

3. Módulo 3. Sistemas y herramientas informáticas

3.1. Documento electrónico y firma digital

- a. En este punto usted encontrará un **video** introductorio sobre Firma Digital

[Link a descargar como parte del material de estudio](#)

Ver Video (click aquí): [La Firma Digital en Argentina](#)



- b. Ver: Preguntas Frecuentes

[Link a descargar como parte del material de estudio](#)

[Preguntas Frecuentes.pdf](#)

- c. Ver: **Manual de firma digital** actualizado del Ministerio de Justicia y Derecho Humanos de la Nación.

[Link a descargar como parte del material de estudio](#)

[Manual de Firma Digital.pdf](#)

3.2. Ingreso de causas y escritos: Mesa de Entradas de Escritos Digitales (MEED) y Portal de Gestión de Causas Judiciales

En la actualidad, en el Poder Judicial conviven 2 sistemas que tienen la misma finalidad, interactuar con abogados y ciudadanos: la MEED y el Portal de Gestión de causas judiciales.

3.2.1. MeeD (Mesa de Entradas de Escritos Digitales)

MeeD es un sistema para la recepción de escritos digitales, que permite subir documentos para realizar distintos tipos de presentaciones en cualquiera de los fueros del Poder Judicial de Mendoza.

El sitio para ingresar a la Mesa de Entradas de Escritos Digitales es:

<http://www.ius.mendoza.gov.ar/meed>

Tutoriales

1. Registro de usuarios al Sistema MEED

<https://youtu.be/s7GQ3ssjmxU>

2. Nueva metodología de carga - Video Tutorial - SISTEMA MEED

<https://youtu.be/XfwSFGNzfDw>

3. Instructivos, Preguntas frecuentes y Reclamos
Ver Instructivo MEED - MEC

[Link a descargar como parte del material de estudio](#)



[Instructivo MEEC.pdf](#)

[Instructivo MEED.pdf](#)

3.2.2. Portal de Gestión de Causas Judiciales

Es el sistema disponible en Internet que utilizan ciudadanos y profesionales para interactuar con los expedientes judiciales.

El sitio para ingresar al Portal es:

<http://www.jus.mendoza.gov.ar/portal-de-gestion-de-causas-judiciales>

Usted deberá ver los siguientes videos o instructivos:

- a. Tutorial registraci3n del usuario:

https://youtu.be/iHZalfU_Uck

- b. Presentar escritos:

<https://youtu.be/avC5rh32Qbc>

- c. Listado de escritos presentados:

<https://youtu.be/qZWbCZN3ulo>

3.3. Gest3n de expedientes o legajos

En el Poder Judicial de Mendoza cuenta con sistemas inform3ticos a los fines de la gesti3n en el 3mbito jurisdiccional, es decir Juzgados, Tribunales, C3maras y Tribunales de gesti3n. Se utilizan m3s de un sistema, dependiendo del tipo de organismo de que se trate. Con ellos se gestionan los expedientes o legajos, que actualmente en su mayor3a son digitales.

3.3.1. IURIX ADF

Este sistema es utilizado por los Juzgados Civiles, de Paz, Tributarios, Concursales, C3maras Civiles y Laborales, y las dos salas de la Suprema Corte de Justicia. Adem3s, lo utilizan en algunos organismos del Ministerio P3blico Fiscal y del Ministerio P3blico de la Defensa.

El proceso de implementación comenzó en el año 2013, restando a la fecha algunos organismos.

Usted deberá visualizar los siguientes videos que se encuentran detallados a continuación:

