los documentos del repositorio según meta-data ingresada, o bien realizar búsqueda de texto dentro de los documentos.

El menú tema se puede acceder desde el botón:

Ilustración 24 - Menú Tema

Una vez seleccionada la opción tema, se desplegará una pantalla como la siguiente:

Ilustración 25 - Búsqueda Documentos – Tema

La sección superior permite realizar una búsqueda con los criterios o campos ingresados como meta-data al momento en que se adjuntó o se subió un documento al repositorio, ello como parte de los documentos globales o como parte del contexto de una pregunta relacionada al cuestionario.

Al realizar la búsqueda ya sea por meta-data o por palabras dentro del documento, se visualizará un listado resultante como el que se aprecia en la figura:

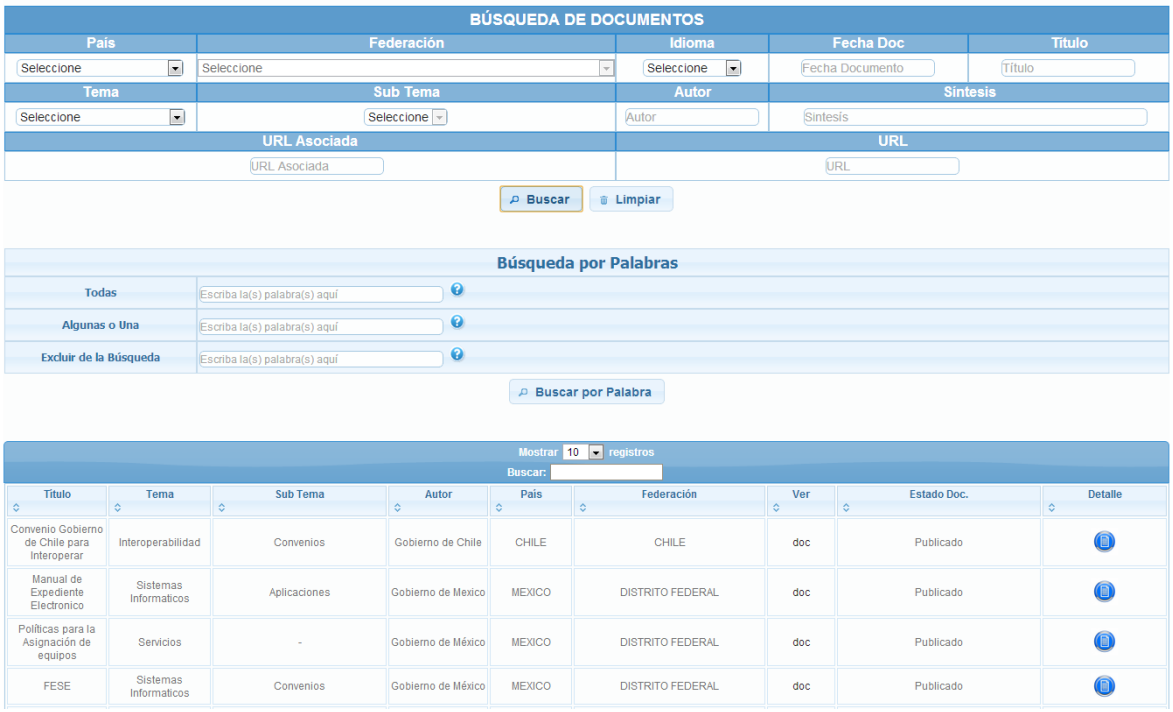


Ilustración 26 - Resultado Búsqueda Documento – Tema

La columna Ver→Doc, permite visualizar/descargar el documento en cuestión, mientras que al pinchar la opción “Detalle”, es posible visualizar toda la meta-data asociada al documento. Esto se aprecia en la siguiente figura:

Ilustración 27 - Meta-data Documento

2.8 Contacto (Propios)

La siguiente opción es la administración de contactos dentro del País/Federación a la que pertenece el usuario. Esto se puede acceder mediante el menú Contacto, identificado con color rojo en la derecha:

Ilustración 28 - Menú Contacto – Propios

Al seleccionar la opción contacto se desplegará un administrador de contactos como el que se aprecia en la figura:

Ilustración 29 - Administrador Contactos – Propios

Este administrador contiene una sección o filtro de búsqueda como también la opción de agregar contactos.

2.9 Usuarios (Propio)

Finalmente en el menú se muestra la opción de Usuario:

Ilustración 30 - Menú Usuario

Esta opción permite la administración de los datos del mismo usuario que se encuentra autenticado en el sistema, mediante un formulario como el que se aprecia en la figura:

Ilustración 31 - Administración Usuario Propio

Con este formulario es posible actualizar los datos propios incluyendo la contraseña.

2.10 TagCloud

Además el sistema cuenta con un TagCloud en los ítems de búsqueda de documentos, esto es se muestra en la pantalla la siguiente figura en la sección superior:

Ilustración 32 – TagCloud

Este TagCloud mostrará el listado de las búsquedas más recurrentes sobre los documentos del **Repositorio Único de Información Tecnológica** y además al presionar sobre la palabra destacada, realizará la búsqueda de documentos utilizando esos criterios.

Sistema Repositorio Único de Información Tecnológica – Mapa Tecnológico Cumbre Judicial Iberoamericana

En la XVI Cumbre Judicial Iberoamericana, el grupo denominado "*Brecha Tecnológica en la Justicia*", trabajó en la definición de indicadores, que permitieran determinar el grado de desarrollo de las tecnologías de información en el sector justicia. En esa edición se presentó y aprobó el documento denominado "*Matriz de Levantamiento de Información Poderes Judiciales*", en el cual se identificaron los grupos y variables que desde la óptica de los expertos en informática judicial, permitirían la generación del mapa de desarrollo tecnológico en la región.

Además, se trabajó en el desarrollo de un programa, para almacenar aquellas experiencias en materia de tecnología que los Poderes Judiciales quisieran compartir, de forma tal que fuese un insumo accesible para todos, donde a partir de la experiencia positiva o negativa vivida por otros países en el impulso de sus proyectos, pudiera servir como base para la generación de nuevas propuestas, llegando incluso a compartir herramientas ya desarrolladas.

Durante esa edición la Asamblea Plenaria señaló la necesidad de unificar esfuerzos en el seno de la Cumbre Judicial, por lo que se sugirió que el "*Mapa Tecnológico*" se integrara a la información contenida en el PLIEJ.

Es a partir de lo anterior que para la XVII Edición, se integró dentro del marco del proyecto de *"Tecnologías para los Poderes Judiciales"*, un subgrupo que continuara trabajando en esas iniciativas.

Como una primera actividad se ajustó con el nuevo equipo la "*Matriz de Levantamiento de Información Poderes Judiciales*". Una vez definido este punto, el Poder Judicial de Chile, desarrolló una aplicación web que facilitara la recolección de los datos de la matriz en modelo tipo encuesta, para a partir de ello se pueda generar el mapa de datos que

será remitido al PLIEJ para su valoración e integración dentro del programa por ellos desarrollado. Además, dicha herramienta permitirá el almacenamiento de documentos y experiencias tecnológicas que podrán ser consultados por otros Poderes Judiciales.

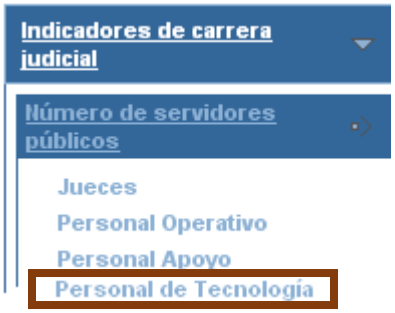
Dentro de la dinámica realizada, y a modo de prueba, se incluyeron los datos de Argentina, Chile, Costa Rica, Ecuador, España, Nicaragua y México.

A partir de los datos recolectados las personas usuarias del sistema podrán obtener información de forma específica por país, o bien, de forma global.

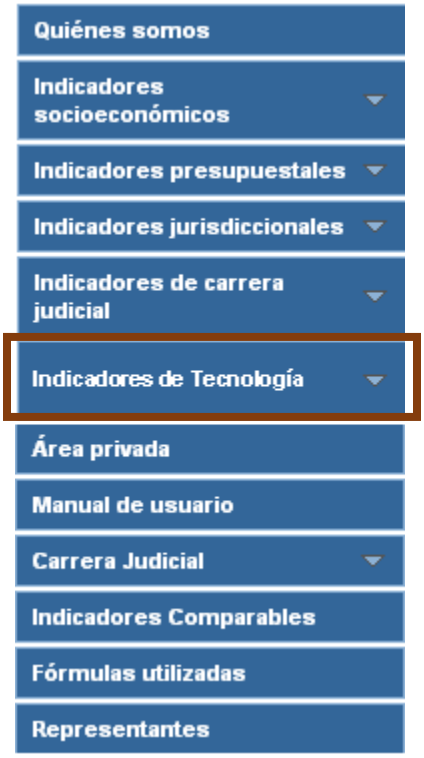
A continuación se muestra el desglose de los resultados, con algunas sugerencias de cómo podrían ser mostrados los datos dentro del PLIEJ.

1. **En el apartado de "Indicadores presupuestales", se recomienda incluir Presupuesto de Tecnología.**

2. **En el apartado de " *Indicadores de Carrera Judicial*", dentro de "Número de Servidores Públicos", incluir la cantidad de "*Personal en Tecnología*"**



3. **Incluir una nueva pestaña denominada "Indicadores de Tecnología" , donde se sugiere la siguiente distribución:**



1. **Equipamiento Tecnológico**
   - Hardware
   - Virtualización
   - Conectividad
   - Almacenamiento de Datos
2. **Sistemas Informáticos**
   - Sistemas Judiciales
   - Sistemas Jurisprudenciales
   - Sistemas Administrativos
   - Sistemas de Archivo Judicial para Expedientes Electrónicos y Audiencias Orales
3. **Servicios**
   - Servicios Internos
   - Servicios Externos
4. **Seguridad Informática**
5. **Organizacional**

Los datos correspondientes a los indicadores anteriores, se encuentran almacenados en el *"Sistema Repositorio Único de Información Tecnológica".*

La dinámica para la recolección de esta información se realizará a través de un usuario y clave que se le entregará a cada país para que proceda a complementar la información.

Con los datos obtenidos, se recomienda que sean los especialistas del PLIEJ, quienes dispongan la mejor forma de presentar esta información.

Recomendaciones

1. Es importante tener presente que la tecnología evoluciona constantemente, por lo tanto, los indicadores deben ser revisados y actualizados al menos cada dos años, para incluir las nuevas tendencias tecnológicas en la Administración de Justicia y excluir aquellas que ya se consideran fueron superadas.

   Para ello se recomienda que a través del grupo de e-Justicia, Hijo de Cumbre Judicial, se establezca un grupo permanente de trabajo que continúe trabajando en la actualización de esta matriz de datos, así como en los otros proyectos tecnológicos que se gestionen en el ámbito de Cumbre Judicial.

2. Motivar a los países miembros de la Cumbre Judicial para que en una primera instancia incluyan la información correspondiente a cada Institución. Entre mayor cantidad de países participantes, se tiene información precisa de las tendencias en esta materia en la Administración de Justicia.

   De igual forma una vez que incluyan los datos, se debe concientizar en la importancia de mantener dicha información actualizada, por cuanto los datos allí contenidos podrán resultar un insumo valioso para la toma de decisiones de los Poderes Judiciales.

Para ello es necesario contar con un punto de contacto, encargado y responsable de los datos por cada país.

3. Se recomienda potenciar y fortalecer el sistema, en lo que respecta a la información que se ha recopilado relativa a normas, políticas, sistemas, experiencias, etc. De forma tal que sea una herramienta dinámica, que sirva de insumo para el desarrollo de proyectos tecnológicos en la región Iberoamericana.

La información del punto de contacto, o cualquier sugerencia y/o recomendación respecto a la herramienta o el proyecto, pueden realizarla a través de (anotar acá la persona o correo contacto)

A continuación se muestra los resultados obtenidos en la dinámica realizada con los siete países señalados.

RESULTADOS

1. Equipo Tecnológico

Son todos aquellos componentes que hacen posible el funcionamiento de los sistemas informáticos. Se han dividido en cuatro grupos: a) Hardware, b) Virtualización, c) Conectividad y d) Almacenamiento de datos.

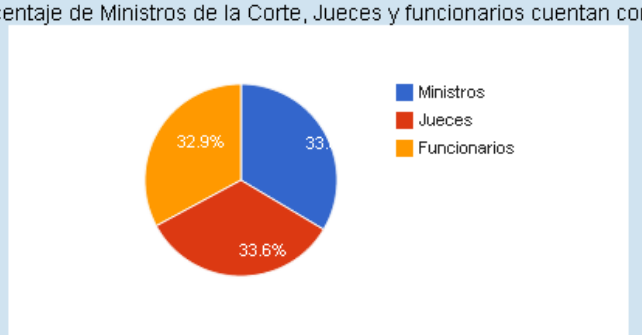
El hardware se refiere a aquellos componentes físicos que hacen posible el funcionamiento de los sistemas informáticos, tal como, computadoras, portátiles, equipos servidores, etc. Es lo que comúnmente se conoce como "*equipos informáticos*".

Mediante la tecnología de la "virtualización" es posible aprovechar la capacidad y potencia de los equipos actuales. A través de programas informáticos (software), se puede dividir los recursos del equipo servidor o bien de una computadora, creando en una sola máquina, distintas máquinas virtuales. En un equipo físico se pueden crear de forma virtual dos o más equipos, los cuales funcionan de manera independiente aunque no existan físicamente.

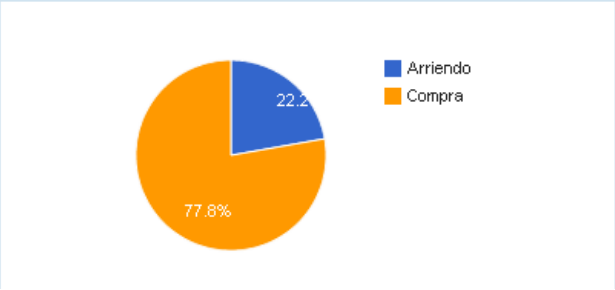
En "Conectividad" se analizan temas relativos a las redes de datos, Internet y Videoconferencia. Y en "Almacenamiento de Datos" se valoran aspectos sobre formas de almacenamiento para darle continuidad al servicio.

Hardware

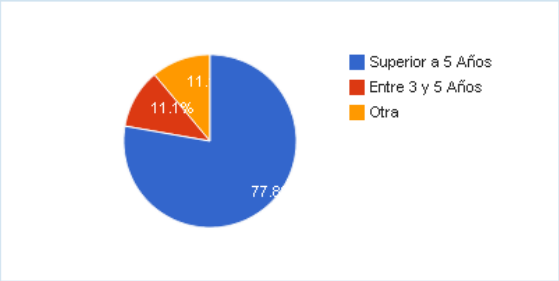
Pregunta: 1.¿Qué Porcentaje de Ministros de la Corte, Jueces y funcionarios cuentan con equipos informáticos?



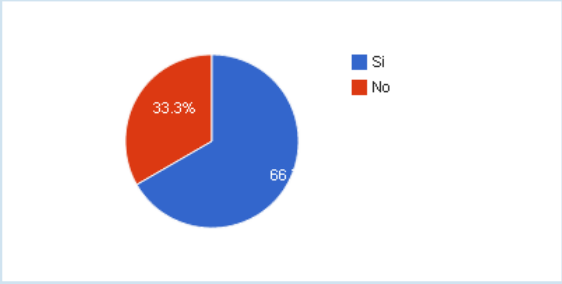
Pregunta: 2.¿Qué modalidad utiliza para proveer el equipamiento computacional para los funcionarios?



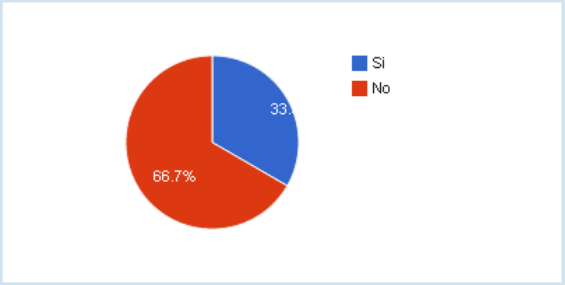
Pregunta: 3.¿Qué nivel de obsolescencia le asigna al equipamiento computacional?



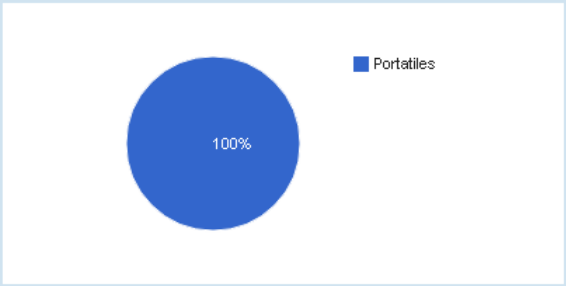
Pregunta: 4.¿Cuenta con políticas de respaldo a nivel institucional para la información que manejan directamente en sus equipos los jueces y funcionarios?



Pregunta: 5.¿Posee políticas y/o procedimientos para el reemplazo del equipamiento y su término de vida útil? En caso afirmativo, señalar cuáles.

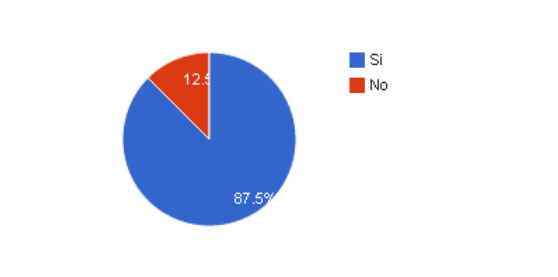


Pregunta: 6.¿Qué porcentaje del equipamiento representan los equipos portátiles?

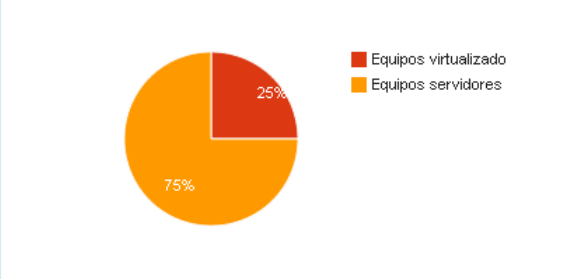


Virtualización

Pregunta: 1. ¿Cuenta con herramientas de virtualización dentro de la plataforma tecnológica?



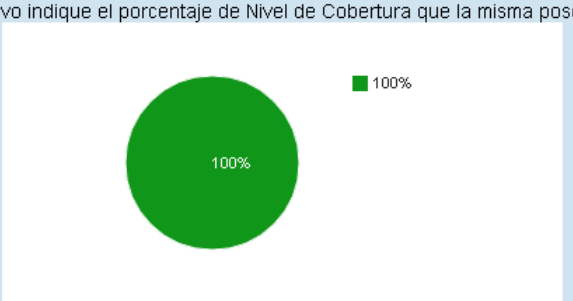
Pregunta: 2. ¿Que tiene virtualizado y en qué proporción?



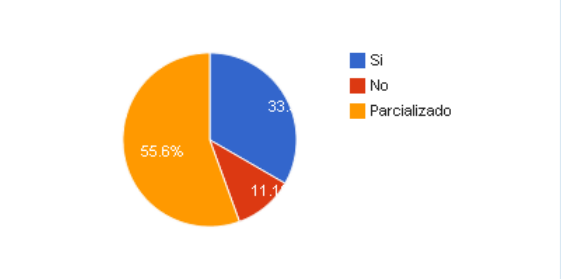
Pregunta: 3. ¿Posee políticas de Virtualización y Consolidación, respaldo y alta disponibilidad del equipamiento tecnológico virtualizado?