INTRODUCCIÓN

1. Introducción al Sistema IURIX

<https://youtu.be/KExzad66GqY>

2. Inicio de sesión en IURIX

<https://youtu.be/SrAy5d6rFxE>

3. Ficha del expediente

https://youtu.be/p64MQOZnL_M

4. Búsqueda simple de expedientes

<https://youtu.be/Y2JPkEB9zq8>

REGISTRACIÓN

5. Inicio de expedientes con Mesa Central

<https://youtu.be/Byqz-TW53pg>

6. Ingresos nuevos

<https://youtu.be/EFc55swXrCY>

CARGOS

7. Cargo individual

<https://youtu.be/sOV3K5IGCxc>

8. Agregar escrito suelto

<https://youtu.be/Y5CGWKpQBvY>



9. Buscar. Editar. Eliminar cargos.

<https://youtu.be/89RrH0kAIU0>

MOVIMIENTOS

10. Movimientos internos

<https://youtu.be/1uE1ocpl4LI>

11. Pase interno

<https://youtu.be/bDYuMtlS8zc>

12. Remisión de expedientes

<https://youtu.be/tt8NYEYkWBo>

13. Movimientos externos

<https://youtu.be/JMab8jcPFFU>

ACTUACIONES

14. Catálogo documental

<https://youtu.be/BEYrAtwOpJo>

15. Nueva actuación

<https://youtu.be/Hon0u836UW0>

16. Estado de Actuaciones y Edición

<https://youtu.be/YzVmBDtjGeQ>

17. Adjuntar documentación en actuación

<https://youtu.be/RcKtnc3koKo>

18. Bandeja Escritos para Proveer

<https://youtu.be/EEs3vP7yEvI>

DESTACADAS

19. Expediente Privado

<https://youtu.be/PuL99lqChgg>

20. Expediente Urgente

<https://youtu.be/Zjcwqb4h3KE>

3.3.2. IURIX Flex

El sistema Iurix Flex se utiliza desde abril de 2021 en la Suprema Corte de Justicia de Mendoza para la gestión de expedientes digitales en el fuero de Familia. El sistema de gestión Iurix Flex permite la tramitación de los expedientes en primera (Juzgados y GEJUAF) y en segunda instancia (Cámara de Apelaciones de Familia). También está en funcionamiento en las dependencias con las que se interactúa C.A.I (cuerpo auxiliar interdisciplinario), Asesorías de niñas, niños y adolescentes; y la Fiscalía Civil.

El sistema de gestión Iurix Flex, gestión de expediente digital, se aplicó en el GEJUAF de Luján de Cuyo (Gestión Judicial Asociada de Familia) como piloto y gradualmente se replicó al resto de los GEJUAF y Cámara de Apelación de Familia.

Usted deberá leer los documentos que se encuentran adjuntos y bajo el siguiente nombre:
IURIX FLEX - Manuales e instructivos:

[Link a descargar como parte del material de estudio](#)

1. [Manual de uso del Sistema IURIX FLEX.pdf](#)

2. Instructivos IURIX FLEX:

[Generación de una actuación privada.pdf](#)

[Gestión de escritos y expedientes urgentes.pdf](#)

[Proveer escritos sueltos.pdf](#)

[Generación de una compulsas.pdf](#)

[▶ Registración de múltiples representantes legales.pdf](#)

[▶ Remisión de un expediente a lista diaria con movimiento posterior.pdf](#)

3.3.3. LED - Sistema Legajo Digital (LED) Penal:

A fin de cumplir con el artículo 85 de la ley 9040 que establece que “Todas las normas del Código Procesal Penal de la Provincia de Mendoza, deberán ser interpretadas en beneficio de lo dispuesto por la presente ley, asegurando la metodología de la audiencia oral, la registración en soporte digital, las notificaciones electrónicas, en lugar del procedimiento escrito y los expedientes”, en agosto del año 2020 la Suprema Corte de Justicia implementó el sistema Led Penal – Legajo Digital –, para el Fuero Penal Colegiado en todas las circunscripciones judiciales de la provincia.

Este sistema de desarrollo propio del Poder Judicial logró la despapelización del fuero penal, al permitir que todas las causas sean tramitadas en forma electrónica, a través de legajos digitales que reemplazan completamente al expediente papel, así como también la asignación interna de tareas al personal, permitiendo la trazabilidad de las mismas. A su vez, este sistema interopera con la actual agenda electrónica de audiencias penales.

Este sistema cuenta con un módulo local, al que solamente pueden acceder los usuarios autenticados del fuero penal, como así también un módulo de consulta externa para los abogados matriculados.

El sistema Legajo Digital (LED), se caracteriza por:

- ▶ Despapelización total para la tramitación de expedientes reemplazando de esa manera al expediente papel.
- ▶ La digitalización de las actuaciones permite incorporar en el mismo legajo digital las registraciones audiovisuales de las audiencias y así amalgamar el registro de las audiencias orales con las actuaciones escritas y poder acceder a ellas en forma eficiente.
- ▶ El acceso rápido y eficaz a la información por parte de actores internos y externos (Partes).