Conectividad

Pregunta: 1. Actualmente la institución cuenta con una red de datos Institucional.
En caso afirmativo indique el porcentaje de Nivel de Cobertura que la misma posee a nivel país.

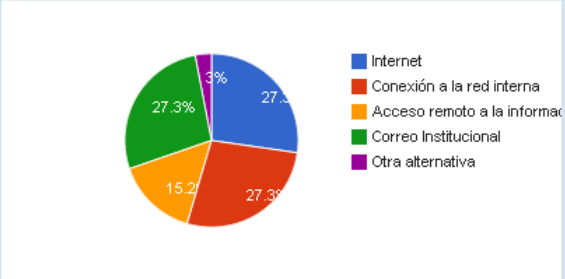


Pregunta: 2. Disponen de conexión a Internet para todos los funcionarios de la Institución

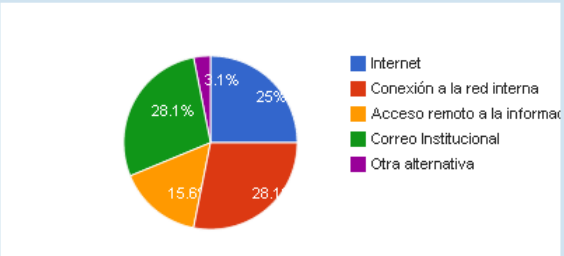


Pregunta: 3.¿Qué herramientas de conectividad se brindan a los Ministros de Corte, jueces y funcionarios?

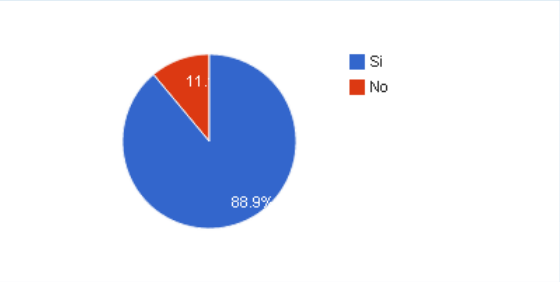
MINISTROS DE CORTE /JUECES



FUNCIONARIOS

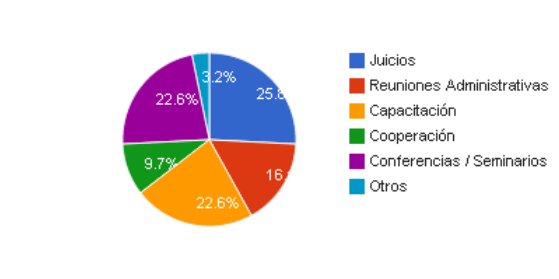


Pregunta: 4.¿Posee políticas y/o procedimientos para normar los accesos señalados?

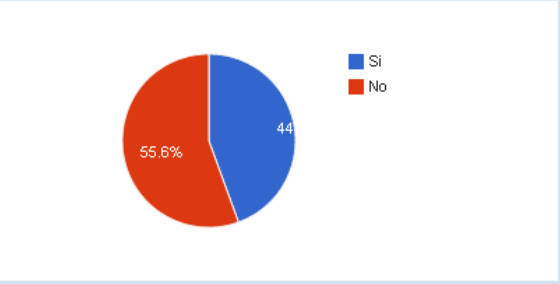


Pregunta: 5.¿Cuenta con una plataforma de videoconferencia en la Institución?

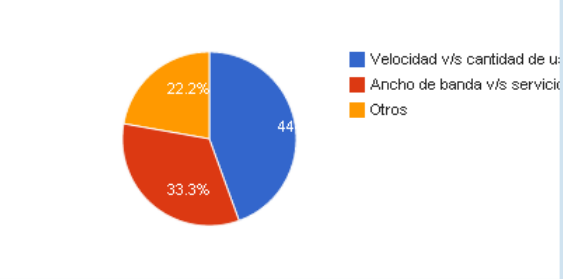
Pregunta: 6.¿Para qué tipo de actividades y con qué cobertura se utiliza la plataforma?



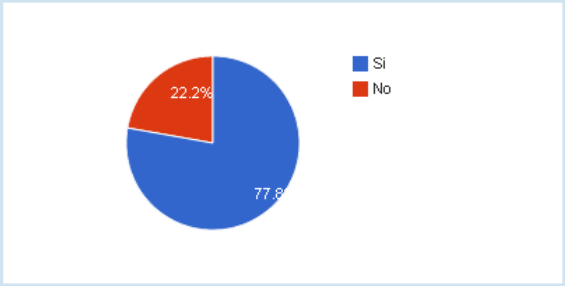
Pregunta: 7.¿Posee protocolos de operación para los procesos judiciales frente a fallas en los enlaces de comunicación?



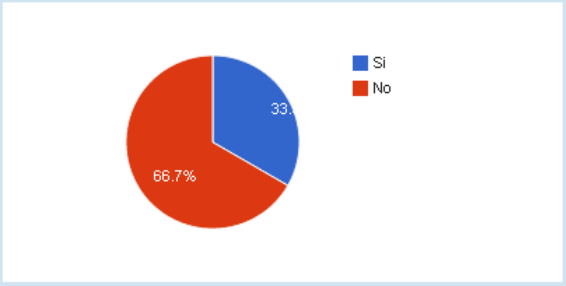
Pregunta: 8.¿Los anchos de bandas asignados a los tribunales obedecen a algún tipo de criterio o política?



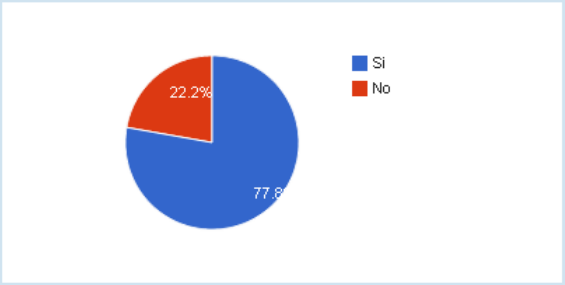
Pregunta: 9.¿Dispone la red de enlaces de respaldo o contingencia en caso de falla del principal?



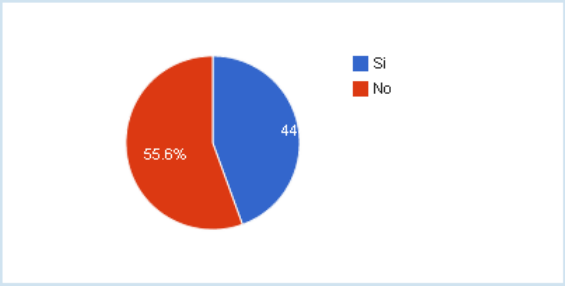
Pregunta: 10.¿Dispone de medidas de contingencia en caso de fallas del enlace principal y respaldo?



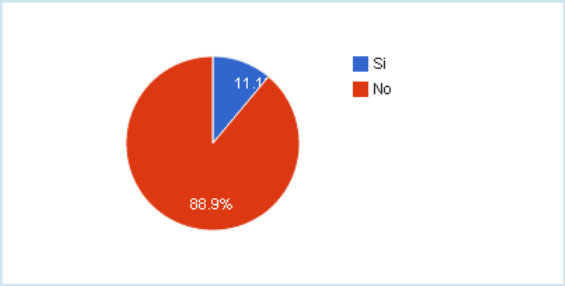
Pregunta: 11.¿Dispone de algún Software de monitoreo de enlaces de comunicaciones que permita alertar eventos y analizar el trafico dentro de los enlaces? En caso afirmativo, adjunte documento.



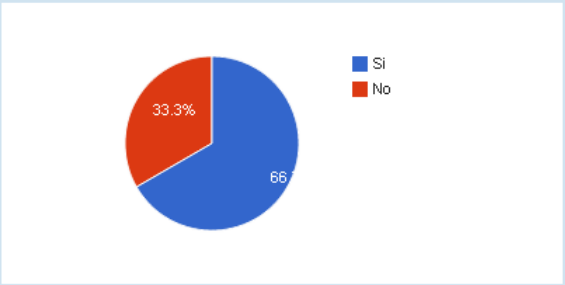
Pregunta: 12.¿Posee actualmente herramientas de optimización de anchos de banda?



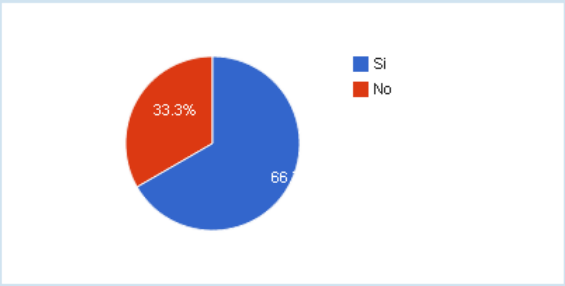
Pregunta: 13.¿Tiene algún estándar de seguridad y certificaciones en el tema de conectividad?



Pregunta: 14.¿Cuenta con políticas de confidencialidad respecto al tráfico de información?



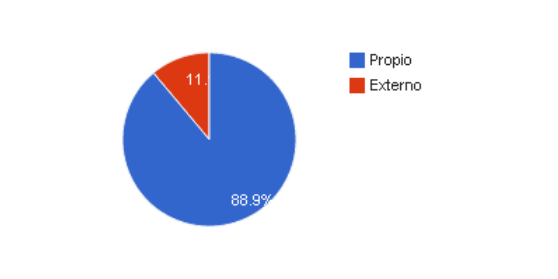
Pregunta: 15.¿Cuenta con herramientas de encriptación de datos?



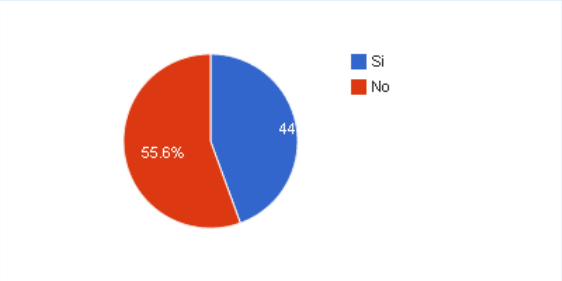
Almacenamiento de Datos

Pregunta: 1. ¿Cuenta la Institución con Data Center?

Pregunta: 2. Dicho centro de procesamiento de datos es:



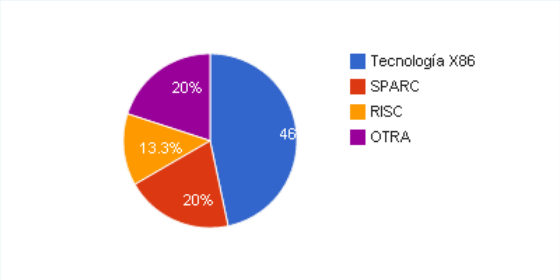
Pregunta: 3. ¿Cuenta actualmente la Institución con un centro de procesamiento de datos alternativo? En caso afirmativo, señalar que servicios posee replicado.



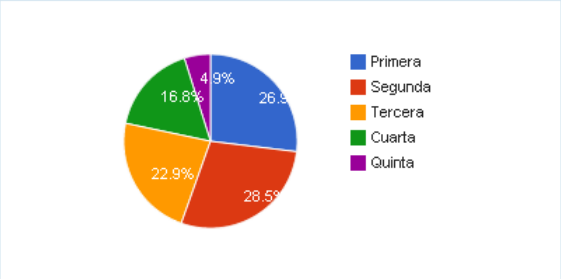
Pregunta: 4. ¿Utiliza motor de base de datos?

Indique si es:

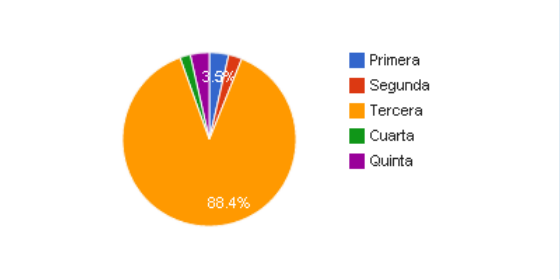
Pregunta: 5. ¿Qué tipo de tecnología de procesamiento utiliza para las bases de datos?



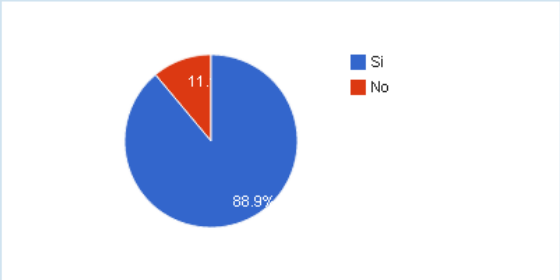
Pregunta: 6. Señale el tamaño de gigabytes y descripción de cada una de las 5 bases de datos principales que gestiona



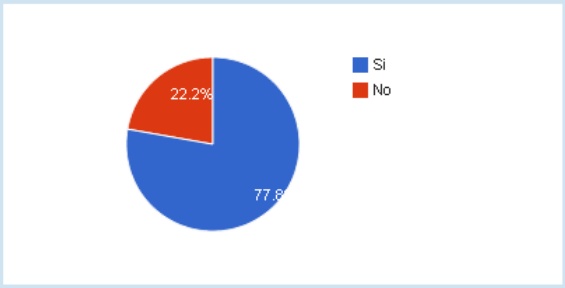
Pregunta: 7. Señale la cantidad de usuarios por cada una de las 5 bases de datos señaladas en el punto anterior



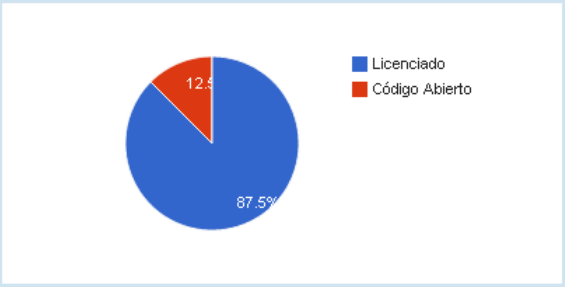
Pregunta: 8. ¿Posee normativas o procedimientos referentes a las políticas de administración y roles de la administración de las bases de datos?



Pregunta: 9. ¿Posee normativas o procedimientos para respaldo, su periodicidad y vigencia de datos almacenados en bases de datos?



Pregunta: 10. ¿Dispone de herramientas de software para monitorear el rendimiento del motor de bases de datos?



2. Sistemas

Cuando se habla de sistemas de información se está ante un conjunto organizado de elementos, quienes interactúan entre sí para procesar información.

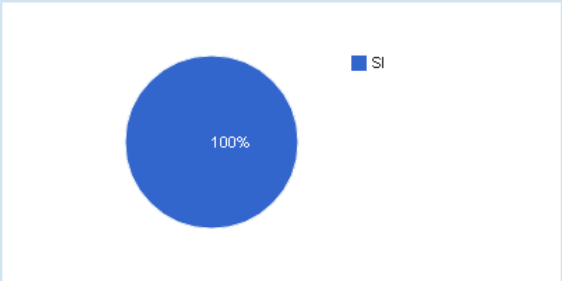
En el caso de la Administración de Justicia se han desarrollado una serie de sistemas que han facilitado y mejorado la interacción con la población ciudadana.

Durante más de una década el auge de este tipo de sistemas ha ido en constante evolución, en una primera instancia se inicio con sistemas que permitieran almacenar la información básica de las causas judiciales, sin embargo estos mismos sistemas fueron creciendo en funcionalidades que facilitan y agilizan la tramitación procesal.

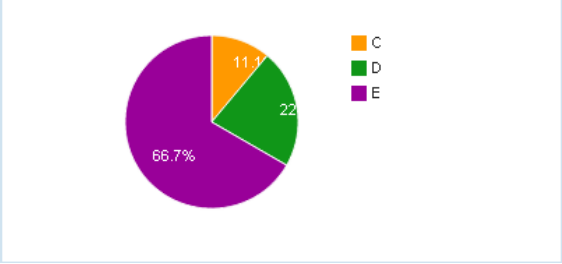
Este título se dividió en: a) Sistemas Informáticos, b) Sistemas Jurisprudenciales, c) Sistemas Administrativos y d) Sistemas de Archivo Judicial para Expedientes Electrónicos y Audiencias Orales.

SISTEMAS INFORMÁTICOS

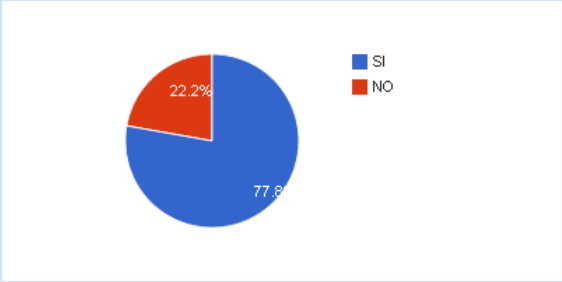
Pregunta: 1.¿Cuenta la Institución con sistemas informáticos para el Registro, Control, Gestión y/o tramitación de causas?



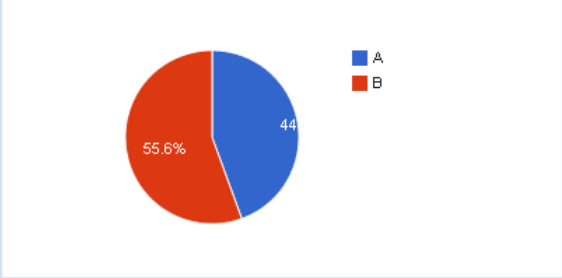
Pregunta: 2.¿Qué porcentaje del total de tribunales utiliza sistemas informáticos para la tramitación de causas?



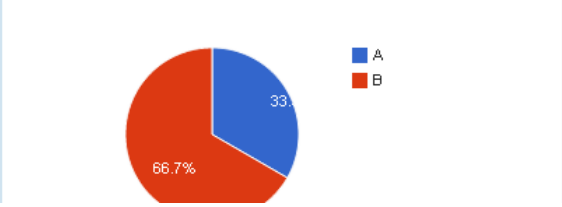
Pregunta: 3.¿Se utilizan sistemas informáticos para la tramitación íntegra de las causas como un mecanismo de respaldo, seguimiento y/o apoyo a la tramitación en papel?



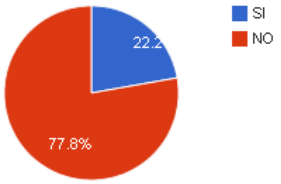
Pregunta: 4.Describa cómo es la relación actual entre ambas formas de registro (digital y papel)



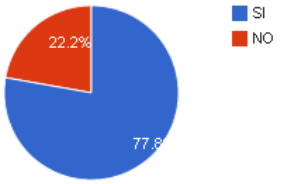
Pregunta: 5.¿La tramitación electrónica o expediente electrónico es optativo u obligatorio?



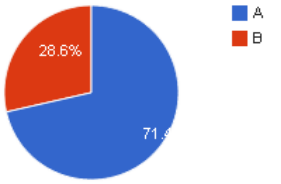
Pregunta: 6.¿Se utiliza la firma electrónica en las resoluciones de los expedientes electrónicos?



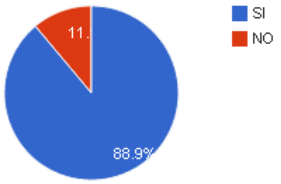
Pregunta: 7.¿Se encuentra estandarizado el formato de documentos digitales que se utilizan dentro de la organización?