▶ Permite la gestión interna de tareas dentro de cada OGAP, y presenta pantallas de inicio con información personalizada y funcionalidades que se adecuan al rol que cumple el usuario: juez, administrador, funcionario, auxiliar.

Usted deberá ver los videos siguientes:

1- Ingreso al Sistema LED:

<https://youtu.be/oz73vz9bn2M>

2- Mis Tareas LED:

<https://youtu.be/46h5xUsXrHg>

3- Legajos del Organismo y Alertas LED:

<https://youtu.be/sZIAP1k62Lo>

4- Crear y Registro de Personas LED:

<https://youtu.be/hDLFHKoTw-8>

5- Audiencias LED:

<https://youtu.be/8qOWCd6S1zE>

6- Transferidos y Recurridos LED:

<https://youtu.be/S6tb5SPpeUs>

7- Información del caso LED:

<https://youtu.be/aT60uMG7iZE>

8- Actuaciones digitalizadas LED:

<https://youtu.be/wXRth41RbGA>

9- Visualización completa LED:

https://youtu.be/mJ_l3kZlqpk

3.4. Sistemas de comunicación SINEA

1. Ingresar al sitio web del Poder Judicial Mendoza: www.jus.mendoza.gov.ar
2. En la barra de menú, hacer clic en **Dependencias** y seleccionar **Dirección de Recursos Humanos**.
3. Una vez dentro del subsitio de la Dirección de Recursos Humanos, situado en la pantalla de Inicio, hacer clic en el botón del “**Sistema de Notificaciones Electrónicas**”.
4. Para ingresar al sistema, se debe completar los campos “Usuario” y “Contraseña”, que serán informadas en el instructivo que informará Dirección de Recursos Humanos

Consideraciones generales

1. **¿En qué consiste el Sistema de Notificaciones Electrónicas Administrativas (SiNEA)?**

Toda comunicación y notificación de dependencias administrativas de la Unidad Organizativa de la Suprema Corte de Justicia, destinadas a magistrados, funcionarios y empleados, a partir del 1 de agosto de 2018, deberá hacerse a través de documentos electrónicos firmados digitalmente, eliminando la confección de los mismos en soporte papel.

2. **¿Cómo se implementará el Sistema de Notificaciones Electrónicas?**

Cada magistrado, funcionario o empleado tendrá una casilla personal en el Sistema de Notificación Electrónica donde recibirá todo tipo de comunicaciones emitidas por dependencias administrativas (Dirección de Recursos Humanos, Dirección de Contabilidad y Finanzas, Secretaría Administrativa, entre otras dependencias).

3. ¿Qué necesito para acceder a consultar mis notificaciones electrónicas?

Puedo acceder ya sea desde una computadora en mi lugar de trabajo o a través de cualquier dispositivo inteligente con conexión a internet (ejemplo: celular, computadora, tablet). El servicio está disponible las 24 horas, todos los días del año.

4. ¿Se trata de una casilla de correo electrónico?

No. Es una casilla personal en el Sistema de Notificaciones Electrónicas Administrativas, a la que podrás acceder con tu usuario y contraseña desde el subsitio de la Dirección de Recursos Humanos en la página del Poder Judicial de Mendoza.

5. ¿Qué tipo de notificación puedo recibir?

Toda comunicación o notificación personal que involucre cualquier acto administrativo que surja de mi vínculo laboral, como agente de la Unidad Organizativa de la Suprema Corte de Justicia. Por ejemplo: disposiciones, ascensos, avances y resultados de solicitudes, sanciones, faltas de marcación, concesión de licencias, estado de trámites iniciados, subrogancias de magistrados.

6. ¿Qué características tiene la notificación electrónica?

Tiene plena eficacia jurídica en la medida que se encuentra firmada digitalmente con certificación vigente de Firma Digital.

7. ¿Cuándo comienzan a regir los plazos de notificación?

El día siguiente hábil posterior a la fecha en la cual ingresó la notificación a la mi casilla electrónica. Para tener en cuenta, tanto la emisión y recepción de las notificaciones quedan registradas en el sistema.

8. ¿Qué pasa si no ingreso a mi casilla electrónica?

Aunque no haya ingresado a mi casilla, **se me tendrá por notificado** conforme lo dispuesto en Acordada 28.772.