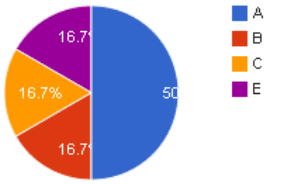
Pregunta: 8.¿Qué tipo de firma se utiliza?



Pregunta: 9.¿Cuenta la Institución con registro de audio de audiencias u otros trámites?

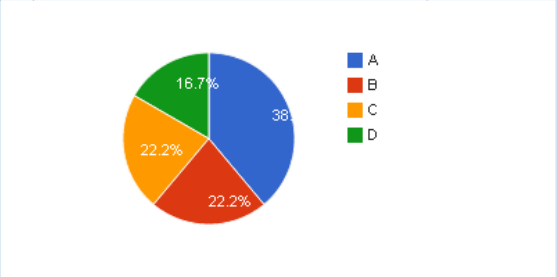


Pregunta: 10.¿Cuál es el porcentaje de implementación en la Institución del expediente electrónico?

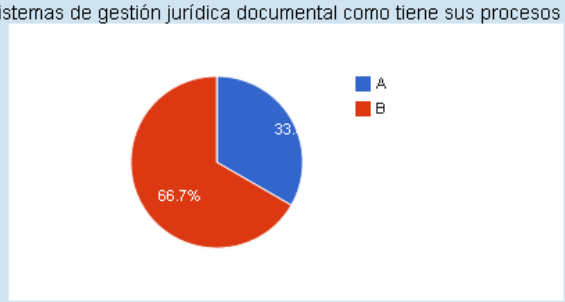


SISTEMAS JURISPRUDENCIALES

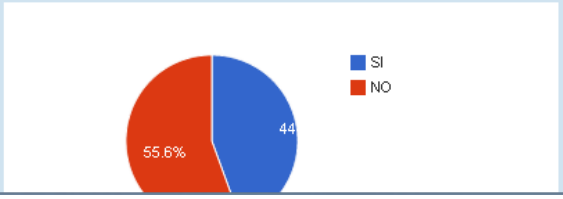
Pregunta: 1. ¿Dispone la Institución con sistemas informáticos para la Gestión Documental?.



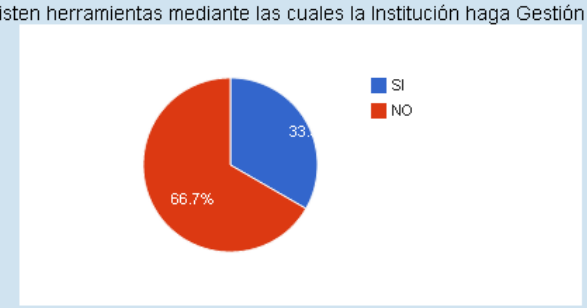
Pregunta: 2. ¿Los sistemas de gestión jurídica documental como tiene sus procesos de registro y gestión?



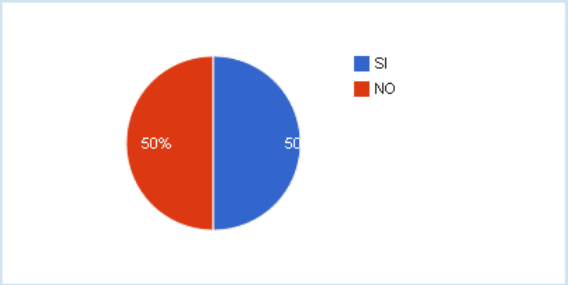
Pregunta: 3.¿Los sistemas de gestión jurídica documental están integrados con los sistemas de gestión de causas?



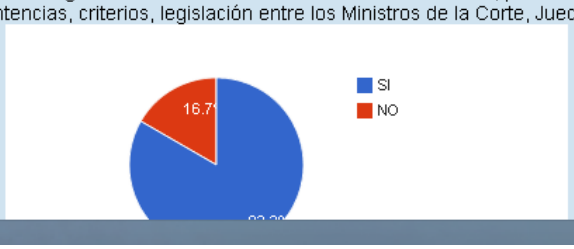
Pregunta: 4.¿Existen herramientas mediante las cuales la Institución haga Gestión del Conocimiento?



Pregunta: 5.¿Existen sistemas de información de Tesauro Jurídico vinculados a los sistemas de Gestión Jurídica Documental?

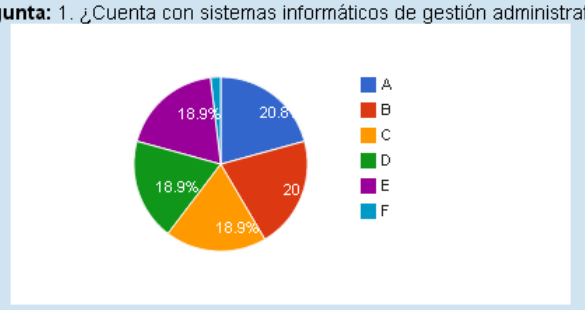


Pregunta: 6.¿Dispone la Institución algún buscador electrónico de información interna, particularmente para el conocimiento e intercambio de sentencias, criterios, legislación entre los Ministros de la Corte, Jueces y funcionarios?



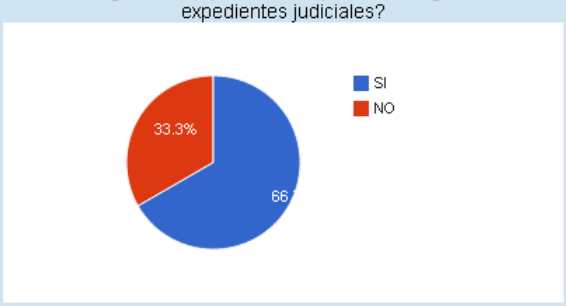
SISTEMAS ADMINISTRATIVOS

Pregunta: 1. ¿Cuenta con sistemas informáticos de gestión administrativa?



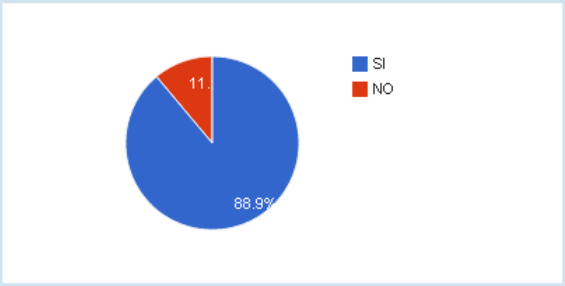
SISTEMAS DE ARCHIVO JUDICIAL PARA EXPEDIENTES ELECTRÓNICOS Y AUDIENCIAS ORALES

Pregunta: 1. ¿Existe en la Institución un organismo especializado que se encargue de la función de archivar y resguardar los expedientes judiciales?



Pregunta: 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?

Pregunta: 3. ¿De qué forma se están archivando las audiencias orales grabadas tanto para procesos activos como para procesos terminados?

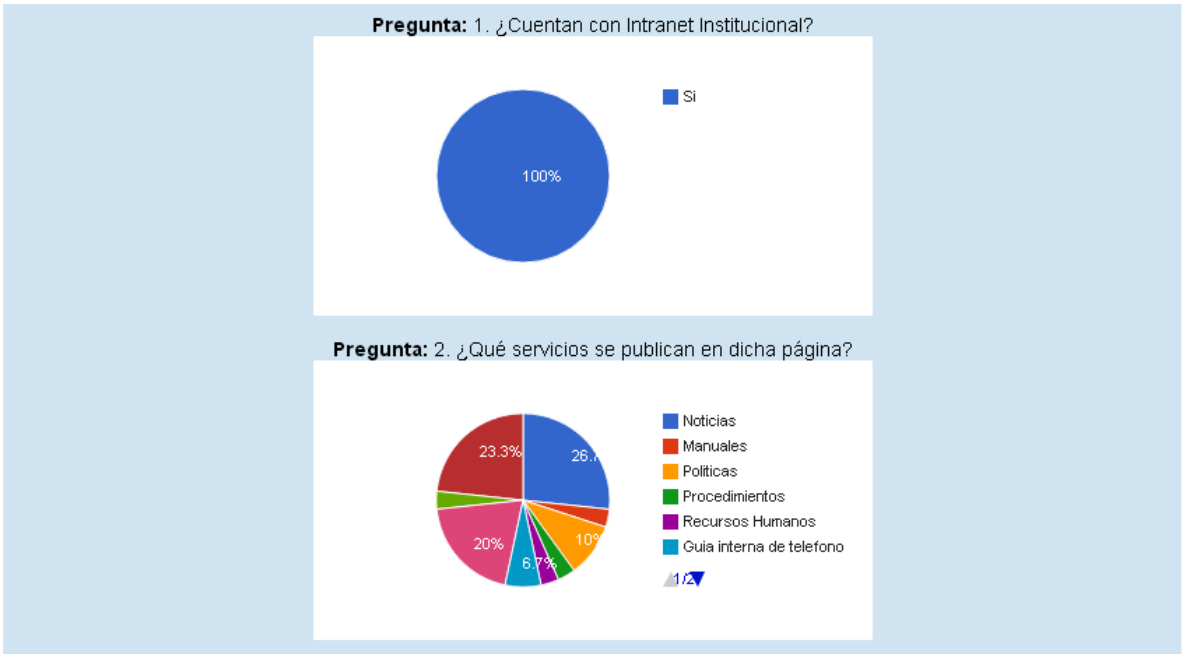


Pregunta: 4. ¿Qué alternativas de acceso tienen actualmente los usuarios al momento de querer consultar un expediente digital de una causa terminada, o bien un audio y/o video de una grabación de una audiencia oral?

3. Servicios electrónicos

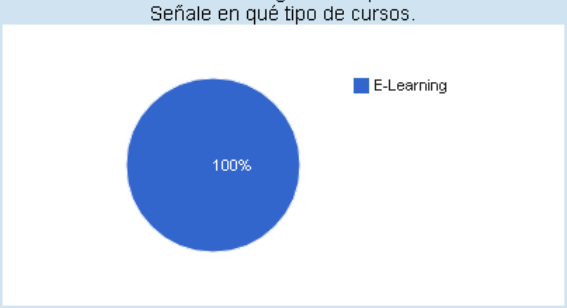
Ofrecen a las personas usuarias la posibilidad de acceder a los servicios que brindan las Instituciones de forma electrónica. Se dividen en dos categorías: a) Servicios Internos a través de la Intranet y b) Servicios Externos a través de Internet.

SERVICIOS INTERNOS



Pregunta: 3. ¿Qué metodologías de capacitación está utilizando la Institución en la actualidad?

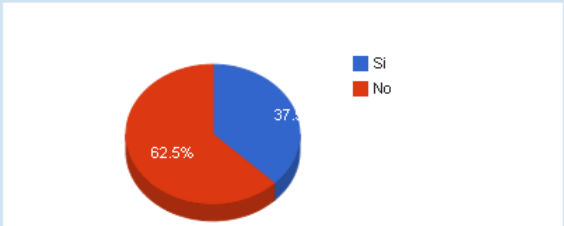
Pregunta: 4. ¿La Institución hace uso de metodologías de capacitación como E-Learning o B-Learning? Señale en qué tipo de cursos.



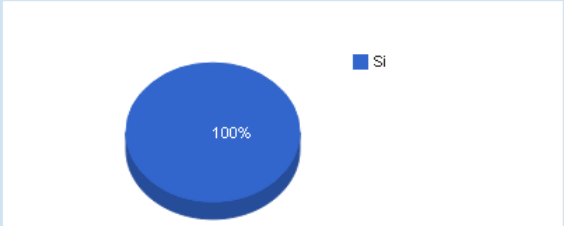
SERVICIOS EXTERNOS

Pregunta: 1. ¿Los usuarios pueden consultar el estado de las causas que se encuentran en tramitación en línea?

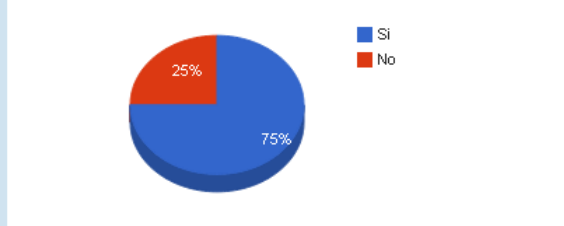
Pregunta: 2. ¿Existen mecanismos de tramitación en línea a través de los cuales los usuarios puedan realizar presentaciones a los tribunales directamente utilizando Internet?



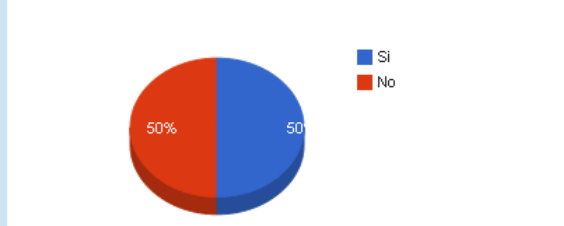
Pregunta: 3. ¿Se han implementado mecanismos de notificación alternativos, como correo electrónico o mensajería de texto?



Pregunta: 4. ¿Existen interconexiones con otros organismos o instituciones, que permitan el intercambio de información que disminuyan la cantidad de trámites al ciudadano o agilicen los procesos?



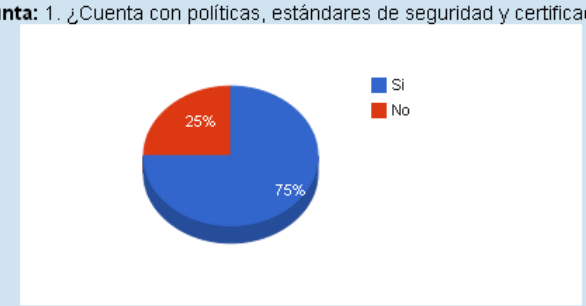
Pregunta: 5. ¿Se hace uso de redes sociales para brindar información y promover el acercamiento con los usuarios? Señale cuáles son esas experiencias



4. Seguridad Informática

La seguridad informática se encarga de proteger la plataforma tecnológica, principalmente la integridad y privacidad de la información almacenada en los sistemas informáticos. Para ello se han definido una serie de estándares y políticas que permiten minimizar el riesgo.

Pregunta: 1. ¿Cuenta con políticas, estándares de seguridad y certificaciones?

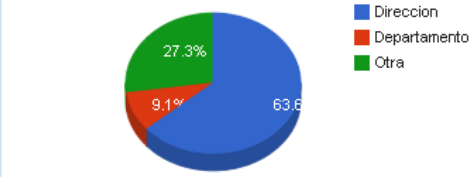


Pregunta: 2. ¿Cuenta con procedimientos estandarizados referente al resguardo y seguridad de la plataforma tecnológica? (servidores, equipos de almacenamiento y de comunicación).

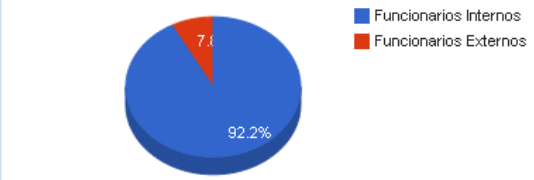
5. Organizacional

En la parte organizacional, se pretende conocer detalles relacionados con la estructura organizacional y de planificación del área de tecnología de cada Institución.

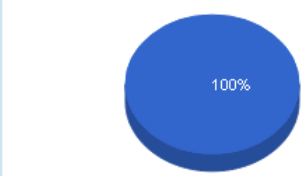
Pregunta: 1. ¿Cuál es el nivel en la estructura organizacional que ocupa el área de tecnología?



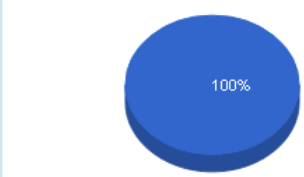
Pregunta: 2. ¿Cuántas personas en total laboran en el área de tecnología?



Pregunta: 3. ¿Cuentan con presupuesto específico para las TICS?



Pregunta: 4. ¿Cuenta con Plan Estratégico de Tecnologías de Información?



MODELO EXPEDIENTE ELECTRÓNICO IBEROAMERICANO

(Dr. Francisco Boada, Dr. Cesar Chaparro, Ingeniera Paola Alzate, Ingeniero Luis Eduardo Yepes)

PROPÓSITO:

El propósito del modelo de expediente electrónico Iberoamericano es brindar herramientas que permitan avanzar de manera estandarizada y planificada en la implementación y/o puesta en producción del expediente electrónico de los poderes judiciales. El modelo propone inicialmente identificar en qué fase se encuentra cada uno de los países miembros a efectos de lograr aportes de experiencia y conocimiento de los modelos implementados a la fecha, posteriormente, trazar un plan de trabajo común interoperacional que permita a todos y cada uno de los miembros alcanzar gradualmente la siguiente fase con eficiencia implicando la interoperabilidad y consulta entre los sistemas de información de los poderes judiciales iberoamericanos. Adicionalmente el modelo proporciona las lecciones aprendidas y referencias en cada uno de los componentes identificados con el fin de tener un referente que facilite el trabajo colaborativo entre los países miembro de la cumbre iberoamericana.

DEFINICIONES:

Documento Digital: Es todo objeto digital, documentos, graficas, fotos, audios, videos que posteriormente se permita su incorporación al sistema de información y asociarlo a una causa o proceso judicial con la posibilidad de consultarlo con posterioridad.

Carpeta Digital: se define como el conjunto de documentos digitales organizados cronológicamente, asociados a un procedimiento judicial.

Litigió en Línea o Expediente Electrónico: Es el uso de herramientas tecnológicas que permitan un diálogo seguro, eficaz, confiable del despacho judicial con los sujetos procesales a través de medios electrónicos e implica la actualización inmediata del sistema de información judicial con las intervenciones en línea de las partes y la consulta confidencial del estado del proceso y sus documentos digitales por parte de los actores que la ley permita.

Subpracticas: son prácticas que pueden llevar al logro de los productos esperados

GUÍA DEL MODELO:

El modelo plantea la división de las tareas en tres (3) categorías:

C.1. Ingreso
C.2. Tramite
C.3. Terminación

Y seis (6) componentes trasversales:

T.1. Manejo Documental
T.2. Seguridad
T.3. Procesos de apoyo
T.4. Talento Humano
T.5. Infraestructura
T.6. Marco Normativo

NOTAS INTRODUCTORIAS:

La aplicación del modelo Expediente Electrónico Iberoamericano implica para los países iberoamericanos:

- Evaluar anualmente el estado del país utilizando las fases y componentes establecidos en el modelo para cada área de trabajo.
- Identificar las alternativas que permitirán guiar hacia el avance.
- Retroalimentar el modelo de Expediente electrónico iberoamericano con los avances obtenidos por cada país: Tanto en las lecciones aprendidas, como en la estructura del modelo.

MODELO FUNCIONAL PARA LA IMPLEMENTACIÓN DEL MODELO:

C.1 CATEGORÍA INGRESO

Propósito:

Abarca la recepción de las causas y/o actuaciones asociadas con un trámite judicial, realizadas por los ciudadanos, participantes o sujetos procesales con el fin de proponer, aclarar, responder y allegar información a un despacho judicial.

FASE	ALCANCE
FASE CERO O INICIAL	Se presentan las actuaciones de manera escrita.
FASE 1	Se presentan las actuaciones de manera escrita y escaneada como un documento digital anexo (CD, DVD, Memorias USB otros).
FASE 2	Se utiliza el portal del poder judicial para registro o recepción de las actuaciones anexando los documentos digitalizados.
FASE 3	-Se utiliza el portal del poder judicial para ingreso de las actuaciones por formularios inteligentes con la descripción detallada y organizada procesalmente incorporando por este medio los anexos digitales. -Se cuentan con herramientas o servicios que permitan presentar actuaciones masivas ante el poder judicial.
FASE 4	Se cuentan con herramientas o servicios que permitan interactuar con los sistemas judiciales de los estados iberoamericanos para presentar actuaciones como exhortos, execuátur o la realización de las consultas ante otros poderes judiciales.
FASE 5	Se utiliza el portal del poder judicial para la presentación de las actuaciones a través de medios audiovisuales.

Guía de Exploración

COMPONENTES CLAVE					
1. Mecanismos de ingreso	**1**	**2**	**3**	**4**	**5**
1.1. Recepción de actuaciones en formato papel y/o con anexos digitales en medios físicos (CD, DVD, Memorias USB otros) y escaneo por parte del poder judicial.	X	X	X	X	X
1.2. Recepción de las causas y las actuaciones digitalizadas a través del portal.					
1.3. Uso de formularios inteligentes en portal			X X	X X	X
1.4. Uso medios audiovisuales con catalogación en el portal.					
1.5. Asignación automática del despacho para actuaciones que impliquen la presentación de nuevas causas.			X	X	X
1.6. Remisión de causas entre despachos.			X	X	
1.7. Interoperar con otras instituciones Nacionales				X	X X
1.8. Interoperar con otras instituciones Internacionales Cooperación jurídica internacional para el ingreso de causas.			X	X	X

C1.1 RECEPCIÓN DE ACTUACIONES EN FORMATO PAPEL Y/O EN FORMATO DIGITAL ANEXO

Descripción:

La entidad judicial recibe documentación en formato físico (papel) con la posibilidad de presentarse el documento digital anexo, el poder judicial cuenta con políticas de digitalización documental validadas de conocimiento público, establecidas y divulgadas a los despachos judiciales y la ciudadanía.

Productos de trabajo:

1. Políticas establecidas y divulgadas para la digitalización de los documentos que hacen parte de un proceso judicial.

2. Política para la conservación de los documentos que hacen parte del proceso judicial y los procedimientos para asociarlos al sistema de información.

3. Controles establecidos frente a la calidad y disposición de los documentos que se están digitalizando por parte del poder judicial.

4. Consolidación del Comité evaluador de la estrategia.

5. Lecciones aprendidas y recomendaciones frente a las situaciones originadas con la implementación de esta estrategia.

6. Guía validada de características técnicas documentales que se controlaran en la fase de ingreso de documentos desde el portal web.

Subprácticas/Tecnologías/Indicadores:

1. Revisar precedentes frente a las guías, políticas de digitalización de documentos judiciales y los metadatos de documentos judiciales digitales.
2. Construir, validar e institucionalizar las políticas de digitalización para el manejo documental electrónico conservando la calidad, la confiabilidad y la indexación (de ser posible del documento).
3. Establecer y mantener una política de la organización para la conservación y disposición de los documentos digitalizados y que hacen parte de un proceso judicial.
4. Establecer elementos de control de los documentos que se están aportando.
5. Identificar y corregir las causas de los defectos en el ingreso de los documentos aportados.
6. Asociar los documentos digitales a las actuaciones del sistema de información conformando la carpeta digital.

Lecciones aprendidas: (casos de los países)

1. Colombia
    a. Caso Jurisdicción Contencioso Administrativos de Colombia
    b. Caso cero Papel Colombia en despachos de restitución de tierras
    c. Caso digitalización documental en juzgados penales de Colombia

Referencias

- Recomendaciones para la digitalización de documentos en los archivos. Grupo de trabajo para la elaboración de Recomendaciones para la digitalización de documentos en los archivos, 2010, Castilla y León.

C1.2 RECEPCIÓN DE LAS CAUSAS Y LAS ACTUACIONES DIGITALIZADAS A TRAVÉS DEL PORTAL

Descripción:

La entidad judicial recibe documentación digital a través del portal del poder judicial, que estará en capacidad de validar la identidad de la persona que aporta el documento digital y asegurar la integridad del mismo.

Productos de trabajo:

1. Criterios para la validación de la identificación de los actores que ingresan información al portal del poder judicial.
2. Políticas de seguridad frente a la identificación de los actores a través del portal.
3. Criterios para asegurar el cumplimiento de las características de confiabilidad, disponibilidad e integridad de los documentos digitales aportados.
4. Portal web del poder judicial validado y ajustado para el cumplimiento de las necesidades del componente.

Subprácticas/Tecnologías/Indicadores:

1. Revisar las guías y buenas prácticas para la validación de la persona que está aportando la documentación
2. Selección de los mecanismos de autenticación de las personas que aportaran información.
3. Revisar las guías y buenas prácticas para el control de integridad e inmodificabilidad de los documentos recepcionados.
4. Selección de los criterios para la certificación de la integridad e inmodificabilidad de los documentos.

5. Elaboración de convenios con entidades de registro de identidad de orden nacional.

Lecciones aprendidas: (casos de los países)

- Caso de validación de inicio: Singapur, México, Chile, Costa Rica, México, Nicaragua
- Recomendaciones del Ministerio de Tecnologías de Colombia

C1.3 FORMULARIOS INTELIGENTES EN EL PORTAL

Descripción:

La entidad judicial recibe las causas desde el portal con el diligenciamiento de formularios inteligentes y se hace el recibo de documentación digital como anexos soporte.

Productos de trabajo:

1. Criterios para la validación de la identificación de los actores que ingresan información al portal del poder judicial.
2. Políticas de seguridad frente a la identificación de los actores a través del portal.
3. Criterios para asegurar el cumplimiento de las características de confiabilidad, disponibilidad e integridad de los documentos digitales aportados.
4. Portal web del poder judicial validado y ajustado para el cumplimiento de las necesidades del componente.

Subprácticas/Tecnologías/Indicadores:

1. Revisar las guías y buenas prácticas para la validación de la persona que está diligenciando los formularios y aportando los anexos y seleccionar los mecanismos de autenticación de las personas que aportaran información.
2. Revisar las guías y buenas prácticas para el control de integridad e inmodificabilidad de los documentos recepcionados y seleccionar los criterios para la certificación de la integridad e inmodificabilidad de los documentos.
3. Elaboración de convenios con entidades de registro de identidad de orden nacional.

Lecciones aprendidas: (casos de los países)

1. Recibir las consideraciones de Chile, Costa Rica, España y Nicaragua

C.2 CATEGORÍA TRÁMITES

Propósito:

En esta categoría se considera todo lo relacionado con la tramitación, actuaciones, diligencias, notificaciones, escritos y resoluciones de la causa, realizadas por los ciudadanos participantes y los Tribunales una vez ingresada la causa al sistema legal, con el fin de dar curso a la causa.

FASE	**ALCANCE**
FASE CERO O INICIAL	
FASE 1	

FASE 2	
FASE 3	
FASE 4	
FASE 5	

Guía de Exploración

COMPONENTES CLAVE					
2. Mecanismos de Tramitación	**1**	**2**	**3**	**4**	**5**

C.3 CATEGORÍA TÉRMINO

Propósito:

La etapa de término de una causa se entenderá para estos efectos, como la que transcurre desde la resolución que pone término a la etapa declarativa (sentencia, conciliación, etc.) y el cumplimiento efectivo de lo sentenciado.

Para la primera sub etapa, esto es, la dictación de la resolución "final" que pone término a la controversia, por la relevancia de la misma, se propone contar con plantillas inteligentes, las cuales por una parte permitan al juez plasmar de manera rápida y eficiente su decisión, y por otra, faciliten el rescate posterior de la información contenida en ellas, toda vez que esos datos son insumo de las sub etapas siguientes. Estas plantillas deben permitir diferenciar las distintas partes de una sentencia (expositiva, considerativa y resolutiva), los montos o cuantías expresados en ellas, los plazos y a quienes afectan, y por supuesto, ser almacenadas en formato digital (XML).

Con un texto de sentencia de estas características, resulta mucho más eficiente y trazable la segunda sub etapa, que es el seguimiento y registro del cumplimiento, por cuanto del mismo contenido de la resolución antes mencionada, se puede ir realizando supervisión de los pagos realizados, los plazos, los responsables y así permitir tomar medidas preventivas y correctivas que en definitiva lleven a dar por cumplido lo ordenado por el juez.

Complementariamente, en los sistemas de tramitación se pueden implementar mecanismos de control de gestión y del cumplimiento con indicadores específicos.

La integración de la información, además puede tener diversas aristas, desde la inclusión de registros de audio o video de fácil acceso para apoyar la toma de decisión, hasta la interconexión con otras instituciones que permita materializar la eficiencia del proceso de cumplimiento a través de información (direcciones, solvencia) o directamente retenciones y traspasos de dinero (embargo de cuentas corrientes bancarias, devoluciones de impuestos, etc.)

Luego de tener toda la información en formatos digitales inteligentes como el XML, que a través del ordenamiento de los datos en campos permite mostrar información de manera selectiva, se puede publicar en los Portales Web lo que se estime pertinente de acuerdo a las normas legales vigentes de protección de datos personales y transparencia en cada materia, competencia o país.

Es importante mencionar que la sentencia se tomará del audio y será transcrita al formato predefinido de manera automática con una herramienta de transcripción de audio a plantilla o texto en el formato propuesto anteriormente (XML).

FASE	ALCANCE
FASE CERO O INICIAL	Se elabora la sentencia en Word y se imprime, esta es firmada físicamente por el Juez, para posteriormente ser adjuntada al expediente físico. Se escanea la sentencia y se publica a través del Portal de la institución. Se entrega a solicitud, una copia de la sentencia debidamente firmada por el Ministro de Fe, en papel. No se tienen antecedentes del cumplimiento, solo por reclamo escrito de las partes. Se envía el expediente físico al archivo judicial.
FASE 1	Se elabora la Sentencia a través de un sistema de registro de causa con firma simple. Es subida al portal de la institución para su publicación, a través de un proceso. Se entrega a solicitud, una copia de la sentencia debidamente firmada por el Ministro de Fe, en papel. No se tienen antecedentes del cumplimiento, solo por reclamo escrito de las partes. Se imprime la sentencia y se incorpora al expediente físico para ser enviada al archivo judicial.
FASE 2	Se elabora la Sentencia a través de un sistema de tramitación de causa, asociándola a una metada con firma simple. Es subida al portal de la institución para su publicación, a través de un proceso. Se entrega a solicitud, una copia de la sentencia debidamente firmada por el Ministro de Fe, en papel. No se tienen antecedentes del cumplimiento, solo por reclamo escrito de las partes. Se archiva de forma electrónica sin necesidad de ser enviada en papel al archivo judicial.
FASE 3	Se elabora la Sentencia a través de un sistema de tramitación de causa, asociándola a una metada con firma Electrónica avanzada y un código de barra. Es subida al portal de la institución para su publicación, a través de un proceso. Se expide un certificado de la sentencia para que esta sea consultada en el portal de la institución. Se incorporan a la tramitación elementos esenciales de lo sentenciado para poder efectuar seguimiento del cumplimiento. Se archiva de forma electrónica sin necesidad de ser enviada en papel al archivo judicial.
FASE 4	Se elabora la Sentencia en un formato XML con una lógica predefinida a través de un sistema de tramitación de causa, asociándola a una metada con firma Electrónica avanzada y un código de barra. Es subida al portal de la institución para su publicación, a través de un proceso. Se expide un certificado de la sentencia para que esta sea consultada en el

	portal de la institución. Se generan interconexiones con organismos relacionados a los cumplimientos de la sentencia que permitan de forma automática alimentar el expediente electrónico de la efectividad del cumplimiento y poder hacer gestión. Se archiva de forma electrónica sin necesidad de ser enviada en papel al archivo judicial.
FASE 5 OPTIMIZACION	Se elabora la Sentencia en un formato XML con una lógica predefinida a través de un sistema de tramitación de causa, asociándola a una metada con firma Electrónica avanzada y un código de barra. Es subida al portal de la institución para su publicación, a través de un proceso. Se expide un certificado de la sentencia para que esta sea consultada en el portal de la institución. Se enviará por interconexión a los organismos que así lo requieran (Registro Civil, MP, DPP, TGR, CGR y demás) Se generan interconexiones con organismos relacionados a los cumplimientos de la sentencia que permitan de forma automática alimentar el expediente electrónico de la efectividad del cumplimiento y poder hacer gestión. Se elabora un proceso inteligente y automatizado para enviar al archivo judicial una vez proceda y de igual forma a través de este proceso se pueda solicitar el desarchivo de esta causa y quedar disponible para retomar su tramitación.

Guía de Exploración

COMPONENTES CLAVE	**FASE**				
3. Mecanismos de Termino de Demanda	**1**	**2**	**3**	**4**	**5**
3.1 Elaborar la Sentencia y firmarla en papel e incorporarla en expediente físico.	X				
3.2 Elaborar la Sentencia en un formato de texto plano, imprimirla para su firma, escanearla y subirla al sistema de tramitación.		X	X		
3.3 Elaborar la Sentencia en formato digital inteligente, que pueda ser Firmado Electrónica Avanzada, almacenarla en expediente electrónico y poderlo consultar en su contenido.			X	X	X

C3.1 ELABORAR LA SENTENCIA Y FIRMA EN PAPEL E INCORPORARLA EN EL EXPEDIENTE FISICO.

Descripción:

La entidad judicial elabora una sentencia en formato físico (papel), el poder judicial cuenta con un aplicativo al cual se puede subir el documento de la Sentencia de forma digital.

Productos de trabajo:

1. Definir el proceso para que una vez elaborada la sentencia en papel, como se debe resguardar está en el expediente (físico/digital) estableciendo si debe ser subido a un aplicativo con Firma de puño y letra.

2. Política para la conservación de los documentos que hacen parte del proceso judicial y los procedimientos para asociarlos al sistema de información.

3. Controles establecidos frente a la calidad y disposición de los documentos que se están digitalizando por parte del poder judicial.

4. Registro de la sentencia en diferentes instancias o procesos para dejar constancia de la misma.

Sub prácticas/Tecnologías/Indicadores:

1. **1.** Establecer y mantener una política de la organización para la conservación y disposición de los documentos digitalizados y que hacen parte de un proceso judicial.
2. **2.** Establecer elementos de control de los documentos que se están aportando.
3. **3.** Identificar y corregir las causas de los defectos en el ingreso de los documentos aportados.

Lecciones aprendidas: (casos de los países)

1. Chile
    a. Caso competencia Civil expedientes paralelos (físico y digital)
    b. Caso cero Papel Tribunales de Garantía y de Juicio Oral en lo penal, Familia, Cobranza, Letras del Trabajo

Referencias

- Para el manejo paralelo del expediente físico y digital se incorpora el concepto de inventario de causas (físico vs digital) y se apoya la gestión con el uso de los capturadores de código de barra.

C3.2 ELABORAR SENTENCIA EN UN FORMATI DE TEXTO PLANO, IMPRIMIRLA PARA SU FIRMA, ESCANEARLA Y SUBIRLA AL SISTEMA DE TRAMITACIÓN.

Descripción:

La entidad judicial elabora una sentencia en formato digital (Word), este contiene firma simple y se elabora a través del sistema de tramitación de causas, tanto para su generación, como para su resguardo.

Productos de trabajo:

1. Políticas establecidas para la digitalización y guardado del documento con firma digital simple. Que la institución lo reconozca como un proceso valido.

2. Política para la conservación de los documentos que hacen parte del proceso judicial y los procedimientos para asociarlos al sistema de información.

2. Elementos que permitan garantizar la confiabilidad en el documento.

3. Controles establecidos frente a la calidad y disposición de los documentos que se están digitalizando por parte del poder judicial.

4. Registro de la sentencia en diferentes instancias o procesos para dejar constancia de la misma.

Sub prácticas/Tecnologías/Indicadores:

1. Generar una metadata que permitan la búsqueda de las sentencias a posterior.
2. Establecer y mantener una política de la organización para la conservación y disposición de los documentos digitalizados y que hacen parte de un proceso judicial.
3. Generar documentos que sean borradores de la sentencia durante el proceso, hasta que este sea firmado con firma simple
4. Establecer elementos de control de los documentos que se están aportando.
5. Identificar y corregir las causas de los defectos en el ingreso de los documentos aportados.

Lecciones aprendidas: (casos de los países)

1. Chile
    a. Para que estas prácticas sean acogidas por los Tribunales del País la solicitud debe ser emanada desde la instancia superior, Chile, instrucción impartida por el Pleno de la Corte Suprema.
    b. Sensibilizar inicialmente a los órganos interinstitucionales con que el documento sentencia que se encontraba en el expediente y que contenía firma simple era reconocido por la organización.

Referencias

- Acta 91 dictada por la corte Suprema de Chile, que define y formaliza el proceso digital de un expediente, considerando la sentencia dentro y fuera de audiencia.

C3.3 ELABORAR LA SENTENCIA EN FORMATO DIGITAL INTELIGENTE, FIRMADO CON FIRMA ELECTRONICA AVANZADA, ALMACENADA EN EXPEDIENTE ELECTRONICO Y PODER CONSULTAR EN SU CONTENIDO.

Descripción:

La entidad judicial elabora una sentencia en formato digital inteligente, formato XML con campos dinámicos asociados al documento sentencia de elementos esenciales de la sentencia y otros asociados al cumplimiento de la misma, este formato contiene firma digital avanzada y se elabora a través del sistema de tramitación de causas, tanto para su generación, como para su resguardo. No requiere ser impreso, sino que se disponibiliza a través del portal del Poder judicial y se le asigna un código de barra para ser consultada su veracidad.

Productos de trabajo:

1. Definir las variables esenciales de una sentencia.
2. Políticas establecidas para la digitalización y guardado del documento con firma digital avanzada. Que la institución lo reconozca como un proceso valido.
3. Incorporar la Firma digital avanzada y el proceso para su incorporación o firma en el expediente digital.
4. Considerar la firma para sentencias masivas y para sentencias individuales.
5. Considerar más de una firma para una sentencia.
6. Asociar a cada sentencia un código de barra con una inteligencia relacionada con datos de la causa como el cataratulado por ejemplo.
7. Política para la conservación de los documentos que hacen parte del proceso judicial y los procedimientos para asociarlos al sistema de información.
8. Una vez dictada la sentencia rescatar los elementos que forman parte de la etapa de cumplimiento.
9. Una vez el proceso lo permita proceder al archivo del expediente digital.

Sub prácticas/Tecnologías/Indicadores:

1. Generar un procedimiento para la incorporación de la Firma electrónica avanzada a los documentos generados dentro de Tribunales.
2. Evaluar utilizar un ente certificador o convertirse en un organismo autocertificador de la institución.
3. Sensibilizar a la comunidad en el uso de la Firma Electrónica Avanzada.
4. Reconocer que el proceso es 100% digitalizado y la sentencia parte de este.

5. Establecer y mantener una política de la organización para la conservación y disposición de los documentos digitalizados y que hacen parte de un proceso judicial.
6. Generar documentos que sean borradores de la sentencia durante el proceso, hasta que este sea firmado con firma simple
7. Establecer elementos de control de los documentos que se están aportando.

Lecciones aprendidas: (casos de los países)

2. Chile
    a. En materia penal incorporación de la Firma digital avanzada en la generación de Ordenes y Contraordenes, las cuales tienen asociada un código de barra inteligente, que permite ser consultadas a través del Portal del Poder judicial.
    b. En materia civil incorporación de la Firma Digital avanzada en la generación masiva de sentencias para el procedimiento ejecutivo.
    c. En segunda instancia se está incorporando la Firma Electrónica Avanzada para el procedimiento ….
    d. En materia de Familia se ha incorporado la Firma Electrónica Avanzada…

Referencias

DESARROLLO DE COMPONENTES TRASVERSALES DEL MODELO

COMPONENTES TRASVERSALES	1	2	3	4	5
1. Manejo Documental, aplicativo de catalogación resguardo y consulta de los documentos digitales, videos y/o audios en la carpeta digital			X	X	X
2. **Control de Seguridad Informática y de la Información**					
2.1 Establecer Mecanismos de Autenticación		X	X	X	X
2.2 Contar con trazabilidad de las causas		X	X	X	X
2.3 Controlar de seguridad de los documentos		X	X	X	X
2.4 Monitorizar y contralar la Seguridad de las transacciones			X	X	X
3. Procesos de apoyo					
3.1 Contar con Soporte y Mesa de Ayuda (recoger información de mejoras)		X	X	X	X
3.2 Manejar Ayudas Automatizadas			X	X	X
3.3 Contar con planes de difusión por cambios de fase de Ingreso					
4. Talento Humano					
4.1 Diseñar y divulgar herramientas de capacitación	X	X	X	X	X
5. Infraestructura					
5.1 Asegurar la continuidad operacional: redundancia, disponibilidad, conexiones alternas, planes de contingencia		X	X	X	X
6. Marco normativo					
6.1 Disponer de un Marco legal que posibilite la implementación del E.E.	X	X	X	X	X

T.1 MANEJO DOCUMENTAL

Descripción:

Se establece el manejo documental y archivístico de los documentos digitales en una unidad procesal integrada -Carpeta Digital-.

Productos de trabajo:

1. Modelo de gestión documental y archivística definido
2. Unidad Procesal definida como una sola carpeta digital, de tal manera que aunque se produzcan documentos en diferentes despachos, todos pertenezcan a la misma Unidad Procesal integrada.
3. Tablas de retención documental y carga de documentos digitales esperados.
4. Matriz de marco normativo vigente relacionado con la organización documental.

Subprácticas/Tecnologías/Indicadores:

1. Definir un marco de referencia para organizar y definir el modelo de gestión documental y archivística, el cual contenga los lineamientos operativos, estructurales, funcionales, conceptuales, el flujo de información y los perfiles de acceso, a tener en cuenta para el manejo documental y archivístico que incluya las transferencias de archivo de gestión a histórico.
2. Definir los niveles de acceso a los elementos digitales.
3. Definir la Unidad Procesal, en la que las actuaciones de los diferentes despachos intervinientes se integren en una sola carpeta digital, de tal manera que aunque se produzcan documentos en diferentes despachos, todos pertenezcan a la misma Unidad Procesal integrada.

Lecciones aprendidas: (casos de los países)

1.

T.2 SEGURIDAD DE LA INFORMÁTICA Y DE LA INFORMACIÓN

Descripción:

Con el fin de asegurar la confiabilidad, integridad y acceso a la información de los procesos judiciales, es necesario se defina este componente de manera claro y concisa.

Productos de trabajo:

1. Manual de Gestión de la seguridad de la información.
2. Manual de políticas de seguridad de la información
3. Matriz de valoración de los activos de la información
4. Matriz de asignación de responsabilidades RASCI.
5. Procedimiento de tratamiento y gestión de incidentes de seguridad de la información
6. Actualización de protocolos de seguridad existentes.
7. Diseño de Actas de presunción, Acuerdos confidencialidad, Acuerdos de corresponsabilidad.
8. Documento de buenas prácticas de seguridad de la información
9. Documento de Recomendaciones para generar un modelo de gestión integral con el fin de incluir en los criterios de la norma ISO27001:2005 en los procesos actuales de la norma ISO 9001:2008.
10. Documento de Recomendaciones de actividades para la implementación de planes de contingencia para los procesos críticos.
11. Documento de Recomendaciones y análisis de seguridad de infraestructura.
12. Documento de Recomendaciones y análisis de proyección para garantizar la disponibilidad del sistema.
13. Políticas para la auditoria
14. Matriz de documentos digitales con los niveles de acceso a los elementos digitales
15. Documento de perfiles de acceso a los documentos digitales.
16. Marcos de referencia para la seguridad de la información debidamente estandarizada.

Subprácticas/Tecnologías/Indicadores:

1. Identificar los riesgos de la seguridad de la información.
2. Formular y consolidar las políticas y protocolos de seguridad de la información para su manejo, comunicación e intercambio de información interinstitucional, tanto para el manejo de documentos físicos como de documentos electrónicos, bajo un enfoque de procesos, el marco legal vigente y el contexto tecnológico de la Rama Judicial.

Lecciones aprendidas: (casos de los países)

T.3 INFRAESTRUCTURA

Descripción:

La infraestructura tecnológica es el conjunto de hardware y software sobre el que se asientan los servicios requeridos para el litigio en línea para operar de manera eficiente y eficaz durante el tiempo previsto con niveles altos de servicios; debe contar con redundancia, disponibilidad, conexiones alternas, sistemas de respaldo o de contingencia, para brindar todo el soporte necesario.

Productos de trabajo:

1. Dimensionamiento de los Centros de Datos con especificaciones técnicas que permitan crecimiento y escalabilidad dinámico.
2. Establecer el tipo de arquitectura del centro de datos con fin de garantizar disponibilidad y contingencia.
3. Manuales y documentación de la arquitectura usada para la implementación en la plataforma tecnológica.
4. Manuales de referencias para la implementación y gestión del Servicio.
5. Protocolos establecidos para mitigar problemas técnicos y reducir al máximo los tiempos de soporte, planes de contingencia, disponibilidad y análisis de riesgo.

Subprácticas/Tecnologías/Indicadores:

1. Definir las especificaciones técnicas de los centros de datos que requiere el poder judicial teniendo en cuenta el crecimiento y escalabilidad dinámico soportar las operaciones de la entidad.
2. Evaluar la arquitectura de la infraestructura de establecer la infraestructura que soporte tecnológicamente el expediente electrónico pero que estarán sujetas a análisis de necesidad, estudios técnicos, modelos de prueba y ajustes para su adecuada operación.
3. Definir los criterios para la ubicación del Centro de Datos y su administración.
4. Realizar el análisis de la necesidad según etapas y/o fases de implementación con el fin de que no se paralice el servicio por motivos técnicos.

Lecciones aprendidas: (casos de los países)

T.4 TALENTO HUMANO

Descripción:

Productos de trabajo:

5. Estrategia para generar un cambio gradual de la tradición jurídica basada en documentos en papel a la gestión electrónica de documentos, teniendo cuidado de cumplir con estándares nacionales e internacionales.

Subprácticas/Tecnologías/Indicadores:

Lecciones aprendidas: (casos de los países)

TECNOLOGÍA DE LOS PODERES JUDICIALES

CONTENIDO

1. Seguridad de la Información

La información es un activo que tiene un alto valor y requiere, en consecuencia, una protección adecuada. Ésta se puede presentar de las siguientes formas:

- impresa o escrita en papel,
- almacenada electrónicamente,
- trasmitida por correo o medios electrónicos,
- hablada en conversación.

La seguridad de la información consiste en procesos y controles diseñados para protegerla de su divulgación no autorizada, transferencia, modificación o destrucción, a efecto de:

- asegurar la continuidad del negocio,
- minimizar posibles daños, y
- maximizar oportunidades.

La seguridad informática debe entenderse en el contexto de la seguridad física y lógica de la información, y por eso intenta proteger cuatro elementos:

- Hardware
- Software
- Datos
- Elementos Consumibles

2. Seguridad de Información Familia ISO/IEC 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI), estas normas incluyen:

1. **ISO/IEC 27000**- es un vocabulario estándar para el SGSI. Se encuentra en desarrollo actualmente.
2. **ISO/IEC 27001** - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.
3. **ISO/IEC 27002** - Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. **Es un código de buenas prácticas para la gestión de seguridad de la información**. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.
4. **ISO/IEC 27003** - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.
5. **ISO/IEC 27004** - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.
6. **ISO/IEC 27005** - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008.
7. **ISO/IEC 27006:2007** - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma específica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
8. **ISO/IEC 27007** - Es una guía para auditar al SGSI. Se encuentra en preparación.
9. **ISO/IEC 27799:2008** - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.
10. **ISO/IEC 27035:2011 -** Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este estándar hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

3. Seguridad de Información (ISO/IEC 27001)

Estándar para la seguridad de la información ISO/IEC 27001 (Information technology - Security techniques – Information security management systems - Requirements)

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

PILARES DE SEGURIDAD DE INFORMACIÓN (ISO/IEC 27001)

4. Seguridad de Información (ISO/IEC 27002)

Es un conjunto de recomendaciones sobre qué medidas tomar en la institución para asegurar los Sistemas de Información.

Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009. Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondonorma ISO/IEC 27002), Argentina (IRAM-ISO-IEC 27002), Chile (NCh-ISO27002), Uruguay (UNIT-ISO/IEC 27002) o Perú (como ISO 17799; descarga gratuita.

- Los **objetivos de seguridad** recogen aquellos aspectos fundamentales que se deben analizar para conseguir un sistema seguro en cada una de las áreas que los agrupa.
  Para conseguir cada uno de estos objetivos, la norma propone una serie de medidas o recomendaciones (controles) que son los que en definitiva se aplican para la gestión del riesgo analizado.

Los **objetivos de control** son los aspectos a asegurar dentro de cada área/sección; y los **controles** son los mecanismos para asegurar los objetivos de control (guía de buenas prácticas). Para cada control establecido, se debe elaborar una guía para su implantación)

Para la elaboración del documento que se presentará como guía de seguridad informática es conveniente utilizar la ISO/IEC 27002, en virtud que incluye controles específicos relacionados con aspectos informáticos.

4.1 Contenido de la norma

- ✓ 11 dominios
- ✓ 39 objetivos de control
- ✓ 133 controles

Los 133 controles y 39 objetivos están agrupados dentro de los 11 dominios descritos abajo:

DOMINIO		DESCRIPCIÓN
5.	Política De Seguridad	El documento de la política de seguridad de la información debiera ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.
6.	Aspectos Organizativos de La Seguridad de la Información	La gerencia debiera apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información.
7.	Gestión de Activos.	Inventario de los activos debiera incluir toda la información necesaria para poder recuperarse de un desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial.
8.	Seguridad Ligada a los Recursos Humanos.	Los roles y responsabilidades de la seguridad debieran ser definidos y claramente comunicados a los candidatos para el puesto durante el proceso de pre-empleo.

DOMINIO		DESCRIPCIÓN
9.	Seguridad Física y del Entorno	Se debieran utilizar perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.
10.	Gestión de Comunicaciones y Operaciones.	Procedimientos documentados para las actividades del sistema asociadas con los medios de procesamiento de la información y comunicación; tales como procedimientos para encender y apagar computadoras, copias de seguridad, mantenimiento del equipo, manejo de medios, cuarto de cómputo, manejo del correo y seguridad.
11.	Control de Acceso.	Establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad para el acceso.
12.	Adquisición, Desarrollo y Mantenimiento De Sistemas de Información.	Identificary acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.
13.	Gestión de Incidentes en la Seguridad de la Información.	Procedimientos formales de reporte y de la intensificación de un evento, ejemplo: cambios del sistema no controlados, mal funcionamiento del software o hardware, violaciones de acceso.
14.	Gestión de la Continuidad del Negocio.	Desarrollar y mantener un proceso gerencial para la continuidad del negocio en toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
15.	Cumplimiento.	Definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales relevantes, y el enfoque de la organización para satisfacer esos requerimientos, para cada sistema de información y la organización.

4.2 Guía de Seguridad Informática

Para el desarrollo de la guía en cuestión, se tomarán de referencia 5 dominios, los cuales se relacionan directamente con el área informática:

No.	DOMINIO
7.	Gestión de Activos.
10.	Gestión de Comunicaciones y Operaciones.
11.	Control de Acceso.
12.	Adquisición, Desarrollo y Mantenimiento De Sistemas de Información.
13.	Gestión de Incidentes en la Seguridad de la Información.

Guía de Seguridad Informática
ISO/IEC 27002

DOMINIO 7: GESTIÓN DE ACTIVOS

Activos.-

- **Información:** Bases de datos, la data (sorteo, providencias o actos procesales, sentencias, jurisprudencia; información administrativa, información financiera), contratos y acuerdos, resoluciones, planes de continuidad del negocio, registros de auditorías
- **Archivos de Software:** sistemas de gestión de trámite jurisdiccional, sistemas de gestión documentas, erp, sistemas operativos, entre otros.
- **Activos de Hardware:** Servidores, equipos de comunicación, equipamiento de TIC´s
- **Personal:** roles y responsabilidades acorde a la capacidad y experiencia del personal de las diferentes unidades de TIC´s
- **Intangibles:** Imagen de transparencia, celeridad, seguridad y justicia.

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
7.1	Inventario de activos	Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.	La organización identificará todos los activos y documentará de acuerdo a su importancia. El inventario incluirá toda la información necesaria para recuperarse de los desastres.	El no contar con un conjunto de políticas específicas así como responsables para el uso de los activos podría verse afectada la integridad y disponibilidad de la información.
	Responsable de los activos	Toda la información y los activos asociados con los servicios de procesamiento de información deben ser asignada a una parte de la organización que actúa como responsable.	Una vez que se ha definido, identificado, elaborado el inventario de todos los activos de Tics de la organización se identificará al responsable o los responsables de controlar el uso y seguridad de estos. Además se realizará una revisión periódica a la clasificación y definición de responsables de los activos y servicios que se ofrecen.	
	Uso aceptable de los activos	Se debe identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.	Las organizaciones establecerán un conjunto de políticas, normas específicas, reglas, manuales de uso y demás directrices, con el fin de garantizar la seguridad y disponibilidad respecto al acceso y uso que se dé a los activos, asociados a los sistemas de información de cada una de las organizaciones.	
7.2	Directrices de clasificación	Se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.	Las organizaciones clasificarán la información en términos de valor, confidencialidad y criticidad para la organización, y será revisada periódicamente manteniéndose actualizada. La clasificación debe ser lo más sencilla y práctica en lo posible.	Al no existir una clasificación acorde a la importancia de la información así como el etiquetado según estándares internos adoptados para la organización podría verse afectada seriamente la integridad, disponibilidad y confidencialidad de la información.
	Etiquetado y manejo de la información	Se debe desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.	Se debe definir un estándar de etiquetado adecuado de la información aprobado por la organización, que comprenda los formatos físicos y electrónicos. De acuerdo al nivel de importancia de la información se debe definir procedimientos de manejo seguro, así como el registro de incidentes de seguridad referido a la cadena de custodia.	

DOMINIO 10: GESTIÓN DE COMUNICACIONES Y OPERACIONES

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
10.1	Procedimientos y responsabilidades operacionales	Procedimientos de operación documentados	Preparar procedimientos documentados para las actividades del sistema asociadas con los medios de procesamiento de la información y comunicación;	Falta de segregación de funciones.
		Gestión del cambio	Sistemas operacionales y el software de aplicación sujetos a un estricto control de autoridades del cambio.	
		Segregación de los deberes	Tener cuidado que nadie pueda tener acceso, modificar o utilizar los activos sin autorización o detección.	
		Separación de los medios de desarrollo, prueba y operación	Identificar el nivel de separación necesario entre los ambientes de desarrollo, prueba y operación para evitar los problemas operacionales e implementar los controles apropiados.	
10.2	Gestión de la entrega del servicio de terceros	Entrega del servicio	Incluir acuerdos de seguridad pactados en la entrega del servicio por un tercero e incluir definiciones del servicio y aspectos de la gestión del servicio.	Falta de calidad en el servicio adquirido.
		Monitoreo y revisión de los servicios de terceros	El monitoreo y revisión de los servicios de terceros debiera asegurar que se cumplan los términos y condiciones de seguridad de los acuerdos, y que se manejen apropiadamente los incidentes y problemas de seguridad de la información.	
		Manejo de cambios en los servicios de terceros	El proceso de manejar los cambios en el servicio de terceros necesita tomarlos cambios realizados por la organización	
10.3	Planeación y aceptación del sistema	Gestión de la capacidad	Identificar los requerimientos de capacidad de cada actividad nueva y en proceso.	Fallas de Operación en los sistemas
		Aceptación del sistema	Asegurar que los requerimientos y criterios de aceptación de los sistemas nuevos estén claramente definidos, aceptados, documentados y probados.	

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
10.4	Protección contra el código malicioso y móvil	Controles contra códigos maliciosos	Basarse en la detección de códigos maliciosos y la reparación de software, conciencia de seguridad, y los apropiados controles de acceso al sistema y gestión del cambio.	Posible pérdida de información y atraso en las operaciones.
		Controles contra códigos móviles	Considerar acciones para evitar que el código móvil realice acciones no-autorizadas	
10.5	Respaldo o Back-Up	Respaldo o Back-Up	Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla de medios.	Posible pérdida de información crítica y suspensión de actividades
10.6	Gestión de seguridad de la red	Controles de redes	Implementar controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados.	Posible intrusión de terceros no autorizados e interrupción del servicio.
		Seguridad de los servicios de la red	Determinar y monitorear regularmente la capacidad del proveedor del servicio de red para manejar los servicios contratados de una manera segura	
10.7	Gestión de medios	Gestión de medios removibles	Considerar lineamientos para la gestión de medios removibles	Posible fuga de información.
		Retirada de soportes	Definición de procedimientos formales para la eliminación de medios confidenciales que ya no serán requeridos.	
		Procedimientos para el manejo de información	Establecer procedimientos para el manipuleo, procesamiento, almacenaje y comunicación de la información consistente con su clasificación.	
		Seguridad de la documentación del sistema	asegurar la documentación del sistema de manera segura	
10.8	Intercambio de información	Políticas y procedimientos de intercambio de información	Definir procedimientos y controles a seguirse cuando se utilizan medios de comunicación electrónicos para el intercambio de información	Posible fuga de información y suplantación de identidades.
		Acuerdos de intercambio	Establecer y mantener las políticas, procedimientos y estándares para proteger la información y medios físicos en tránsito	

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
		Medios físicos en tránsito	Considerar lineamientos para proteger los medios de información transportados entre diferentes ubicaciones	
		Mensajes electrónicos	Definir consideraciones de seguridad para los mensajes electrónicos	
		Sistemas de información	Definir consideraciones a las implicancias de seguridad en la interconexión de los sistemas de información	
10.9	Comercio electrónico	Comercio electrónico	Definir consideraciones de seguridad para el comercio electrónico	Posibles transacciones fraudulentas
		Transacciones en-línea	Definir consideraciones de seguridad para Transacciones en-línea	
		Información públicamente disponible	Proteger mediante mecanismos apropiados el software, data y otra información que requiere un alto nivel de integridad, puesta a disposición en un sistema públicamente disponible,	
10.10	Monitoreo	Registro de auditoría	Considerar registros de auditoría cuando sea relevante.	Posible incapacidad de prevenir fallos de sistemas
		Uso del sistema de monitoreo	Determinar el nivel de monitoreo requerido para los medios individuales mediante una evaluación del riesgo.	
		Protección del registro de información	Establecer controles para protegerse contra cambios no autorizados y problemas operacionales,	
		Registros del administrador y operador	Revisados de manera regular los registros de administrador y operador del sistema.	
		Registro de fallas	Registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con los problemas con el procesamiento de la información o los sistemas de comunicación	
		Sincronización de relojes	Colocar la hora del reloj de acuerdo a un estándar acordado	

DOMINIO 11: CONTROL DE ACCESO

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
11.1	Requerimiento para el control del acceso	Política de control del acceso	Establecer claramente en la política de control de acceso las reglas de control del acceso y los derechos para cada usuario o grupos de usuarios.	Posibles accesos no autorizados.
11.2	Gestión de acceso del usuario	Registro del usuario	Definir el procedimiento de control del acceso para el registro y des-registro del usuario.	Posible otorgamiento inadecuado de permisos
		Gestión de privilegios	Controlar la asignación de privilegios a través de un proceso de autorización formal para los sistemas multi-usuario que requieren protección contra el acceso no autorizado.	
		Gestión de las claves secretas de los usuarios	Definir políticas sobre la gestión de las claves secretas, medio común para verificar la identidad del usuario antes de otorgar acceso a un sistema o servicio de información en concordancia con la autorización del usuario	
		Revisión de los derechos de acceso del usuario	Definir lineamientos para la revisión de los derechos de acceso	
11.3	Responsabilidades del usuario	Uso de claves secretas	Formular política para la el uso de claves secretas de los usuarios	Posible perdida y fuga de información
		Equipo del usuario desatendido	Estar al tanto de los requerimientos de seguridad y los procedimientos para proteger el equipo desatendido por parte de los usuarios.	
		Política de escritorio y pantalla limpios	Tomar en cuenta las clasificaciones de información para políticas de escritorio limpio y pantalla limpia.	
11.4	Control de acceso a la red	Política sobre el uso de los servicios de la red	Formular una política relacionada con el uso de las redes y los servicios de la red.	Posible pérdida y fuga de información e interrupción de actividades.
		Autenticación del usuario para las conexiones externas	Utilizar técnicas basadas en criptografía, dispositivos de hardware o un protocolo de desafío/respuesta para la autenticación de los usuarios remotos.	
		Identificación del equipo en las redes	Utilizar la identificación del equipo si es importante que la comunicación sólo sea iniciada desde una ubicación o equipo específico.	
		Protección del puerto de diagnóstico y configuración remoto	Uso de un seguro y procedimientos de soporte para controlar el acceso físico al puerto que incluya controles potenciales para el acceso a los puertos de diagnostico y configuración.	

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
		Segregación en redes	Un método para controlar la seguridad de grandes redes es dividirlas en dominios de red lógicos separados	
		Control de conexión a la red	Los derechos de acceso a la red de los usuarios se debieran mantener y actualizar conforme lo requiera la política de control de acceso	
		Control de routing de la red	Implementar controles de routing en las redes para asegurar que las conexiones de la computadora y los flujos de información no violen la política de control de acceso de las aplicaciones	
11.5	Control del acceso al sistema operativo	Procedimientos para un registro seguro	Diseño del procedimiento para registrarse en un sistema de operación de manera que minimice la oportunidad de un acceso no autorizado.	Posible suspensión de actividades y del servicio.
		Identificación y autenticación del usuario	Aplicar este control a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de redes, programadores de sistemas y administradores de bases de datos).	
		Sistema de gestión de claves secretas	Los sistemas para el manejo de claves secretas debieran ser interactivos y debieran asegurar claves secretas adecuadas.	
		Uso de las utilidades del sistema	Se debieran considerar lineamientos para el uso de las utilidades del sistema:	
		Cierre de una sesión por inactividad	Un dispositivo de cierre debiera borrar la pantalla de la sesión y también, posiblemente más adelante, cerrar la aplicación y las sesiones en red después de un período de inactividad definido.	
		Limitación del tiempo de conexión	considerar controles sobre el tiempo de conexión para las aplicaciones de cómputo sensibles,	
11.6	Control de acceso a la aplicación y la información	Restricción del acceso a la información	Las restricciones para el acceso se debieran basar en los requerimientos de las aplicaciones.	Posible fuga y pérdida de información
		Aislar el sistema confidencial	considerar los siguientes lineamientos para aislar el sistema sensible o confidencial	
11.7	Computación y tele-trabajo móvil	Computación y comunicaciones móviles	Establecer una política y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móvil.	Posible suplantación de identidad y accesos no autorizados.

DOMINIO 12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
12.1	Requisitos de seguridad de los sistemas de información	Análisis y especificación de los requisitos de seguridad	Definir de líneas base de seguridad en aplicaciones e infraestructura de TI, de acuerdo a la necesidad de cada aplicación.	Posible adquisición e implementación de sistemas que no cumplen con medidas de seguridad reconocidas o aprobadas por la Institución.
12.2	Tratamiento correcto de las aplicaciones	Validación de los datos de entrada.	Validar los datos de entrada para evitar errores por captura de datos incorrectos.	Posible liberación en ambiente productivo de aplicaciones con vulnerabilidades de seguridad y procesamiento de datos incorrecto.
		Control de procesamiento interno	Revisar la seguridad de las aplicaciones a nivel código para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.	
		Integridad de los mensajes	Evaluar los riesgos de seguridad para determinar si se requiere la integridad del mensaje e identificar el método de implementación más apropiado.	
		Validación de los datos de salida	Validar los datos en el procesamiento, para asegurar que la información almacenada sea la correcta y la apropiada para las circunstancias. Ya que aún en los sistemas que han sido probados se puede producir output incorrecto.	
12.3	Controles Criptográficos	Política de uso de controles criptográficos	Desarrollar e implementar una Política para el uso de controles criptográficos, para proteger la información.	Posible afectación a la confidencialidad de la información mantenida en los sistemas y aplicaciones de la Institución. Posible falsificación de la firma digital, reemplazándola con la clave pública de un usuario.
		Gestión de claves	Proteger las claves criptográficas contra una modificación, pérdida y destrucción. Proteger contra la divulgación no-autorizada, las claves secretas y privadas. Brindar seguridad física al equipo utilizado para generar, almacenar y archivar las claves. A manera de ejemplo, los dos tipos de técnicas criptográficas son:	

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
			técnicas de claves secretas y técnicas de claves públicas.	
12.4	Seguridad de los archivos de sistema	Control del Software en explotación	Minimizar el riesgo de corrupción de los sistemas operacionales, considerando lineamientos para controlar los cambios como son: actualización del software operacional, los sistemas operacionales sólo deben mantener códigos ejecutables aprobados, y no códigos de desarrollo o compiladores. Establecer una estrategia de "regreso a la situación original" (rollback) antes de implementar los cambios.	Posibles fugas y pérdidas de información confidencial en posesión de la Institución, que pueden ser utilizadas para fines ajenos a la misma.
		Protección de los datos de prueba del sistema	Para los propósitos de pruebas, evitar el uso de bases de datos operacionales conteniendo información personal o cualquier otra información confidencial. Autorizar por separado cada vez que se copia información operacional en un sistema de aplicación de prueba.	
		Control de acceso al código fuente de los programas	El acceso al código fuente del programa y los ítems asociados (como diseños, especificaciones, planes de verificación y planes de validación) se deben controlar estrictamente para evitar la introducción de una funcionalidad no-autorizada y para evitar cambios no-intencionados. Implementar procedimientos estrictos de control de cambios para el mantenimiento y copiado de las bibliotecas fuentes del programa.	
12.5	Seguridad en los procesos de desarrollo y soporte	Procedimientos de control de cambios	Documentar y hacer cumplir los procedimientos formales de control del cambio para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y los cambios importantes a los sistemas existentes deben realizarse después de un proceso formal de documentación, especificación, prueba,	Posible introducción de cambios no probados y no autorizados en los sistemas y aplicaciones de la Institución. Posibles problemas de segregación de funciones en desarrollo y operación. Posible fuga de Información.

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
			control de calidad e implementación manejada. La buena práctica incluye la prueba del software nuevo en un ambiente segregado de los ambientes de producción y desarrollo.	
		Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Revisar y probar las aplicaciones comerciales críticas, cuando se cambian los sistemas de operación, para asegurar que no exista un impacto adverso sobre las operaciones organizacionales o en la seguridad. Asignar a un grupo o persona específica la responsabilidad de monitorear las vulnerabilidades, así como los parches y arreglos que lancen los vendedores.	
		Restricciones a los cambios en los paquetes de software	Limitar los cambios necesarios y controlarlos estrictamente. Utilizar los paquetes de software suministrados por vendedores sin modificaciones.	
		Fugas de Información	Considerar puntos para limitar la filtración de la información; por ejemplo, a través del uso y explotación de los canales encubiertos (covertchannels). Tomar medidas para protegerse contra códigos Troyanos reduce el riesgo de la explotación de los canales encubiertos.	
		Externalización del desarrollo de software	Supervisar y monitorear, el desarrollo del software abastecido externamente. Considerar puntos como contratos de licencias, propiedad de códigos, derechos de propiedad intelectual.	
12.6	Gestión de la vulnerabilidad técnica	Control de las vulnerabilidades técnicas	Obtener oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de información, la exposición de la organización a dichas vulnerabilidades evaluadas, y las medidas apropiadas tomadas para tratar los riesgos asociados. Un inventario actual y completo de los activos (ver 7.1) es un	Posible incapacidad para detectar problemas de seguridad en los sistemas y aplicaciones de la Institución. Posible incapacidad para tomar las medidas necesarias de contención, y responder oportunamente.

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
			prerrequisito para la gestión efectiva de la vulnerabilidad técnica. La información específica necesaria para apoyar la gestión de la vulnerabilidad técnica incluye al vendedor del software, números de la versión, estado actual del empleo (por ejemplo, cuál software está instalado en cuál sistema), y la(s) persona(s) dentro de la organización responsable(s) del software.	

DOMINIO 13.GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
13.1	Notificación de eventos y puntos débiles de seguridad de la información	Notificación de los eventos de seguridad de la información	Reportar a través de los canales gerenciales apropiados lo más rápidamente posible los eventos de seguridad de la información. Tomar la conducta correcta en el caso de un evento en la seguridad de la información; por ejemplo: No llevar a cabo ninguna acción por cuenta propia, sino reportar inmediatamente al punto de contacto.	Posible incapacidad para detectar problemas de seguridad en los sistemas y aplicaciones de la Institución. Incapacidad para tomar las medidas necesarias de contención, y responder oportunamente.
		Notificación de puntos débiles de seguridad	Requerir que todos los usuarios empleados, contratistas y terceros de los sistemas y servicios de información tomen nota y reporten cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios. El mecanismo de reporte debe ser fácil y estar disponible.	
13.2	Gestión de incidentes y mejoras de seguridad de la información	Responsabilidades y procedimientos	Establecer las responsabilidades y los procedimientos de la gerencia para asegurar una respuesta rápida, efectiva y metódica ante los incidentes de la seguridad de la información.	
		Aprendizaje de los incidentes de seguridad de la información	Establecer mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información. Analizar la información obtenida para identificar los incidentes recurrentes o de alto impacto.	
		Recopilación de evidencias	Recolectar, mantener y presentar evidencia para cumplir con las reglas de evidencia establecidas en la(s) jurisdicción(es) relevante(s). Desarrollar y seguir los procedimientos	

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
			internos cuando se recolecta y presenta evidencia para propósitos de una acción disciplinaria manejada dentro de una organización. Realizar en las copias del material de evidencia cualquier trabajo forense. Lo anterior aplica por ejemplo, para una acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (ya sea civil o criminal);	

4.3 Fases de desarrollo

La implementación de dicha guía debe incluir el desarrollo de objetivos, políticas, procesos y procedimientos, considerando las siguientes definiciones para su elaboración:

5. Tecnología, dimensionamiento y sus costos

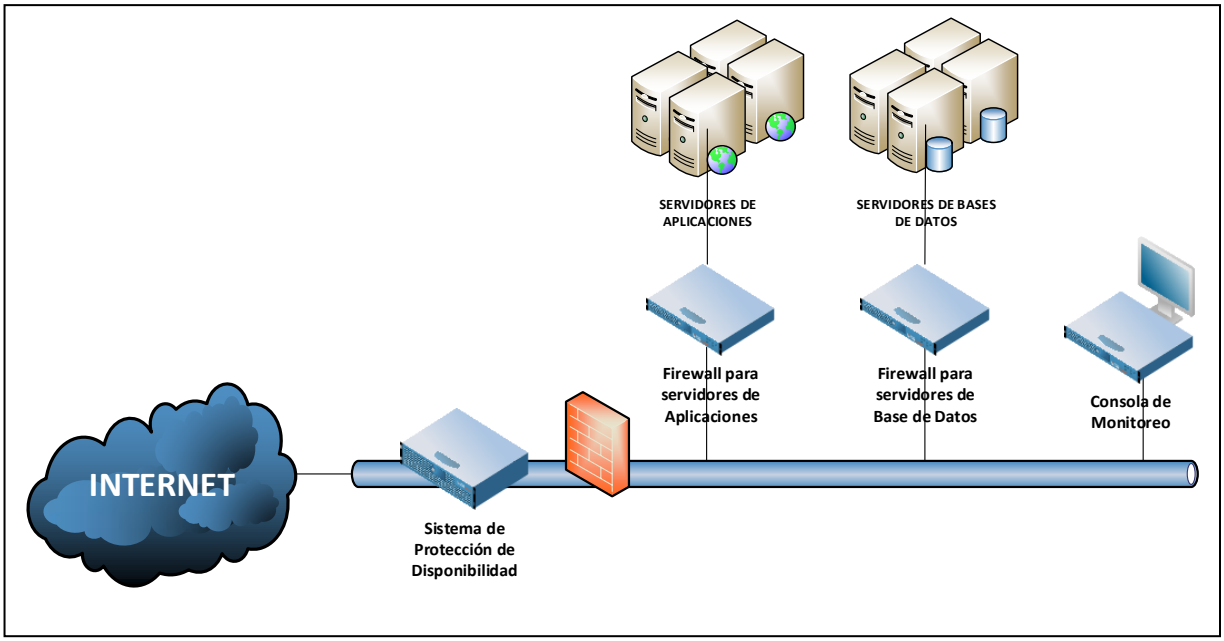
En general se recomienda que se adopten tecnologías para brindar seguridad en las siguientes áreas:

Esquemas de Seguridad	
Área	**Aplicativo / Software**
Escritorio	Antivirus, Antispyware, FireWall Personal IPS local, Filtro Web, Control de Acceso a Red, Dispositivos Móviles Control de Aplicaciones / Listas Blancas/Negras
Datos	Encripción de disco, Encripción de archivos, Control de Dispositivos Prevención de fuga de información local, Prevención de fuga de información en la red, Administración de permisos, Respaldo y Restauración, Almacenamiento Empresarial (SAN)
Servidor	Antivirus, Antispyware, FireWall local IPS local, Filtro Web, Control de Acceso a Red, Control de Aplicaciones / Listas Blancas/Negras, Virtualización
Red	Firewall perimetrales, Prevención de Intrusos, Firewall de Aplicaciones, Control de Acceso a Red, Análisis de Comportamiento, Análisis Forense, Control de Infraestructura.
Correo	Antispam, Antivirus, Prevención de Fuga de Información
Internet	Filtro de Contenidos, Proxy, Antivirus, Antimalware.
Riesgo y Cumplimiento	Manejador de Vulnerabilidades, Remediador de Vulnerabilidades, Auditoria de Políticas, Análisis y reporte de Riesgo, Control de Cambios, Monitor de Integridad de Archivos, SIEM, Manejador de Logs

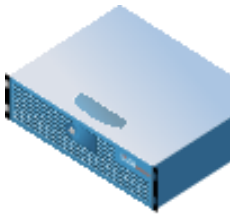
5.1 Casos prácticos

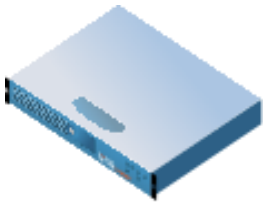
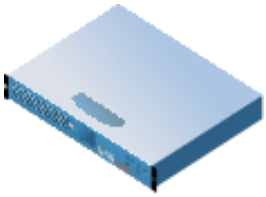
CASO 1

Esquema de seguridad:



ALTA SEGURIDAD - BENEFICIOS POR COMPONENTE:

 **Sistema de Protección de Disponibilidad**	• Protege, desde Internet, las aplicaciones de amenazas de seguridad, combinando en una defensa cohesiva diversos mecanismos de seguridad. • Con esta herramienta se evita que ataques maliciosos vulneren los sistemas y saturen los servidores con la finalidad de bloquear el servicio. • Ofrece actualizaciones para garantizar protección ante patrones de ataque y garantiza la disponibilidad de los servicios que se ofrecen en la organización.

 **Firewall para servidores de Aplicaciones**	• Ofrece el servicio de seguridad autoadaptable, sin saturar los servidores de aplicaciones, entregando una solución de alta seguridad que garantiza la integridad de la información y las aplicaciones web. • Con este componente es posible monitorear en tiempo real, la información que se transmite a través de las aplicaciones web. • Automáticamente aprende el comportamiento de las aplicaciones y de sus usuarios, detectando comportamientos anormales y alertando de ellos en tiempo real. • Identifica el tráfico que es originado por robots y Fuentes maliciosas conocidas, para detener ataques automatizados. • Previene fraudes vía web con su funcionalidad “ThreatRadarFraudPrevention”.
 **Firewall para servidores de Base de Datos**	• Protege a las Bases de Datos de ataques, pérdida y robo de información a través de un monitoreo en tiempo real con el cual, se emiten alertas y bloqueos de acceso basados en políticas de seguridad preestablecidas y que pueden ser configurables según nuestras necesidades. • Es posible controlar y monitorear quién tiene el acceso a las bases de datos y a la información que se accedió, teniendo pleno control de la consulta de la información. • Con este componente de infraestructura se protegerá uno de los recursos más valiosos de la Institución que es la información.
 **Consola de Monitoreo**	• La consola de monitoreo alerta de posibles ataques en cualquiera de los componentes de seguridad instalados y ofrece información detallada de las acciones realizadas en la detención de ataques. • Así mismo, recaba información forense de los intentos de ataque a la infraestructura resguardada.

No.	OBJETIVO DE CONTROL	PUNTOS CLAVE PARA DIMENSIONAMIENTO	TECNOLOGÍAS HW/SW	PRECIO
12.1	Requisitos de seguridad de los sistemas de información	Número de servidores Número de usuarios Número de direcciones IP	Herramientas de blindaje para sistema operativo Herramienta de Seguridad en Control de Cambios Herramientas de Pruebas de Penetración automatizada Herramienta Análisis de vulnerabilidades	(~520K USD)
12.2	Tratamiento correcto de las aplicaciones	Número de desarrolladores de aplicaciones Número de aplicaciones y tamaño de estas Número de direcciones IP	Servidores de aplicaciones Servidores de bases de datos Firewall para servidores de aplicaciones Firewall para servidores de bases de datos Consola de monitoreo Sistema de protección de disponibilidad	(~19,743,750USD)
12.3	Controles Criptográficos	Número de aplicaciones a integrar en el bus criptográfico ya sean legacy o de terceros. Número de sistemas que manejan certificados digitales SSL o llaves de SSH (F5, firewalls, BlueCoat, web, servidores, etc.)		

No.	OBJETIVO DE CONTROL	PUNTOS CLAVE PARA DIMENSIONAMIENTO	TECNOLOGÍAS HW/SW	PRECIO
12.4	Seguridad de los archivos de sistema	Número de aplicaciones, servidor(es) donde se encuentra instalada la base de datos, tamaño de la base de datos Número de base de datos, segmentos de red, número de sites Número de sistemas a integrar (Switches, Sistemas operativos, bases de datos, etc.) Número de servidores Unix o Windows Número de endpoints, Número de usuarios		
12.5	Seguridad en los procesos de desarrollo y soporte	Número de servidores virtuales y número de hypervisors Número de sistemas a integrar (Switches, Sistemas operativos, bases de datos, etc.) Número de endpoints, Número de salidas a Internet		
12.6	Gestión de la vulnerabilidad técnica	Número de direcciones IP		
13.1	Notificación de eventos y puntos débiles de seguridad de la información	Número de Segmentos de red Numero de bases de datos y transacciones por base de datos, Throughput Número de aplicaciones web Número de correo saliente en hora pico / Número y tamaño de los enlaces a Internet Período de retención, Número de enlaces de red, Número de dispositivos de red con sus eventos por		

No.	OBJETIVO DE CONTROL	PUNTOS CLAVE PARA DIMENSIONAMIENTO	TECNOLOGÍAS HW/SW	PRECIO
		segundo		
13.2	Gestión de incidentes y mejoras de seguridad de la información	Organigrama de la institución Período de retención, Número de enlaces de red, Número de dispositivos de red con sus eventos por segundo Número de administradores de servicios		

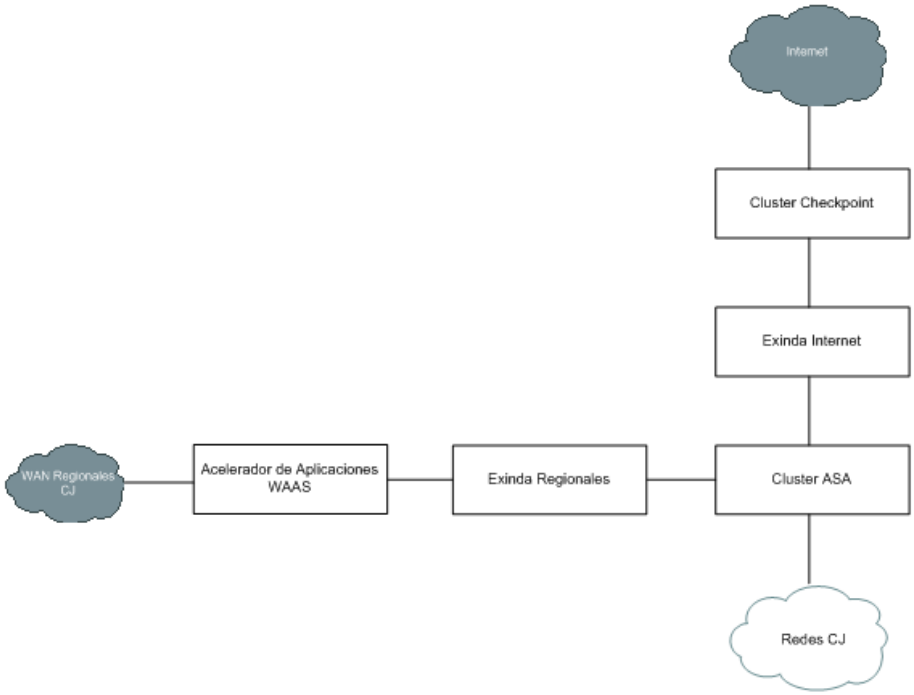
CASO 2

El caso de éxito más importante ha sido la implementación de un Data Center, en donde se centraliza todo el equipamiento y la aplicación de políticas de seguridad, de acuerdo a la recomendación de buenas prácticas, modelos y metodologías adoptadas en consultorías efectuadas para la implementación de la ISO 27000.
Se recomienda adoptar la estandarización de equipos en cada una de las regionales, lo que permite que las políticas sean de fácil aplicación, pues el manejo de protocolos comunes representa una gran ventaja.
Adicionalmente se debe implementar un Data Center Alterno de iguales características en otra regional, lo que permite la replicación de toda la información y garantiza la alta disponibilidad de todas las aplicaciones.
La inversión aproximada en equipamiento y Data Center ha sido de: USD 25'000.000

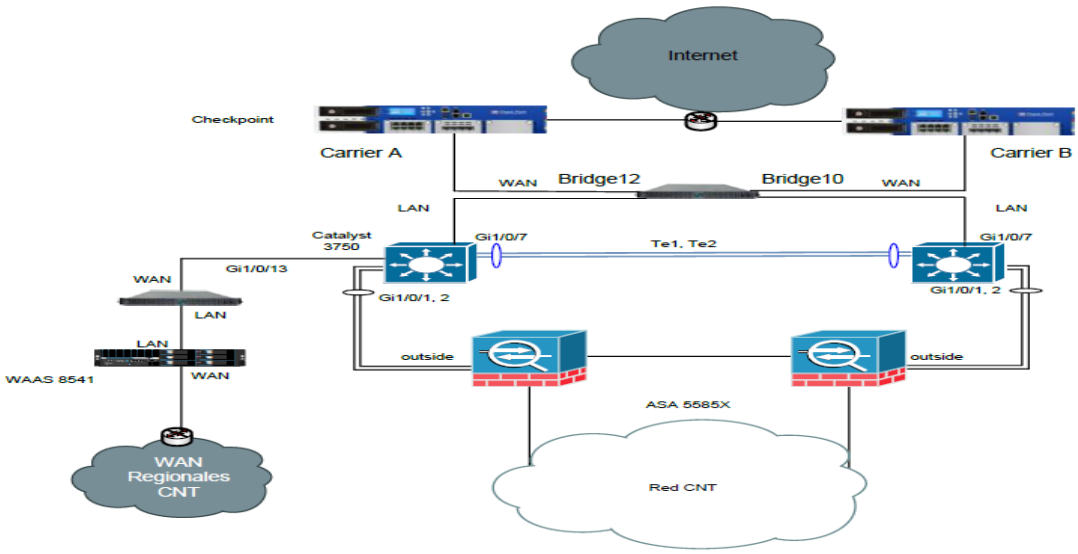
SISTEMA DE SEGURIDAD INFORMATICA

SEGURIDAD PERIMETRAL		
Seguridad de acceso web	Exinda	Administrador de ancho de banda
Seguridad de acceso web	Checkpoint	Filtrado Web
Seguridad de correo electrónico	IronPortmail - Cisco	Antispam
Seguridad de autenticación	ASA - Cisco	Firewall, IPS
Optimización de tráfico	Cisco- Wave	WASS - Acelerador de tráfico
Autenticación	Cisco - ACS	Autenticación activos equipos de red
Gestión de aplicaciones	Cisco- ACE	Balanceador de carga
SEGURIDAD INTERNA		
Acceso a servidores de aplicación	Cisco - VCG	Seguridad de acceso a aplicaciones en ambiente virtual
Antivirus	MacAfee	Protección antivirus
Protección de equipos	Microsoft - WSUS	Distribución de parches y actualizaciones
Protección de equipos	Red Hat-Satellite	Distribución de parches y actualizaciones
Protección de equipos de activos	Cisco - ACL	Configuración de funcionalidades de seguridad en equipos activos
Autenticación de usuarios	Microsoft- GPO Active Directory	Configuración de políticas de Grupo para la autenticación de usuarios en el directorio activo
Protección de red inalámbrica	Cisco - WirelessLanController	Configuración de grupos y niveles de seguridad para la autenticación de usuarios a la red inalámbrica, configurando las funcionalidades de la controladora a la que se anexan los accesspoint

TOPOLOGI SEGURIDAD DEL DATACENTER



ESQUEMA DE EQUIPAMIENTO SEGURIDAD DATACENTER



COSTOS APROXIMADOS

Los valores descritos a continuación son referenciales y están ligados a otras soluciones de tecnología informática, por ejemplo en los equipos activos adicionalmente a su funcionalidad de brindar los elementos de conectividad, permiten la configuración de políticas de seguridad como listas de acceso y calidad de servicio para el tráfico que pasa por la red como la telefonía IP.

SEGURIDAD	INVERSIÓN APROXIMADA
Equipamiento de seguridad perimetral	5'000.000,00
Licenciamiento antivirus	1´000.000,00
Consultorías de seguridad	500.000,00
Equipamiento activo y comunicaciones	18'000.000,00
Equipamiento para servidores para autenticación y políticas de seguridad	1'000.000,00

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.

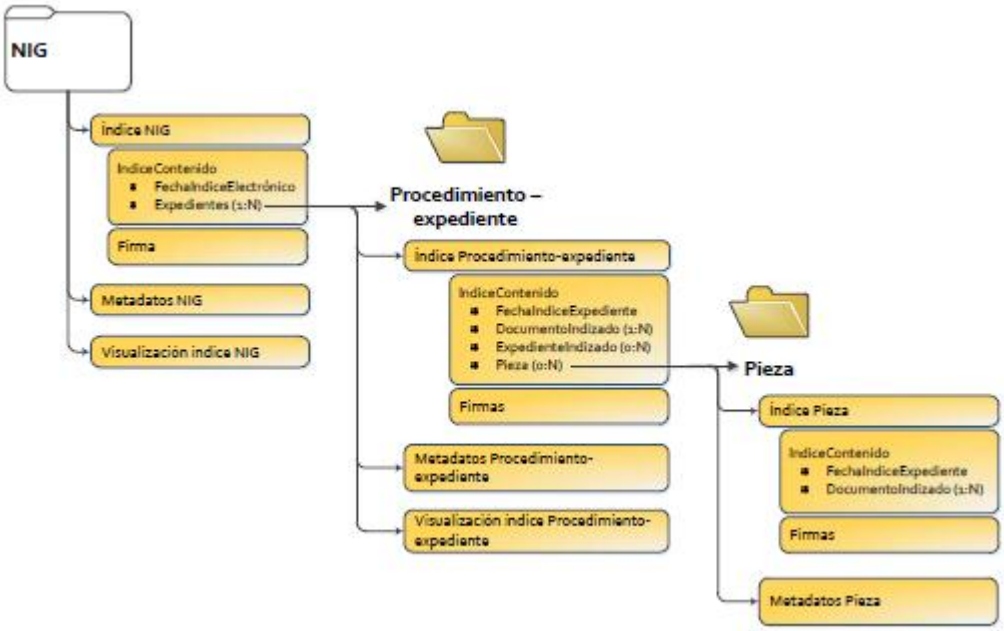
Los componentes de la capa técnica NIG son:

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:

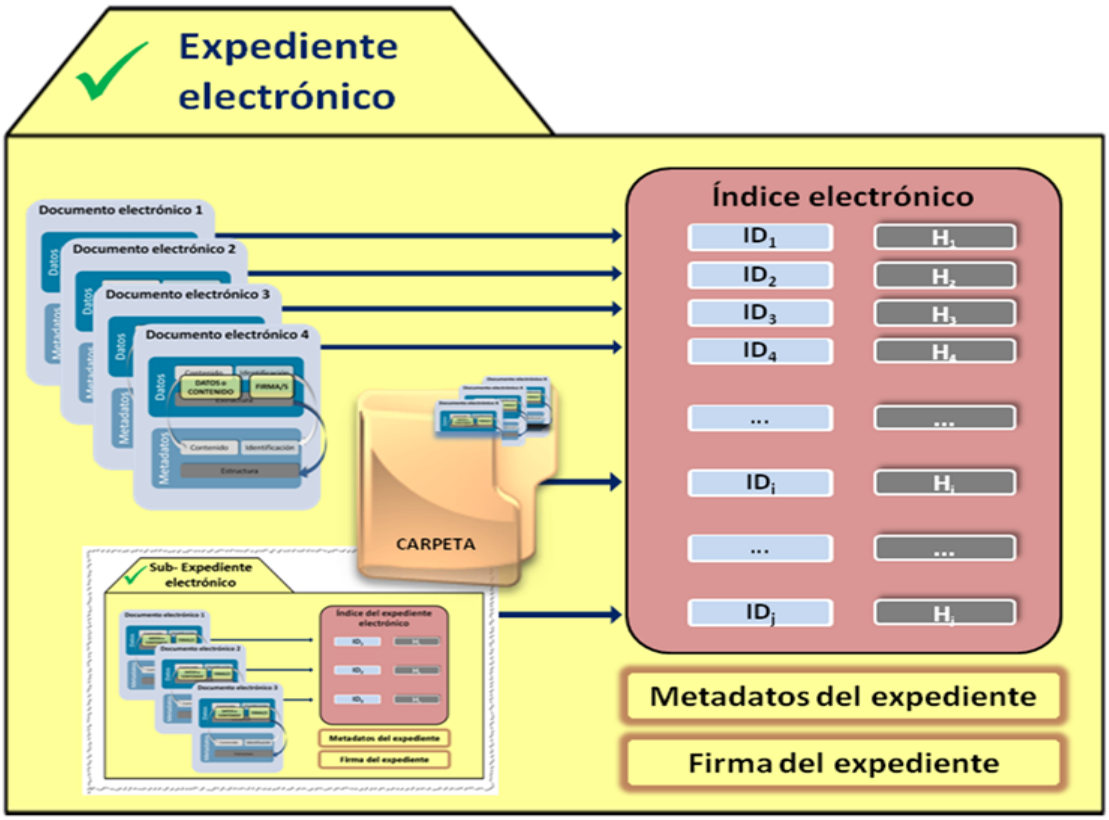
   a) El conjunto de *documentos electrónicos* correspondientes a un procedimiento judicial, que cumplirán con las características de estructura y formato establecidos en la Guía de Interoperabilidad y Seguridad del Documento Judicial Electrónico (ver Guía Documento Judicial Electrónico). Los documentos 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

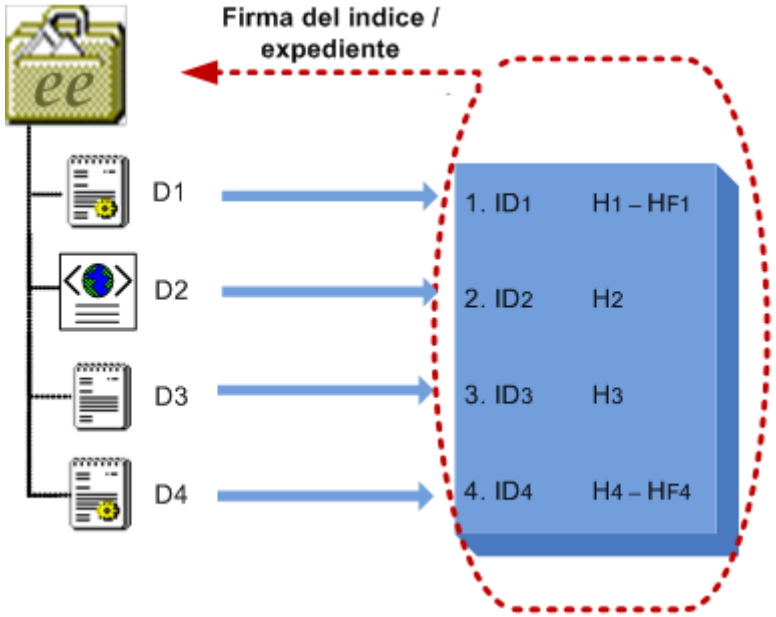
Componentes de la pieza.

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.

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 trasferencia se produzca.

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)/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 HH:MM:SS	<2011-03-12 10:32:15>	
Procedimientos_Expedientes	Listado de las referencias de todos los Procedimientos/Expedientes que forman parte de un NIG	1:N		<CodigoProcedimiento>: Código extraído de la tabla Tipos de Tramitación del Test de Compatibilidad del CGPJ, 3 caracteres + <NumeroProcedimiento>: Secuencial, 7 caracteres + <AnioProcedimiento> Año del procedimiento (Formato: yyyy), 4 caracteres	<MON> <0000088> <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.	1:N	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 - CAdES detached/explicit signature - TF05 - CAdES attached/implicit signature - TF06 - PAdES	<TF02>	
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	Si AGE: 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/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		

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		<4>	
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

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[6]	<000007>	
ProcedimientoExpedienteIndizado	Listado de cada uno de los procedimientos/expedientes que forman parte de este procedimiento/expediente	1:N		Indice procedimiento/expediente Metadatos procedimiento/expediente Visualización		Ver pestañas Indice 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		Indice pieza Metadatos pieza Visualizacion		Ver pestañas Indice Pieza y Metadatos Pieza para los metadatos y esquema de valores
ExpedienteAdminIndizado	Listado de cada uno de los expedientes administrativos que forman parte de este procedimiento/expediente	1:N		Indice expediente administrativo Metadatos expediente administrativo Visualizacion		Ver NTI de Expediente Electrónico
Firmas						
Firma						
TipoFirma	Indica el tipo de firma electrónica que firma el 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 Ley18/2011. Codificación: - TF01 - CSV - TF02 - XAdES Internally detached signature - TF03 - XAdES Enveloped signature - TF04 - CAdES detached/explicit signature - TF05 - CAdES attached/implicit signature - TF06 - PAdES		
ContenidoFirma						
CSV						
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 AGE: 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/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		

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			
NIG	Número de Identificación General	1	Cadena de caracteres (19 caracteres)	Codificación establecida por el CGPJ	<090594212010050102l>	<Código de municipio>: Codificación extraída de la tabla Municipios del Test de Compatibilidad del CGPJ (longitud: 5 caracteres). <Tipo de órgano>: Codificación extraída de la tabla Tipos de Órgano del Test de Compatibilidad del CGPJ (longitud: 2 caracteres). <Orden jurisdiccional>: Codificación extraída de la tabla Jurisdicciones del Test de Compatibilidad del CGPJ (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 CGPJ	<0905942001>	
FechasProcedimientoExpediente	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: <codigo Procedimiento> (3 dígitos) <numero 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 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
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				
PersonaId	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	<D>	
Identificacion	Identificador dependiendo del valor del tipo de identificación seleccionado	1	Cadena de caracteres	String	<12345678Z>	
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 CGPJ	<818>	
Sexo	Sexo de la persona	1	Cadena de caracteres	Código extraído de la tabla Tipos de Sexo del Test de Compatibilidad del CGPJ	<H>	
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>	
Representacion	Información de representación procesal y defensa	0: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>	
PersonaId	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	<Español>	
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				
PersonaId	Identificación como persona física o jurídica. Ver los metadatos del tipo complejo PersonaId	1	Cadena de caracteres	<TipoIdentificacion> + <Identificacion>	<N> + <12345678Z>	
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				
PersonaId	Identificación de persona. Ver los metadatos del tipo complejo PersonaId	1	Cadena de caracteres	<TipoIdentificacion> + <Identificacion>	<N> + <12345678Z>	
PersonaFisica	Datos de la persona física. Ver los metadatos del tipo complejo PersonaFisica	1	Cadena de caracteres	<Nombre> + <PrimerApellido> + <SegundoApellido> + <Nacionalidad> + <Sexo>	<Alberto> + <López> + <Pérez> + <ESP> + <H>	
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 perteneciente 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>	
DocumentoIndizado	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 2 - 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 Ley18/2011. Codificación: - TF01 - CSV - TF02 - XAdES Internally detached signature - TF03 - XAdES Enveloped signature - TF04 - CAdES detached/explicit signature - TF05 - CAdES attached/implicit signature - TF06 - PAdES	<TF01>	
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	Si AGE: 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/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		

EJEMPLO DE METADATOS DE LA PIEZA

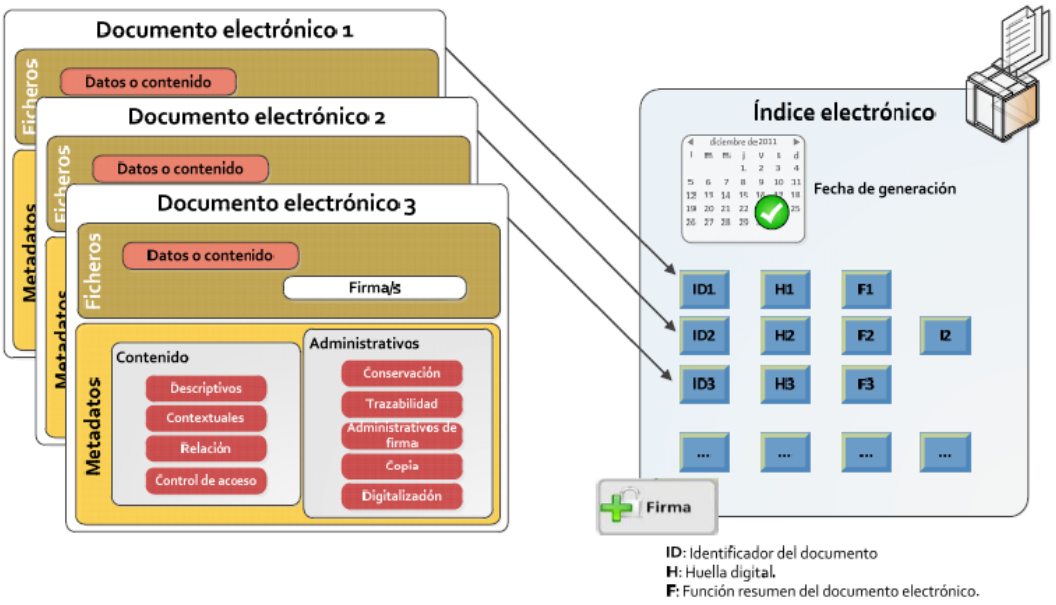
Metadato	Descripción/Condiciones de uso	Cardinalidad	Tipo	Esquema de valores	Ejemplo	Observaciones
VersionGIS	Identificador normalizado de la versión de la Guía de Interoperabilidad y Seguridad del Expediente Judicial Electrónico	1	URI	N/A		
NIG	Número de Identificación General	1	Cadena de caracteres		<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>	
FechasPieza	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) <numero Procedimiento> (7 dígitos) <año Procedimiento> (4 dígitos) La pieza se encuentra compuesta por : <codigoPieza>(3 dígitos) <numero Pieza> (7 dígitos) <año Pieza> (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	Subindice que identifica la pieza dentro del procedimiento/expediente	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				
PersonaId	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	<D>	
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	<12345678Z>	
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 CGPJ	<818>	
Sexo	Sexo de la persona	1	Cadena de caracteres	Código extraído de la tabla Tipos de Sexo del Test de Compatibilidad del CGPJ	<H>	
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>	

Representacion	Información de representación procesal y defensa	0: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>	
PersonaId	Identificación como persona física	0	Cadena de caracteres	<TipoIdentificacion> + <Identificacion>	<N> + <12345678Z>	
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>	
RepresentanteAdmon	Información de representante en caso de ser un profesional de la Administración contemplado por tipo de representación	1				
PersonaId	Identificación como persona física o jurídica. Ver los metadatos del tipo complejo PersonaId	1	Cadena de caracteres	<TipoIdentificacion> + <Identificacion>	<N> + <12345678Z>	
Nombre	Nombre de pila	0	Cadena de caracteres	String	<Alberto>	
PrimerApellido	Primer apellido	0	Cadena de caracteres	String	<López>	
SegundoApellido	Segundo apellido	0	Cadena de caracteres	String	<Pérez>	
RepresentanteLegal	Información de representante en caso de no ser ninguno de los anteriores casos	1				
PersonaId	Identificación de persona. Ver los metadatos del tipo complejo PersonaId	1	Cadena de caracteres	<TipoIdentificacion> + <Identificacion>	<N> + <12345678Z>	
PersonaFisica	Datos de la persona física. Ver los metadatos del tipo complejo PersonaFisica	1	Cadena de caracteres	<Nombre> + <PrimerApellido> + <SegundoApellido> + <Nacionalidad> + <Sexo>	<Alberto> + <López> + <Pérez> + <ESP> + <H>	
PersonaJuridica	Datos de la persona jurídica. Ver los metadatos del tipo complejo PersonaJuridica	1	Cadena de caracteres	<Nombre de la entidad>	<NombreEntidad S.A.>	

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:

a) Contenido, entendido como conjunto de datos o información del documento.

b) Firma electrónica reconocida de acuerdo con lo que establece la sección segunda, capítulo II, Título III.

c) 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						
DatosXML	Contenido en formato XML. En caso de datos XML cuya codificación difiera de la de esta estructura raíz 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	Extraído 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>	<28003> + <13> + <1> + <000000000005> + <2011>	Codificación del identificador del documento: <Código de población>: Codificación extraída de la tabla Municipios del Test de Compatibilidad del CGPJ (longitud: 5 caracteres). <Tipo de órgano>: Codificación extraída de la tabla Tipos de Órgano del Test de Compatibilidad del CGPJ (longitud: 2 caracteres). <Orden jurisdiccional>: Codificación extraída de la tabla Jurisdicciones del Test de Compatibilidad del CGPJ (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).
NIG	Número de Identificación General	1	Cadena de caracteres (19 caracteres)	Codificación establecida por el CGPJ	<090894212010050102 1>	<Código de municipio>: Codificación extraída de la tabla Municipios del Test de Compatibilidad del CGPJ (longitud: 5 caracteres). <Tipo de órgano>: Codificación extraída de la tabla Tipos de Órgano del Test de Compatibilidad del CGPJ (longitud: 2 caracteres). <Orden jurisdiccional>: Codificación extraída de la tabla Jurisdicciones del Test de Compatibilidad del CGPJ (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			
CodigoJurisdiccion	Código de la jurisdicción a la que pertenece el documento	1	Cadena de caracteres		<2>	
CodigoEspecialidad	Código de la especialidad a la que pertenece el documento	1	Cadena de caracteres		<113>	
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					
CodigoProcedimiento	Código del procedimiento	1	Cadena de caracteres		<MON>	3 caracteres
NumeroProcedimiento	Número del procedimiento	1	Cadena de caracteres	Secuencial	<0000001>	7 caracteres
AnioProcedimiento	Año del procedimiento	1	Cadena de caracteres	Año del procedimiento (Formato: yyyy)	<2011>	4 caracteres
CodigoPieza	Código de la pieza	0	Cadena de caracteres			
NumeroPieza	Número de la pieza	0	Cadena de caracteres	Secuencial	<0000002>	7 caracteres
AnioPieza	Año de la pieza	0	Cadena de caracteres	Año de la pieza (Formato: yyyy)	<2011>	4 caracteres
SubindicePieza	Subíndice que identifica la pieza dentro del procedimiento	0	Cadena de caracteres			
OrganoJudicial	Órgano judicial que está conociendo del procedimiento judicial electrónico	1	Cadena de caracteres		<0301437920>	

TipologiaElectronica	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: AAAA-MM-DD 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>	
OrigenCiudadanoAdministracionOrganoJudicial	Indica la condición particular o profesional del emisor del documento	1	Cadena de caracteres	T001 - Interviniente 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						
ValorNaturalezaDocumento	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 28.3) - Copia electrónica auténtica parcial - Otros: LEC	1	Cadena de caracteres	EE01 - Original. EE02 - Copia electrónica auténtica con cambio de formato. EE03 - Copia electrónica auténtica de documento papel. EE04 - Imagen electrónica aportada por el ciudadano. EE05 - Copia electrónica parcial auténtica. EE99 - Otros.	<EE01>	
IdentificadorDocumentoOrigen	Identificador normalizado del documento origen al que corresponde la copia	0	Cadena de caracteres			
SecretoActuacion	Indica si se ha acordado el 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 - Si	<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 o pieza	1	Cadena de caracteres	String[6]	<000009>	

MetadatosDocumentoENI			0			
VersionNTI	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_<Órgano>_<AAAA>_<ID_especifico>	<ES_E00010207_2010_MPR000000000000000000010207>	<Órgano>:9 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 órgano/unidad/oficina 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: AAAA-MM-DD 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	Booleano	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> + [Si 'Estado de elaboración' = EE02 ó EE04] + <IdentificadorDocumentoOrigen>	<EE02> + <ES_E00010207_2010_MPR000000000000000000010207>	EE01 - Original (Ley 11/2007 Art. 30) EE02 - Copia electrónica auténtica con cambio de formato (Ley 11/2007 Art.30.1) EE03 - Copia electrónica auténtica de documento papel (Ley 11/2007 Art.30.2 y 30.3) EE04 - Copia electrónica parcial auténtica EE99 - Otros
TipoDocumental	Descripción del tipo documental del documento	1	Cadena de caracteres	- TD01 - Resolución. - TD02 - Acuerdo. - TD03 - Contrato. - TD04 - Convenio. - TD05 - Declaración. /*Documentos de transmisión*/ - TD06 - Comunicación. - TD07 - Notificación. - TD08 - Publicación. - TD09 - Acuse de recibo. /*Documentos de constancia*/ - TD10 - Acta. - TD11 - Certificado. - TD12 - Diligencia. /*Documentos de juicio*/ - TD13 - Informe. /*Documentos de ciudadano*/ - TD14 - Solicitud. - TD15 - Denuncia. - TD16 - Alegación. - TD17 - Recursos. - TD18 - Comunicación ciudadano. - TD19 - Factura. - TD20 - Otros incautados. /*Otros*/ - TD99 - Otros.	<TD02>	
Firmas		Existirá, al menos, una firma del contenido del índice del documento 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	1:N	Cadena de caracteres	CSV y formatos de firma electrónica definidos en la Ley18/2011. Codificación: - TF01 - CSV - TF02 - XAdES Internally detached signature - TF03 - XAdES Enveloped signature - TF04 - CAdES detached/explicit signature - TF05 - CAdES attached/implicit signature - TF06 - PAdES		<TF02>
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	Si AGE: Referencia BOE:BOE-A-YYYY-XXXXX En otro caso, referencia correspondiente		
FirmaConCertificado						
FirmaBase64	Firma en formato base64	1		base64Binary		
dsSignature	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		

DOCUMENTO REPORTE DE ACTIVIDAD

1. Nombre del grupo de trabajo:

Respuesta: **Tecnologías de los Poderes Judiciales**

2. Grupo presencial / no presencial en Colombia

Respuesta: Presencial

3. Resumen de la actividad realizada (indique brevemente cómo se ha desarrollado la actividad en la mesa, en el caso de ser un grupo presencial; o por otros medios en caso contrario):

Respuesta: Grupo de trabajo Presencial

1.-Dra. Paola Prado, Auditora en representación de la Presidencia del Consejo de la Magistratura, Argentina, paola.prado@pjn.gov.ar, paoprado@hotmail.com

2.-Mauricio Rodríguez, Jefe del Departamento de Informática de la Corporación de Administrativa del Poder Judicial de Chile, mrodriguez@pjud.cl

3.-Patricia Bonilla Rodríguez, Asistente Coordinador Cumbre Judicial, Costa Rica, pbonilla@poder-judicial.go.cr (mediante videoconferencia)

4.-José Suing, Juez Nacional, Ecuador, jdsuing@gmail.com

5.- Maria del Mar Martinez Sanchez, Jefe del área de Informatica Judicial de Consejo General del Poder Judicial, España, mar.martinezsanchez@cgpj.es, juancarlos.garces@cgpj.es

6.-Juan J. García M., Director de Tecnologías de la Información, México, jjgarciam@correo.cjf.gob.mx

7.- José Xavier Luna Gaitán, Director de Informática Jurídica y Tesauro, Nicaragua, jxavier.lunag@gmail.com,jxavier.lunag@poderjudicial.gob.ni

8.- Luis Guillermo Rivas, Magistrado Corte Suprema de Justicia Sala I, Costa Rica, lgrivas@poder-judicial.go.cr

9.- Carlos Fernando Galindo, Director Unidad de Informatica, Direccion Ejecutiva de Administracion Judicial, Consejo Superior de la Judicatura, Colombia , cgalindc@deaj.ramajudicial.gov.co

10.- Hernando Castillo García, Profesional Universitario Informatica, Unidad de Informatica, Direccion Ejecutiva de Administracion Judicial, Consejo Superior de la Judicatura, Colombia, hcastilg@deaj.ramajudicial.gov.co

12.- Cesar Chaparro Rincón, Magistrado Auxiliar, Sala Administrativa, Consejo Superior de la Judicatura, Colombia, cchaparr@consejosuperior.ramajudicial.gov.co

13.-Francisco Boada, Magistrado Auxiliar, Sala Administrativa, Consejo Superior de la Judicatura, Colombia, fboadaconsejosuperior@gmail.com

14.-Luis Eduardo Yepes Gómez, Profesional Especializado, Unidad de Informatica, Direccion Ejecutiva de Administracion Judicial, Consejo Superior de la Judicatura, Colombia, lyepesg@deaj.ramajudicial.gov.co - leysoft@yahoo.com

15.- Paola Andrea Alzate Lozano, Profesional Especializado, Sala Administrativa, Consejo Superior de la Judicatura, Colombia, palzatel@cendoj.ramajudicial.gov.co

16.- Diana Torrez Ortíz, Jefe de División de Informática y Comunicaciones -CENDOJ, Consejo Superior de la Judicatura, Colombia, dtorrezo@cendoj.ramajudicial.gov.co

17.- Ronald Figueroa, Director de Informatica, Guatemala, refigueroa@oj.gob.gt (mediante videoconferencia)

18.- Wilma Mamani Cruz, Consejera, Bolivia, wilmajamas@hotmail.com

19.- Kattia Morales Navarro, Jefe área de Informática de gestión, Costa Rica, kmorales@poder-judicial.go.cr (mediante videoconferencia)

Se realizaron las siguientes actividades:

1. Avances en los proyectos tecnológicos
2. Presentación del Sistema Informático SIRUT
3. Análisis de mejoras del Sistema Informático SIRUT
4. Comentarios y diagnóstico del avances en el resto de los proyectos
5. Revisión del protocolo de uso del Sistema Informático SIRUT
6. Plan de trabajo en los proyectos tecnológicos:
    6.1 Sistema Informático SIRUT

6.2 Innovación

- Interoperabilidad Técnica

- Seguridad Informática

- Expediente digital, Modelo Funcional

6.3. Difusión

- Apartado de Tecnologías en la revista de Cumbre de forma permanente

- Presencia en las redes sociales

- Alertas y avisos automáticos de nuevos eventos en el SIRUT

4. Metodología de trabajo establecida para el desarrollo del proyecto (haga una breve exposición de la metodología de trabajo que se ha previsto para alcanzar los resultados previstos para el proyecto):

Respuesta: Se dividió el proyecto de tecnologías del Poder Judicial en dos subproyectos principales a modo de facilitar el desarrollo, con una visión integradora; los subproyectos y sus responsables son:

1.- Sistema Informático SRUIT (Cartera de proyecto, Brecha tecnológica, Red videoconferencia, mapa tecnológico) (Nicaragua, Paraguay, Chile y Costa Rica)

2.- Innovación Tecnológica

- Expediente Digital, Modelo Funcional (Lidera Colombia, Chile, Costa Rica).

- Interoperabilidad Técnica (Lidera España, Colombia, Argentina, Nicaragua).

- Seguridad Informática (Bolivia, México, Ecuador y Lidera Guatemala)

3.- Difusión (Lidera Guatemala, Ecuador, Nicaragua)

- Apartado de Tecnologías en la revista de Cumbre de forma permanente

- Presencia en las redes sociales

- Alertas y avisos automáticos de nuevos eventos en el SIRUT

Se anexó el subproyecto de Cooperación Jurídica Judicial al subproyecto de Innovación (Interoperabilidad)

No obstante la difusión se considera transversal en todos los proyectos, los grupos se comprometen a participar suministrando información al grupo de difusión.

Los grupos de trabajo conformados por lo subproyectos definen los objetivos específicos, actividades, plan de trabajo, cronograma, con el propósito de obtener los productos respectivos para la Segunda Reunión Preparatoria a efectuarse en Santa Cruz de la Sierra, Bolivia . Se establece que el seguimiento de las actividades se realice utilizando los medios tecnológicos disponibles en los Poderes Judiciales (videoconferencia, correo electrónico, foros, etc.)

5. Plan de trabajo acordado hasta la Segunda Reunión Preparatoria

Respuesta: Se acordaron los planes de trabajo los cuales se adjunta teniendo como objetivo los productos entregables para la Segunda Reunión Preparatoria a efectuarse en Santa Cruz de la Sierra, Bolivia .

6. Resultados alcanzados (exponga brevemente los principales resultados alcanzados para su grupo de trabajo en esta ronda de talleres)

Respuesta:

En el Proyecto Sistema Informático SIRUT se realizaron los siguientes avances :

- Elaboración de la encuesta tecnológica

- Aplicación de la encuesta en los países que conforman la Mesa de Tecnología (contestaron Costa Rica, Nicaragua, Chile, Argentina, Mexico, España, Ecuador y Honduras.

- Desarrollo del Sistema Informático "SRUIT", Sistema Repositorio Único de Información Tecnológica, que permite realizar la administración de encuestas y proyectos, repositorio documental, administración de contactos de los lideres tecnologícos, administración de usuarios, publicación de informes y consultas.

- Elaboración del Protocolo de Administracion y uso del Sistema Informático SIRUT

- Integración de los proyectos históricos de CJI

En los Proyectos de Innovación:

-Recopilación de información

- Videoconferencia con especialista en tecnologías de los Poderes Judiciales (13 países)

- Primera versión de la Guía Técnica de Interoperabilidad

7. **Desviaciones importantes del proyecto original (si han propuesto desviaciones importantes respecto de los objetivos o resultados del proyecto original, por favor indíquelas y razone los motivos de las mismas)**

   Respuesta: No aplica.

8. **Documentos de trabajo que se adjuntan: (por favor haga una relación de los documentos de trabajo resultantes de esta ronda y que son entregados en formato digital a la Secretaría Permanente; así como incluidos en la web de Cumbre, página correspondiente a los grupos de trabajo http://www.cumbrejudicial.org/web/guest/xviiedicion/grupos)**

   Respuesta: Plan de trabajo para Innovacion-seguridad Informatica.xls, Plan de trabajo para Innovacion-Interoperabilidad.xls, Plan de trabajo para Innovacion-Expediente Electronico.xls, Plan de trabajo para sistema informatico SIRUT.xls, Plan de trabajo para difusion.xls, Protocolo de uso del Sistema informatico.doc

9. **Sugerencias para la segunda reunión preparatoria**

   Respuesta:

   - Instar la participación de los países de la cumbre en la respuesta al llenado de la encuesta tecnológica a través del Sistema Informático SIRUT.

   - Que los proyectos ya definidos continúen en la siguiente Cumbre, toda vez que su desarrollo implica un ciclo de vida mayor que el de la XVII Cumbre.

   Conclusiones:

   - Para una Justicia de Futuro: planificada, integrada y tecnológicamente desarrollada se requiere del uso de las TICs para mejorar la eficiencia, la eficacia y efectividad de la función jurisdiccional, con el propósito de obtener que esta sea pronta y de excelencia para garantizar el derecho fundamental de acceso a la Justicia.

   - El grupo de Tecnología de la Información se pone a disposición de los otros grupos de la CJI con el fin de proporcionar asesoría en aspectos tecnológicos.

   - Se reitera la necesidad de contar con el apoyo de todos los titulares de tecnología de la información de los países miembros con los trabajos de la CJI.

   - Se propone que en lo sucesivo se establezca la coordinación entre los grupos de trabajo con el objeto que salga un proyecto unificado de Cumbre, dado que las TICs son transversales a todos los proyectos para que puedan tener un eficiente desarrollo.

- Colombia se incorpora activamente a la mesa de Tecnología de los Poderes Judiciales.

Se agradece a los profesionales del Consejo Superior de la Judicatura y de la Corte Suprema de Justicia de Colombia por el apoyo recibido en la Mesa de Tecnología de los Poderes Judiciales, destacando el compromiso, profesionalismo, soporte técnico y acompañamiento durante la segunda ronda de Talleres en Colombia.