9. ¿Qué pasa si ingreso a mi casilla electrónica, pero no realizo la lectura de mis notificaciones?

Aunque haya ingresado a mi casilla, pero no abro ni leo cada notificación electrónica que he recibido, **se me tendrá por notificado** conforme lo dispuesto en Acordada 28.772.

10. ¿Cuáles son mis obligaciones como empleado para utilizar el Sistema de Notificaciones Electrónicas?

El Punto IX, de la Acordada N° 28772, dispone que está a cargo de todos los empleados de la Unidad Organizativa de la Suprema Corte de Justicia, ingresar a su casilla electrónica personal, aun encontrándome en uso de licencia.

3.4. Ciberseguridad

3.4.1. [Ciberseguridad.pdf](#)

[Link a descargar como parte del material de estudio](#)

Los capítulos detallados de este documento son parte del material de estudio

Capítulo 9: Ciberseguridad

Capítulo 17: Privacidad

Capítulo 51: Desinformación y mal información en Información

Capítulo 71: ¿ Cómo tratar de identificar una víctima? Marco Legal

a. Seguridad y manejo de la información

Al hablar de seguridad de la información, es importante tener en cuenta la norma internacional ISO 27001, que tiende a:

“... el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan” (International Organization for Standardization, 2016, <https://goo.gl/Cqzomn>).

Otros académicos lo definen como el conjunto de medidas técnicas y legales tendientes a la prevención para el resguardo y protección de la información, cumpliendo con los principios de confidencialidad, integridad y disponibilidad.



Por otro lado, es importante destacar que no se debe confundir el concepto de seguridad de la información con el de seguridad informática, ya que este último se encarga de la seguridad solamente del medio informático o infraestructura de tecnología.

Alcances

Dentro de los alcances de la seguridad de la información, debemos tener presente que, en toda organización, el bien más preciado es la información. Para ello, es importante identificar cada uno de los activos (correos de mails, página *web*, bases de datos, contratos, etc.) que existen en cualquier Institución y de qué manera fijar políticas de protección. Existe, para ello, una clasificación de cierta información, que puede ser:

- **Crítica:** es aquella información imprescindible que no puede faltar en la actividad de toda organización (p. ej.: la base de datos de empleados de la organización).
- **Valiosa:** es aquella información que se considera un activo preciado (base de información presupuestaria).

- **Sensible:** es aquella que solo debe ser conocida por personal facultado de acuerdo a niveles de acceso (base de información de expedientes).

Una vez que hemos identificado cada uno, debemos conocer de qué fuente interna provienen, es decir, de qué área y en qué soporte se encuentran alojados, ya sea en documentos, discos duros extraíbles, servidores, pero también debemos tener en cuenta su durabilidad en el tiempo.

A su vez, dentro de la seguridad de la información, encontramos *riesgos*, es decir, las propias debilidades que presentan las organizaciones a través de sus sistemas, que quedan expuestos a terceros debido a la falta de políticas de gestión internas y ponen en peligro la información de la organización y datos de los usuarios.

Con base en ello, podemos clasificar los riesgos en 3 categorías:

- 1) Errores involuntarios de personas o máquinas.
- 2) Desastres naturales en general.
- 3) Ataques voluntarios con un fin determinado.

Dentro de la **categoría 1**, se puede encontrar la mayoría de los problemas de las organizaciones, ello se reduce con la debida formación de los empleados; los desastres naturales, si bien no se sabe cuándo pueden suceder, pero si se debe contar con un plan de contingencia ante una eventual circunstancia involuntaria (**categoría 2**), y por último contamos el caso de ataques voluntarios con un fin determinado de producir un daño u obtener un rédito y afecte de una manera considerable a la organización (**categoría 3**). (Flores Barahona, 2000).

¿Qué es la seguridad de la información?

<https://youtu.be/43hGkBCDB7k>



VIDEO ¿Qué es la seguridad de la Información?

b. Ingeniería social - Cibercrimen

Para empezar, podemos decir en líneas generales que la ingeniería social es el arte de influenciar sobre una o varias personas. Esto significa que es una herramienta que algunos ejercen sobre el resto, lo cual puede verse en distintos casos.

Entre las técnicas de manipulación que pueden verse reflejadas a través de este tipo de arte, tenemos: *phishing*, *smishing* y *vishing* o suplantación de identidad (Social Engineer, Inc., s. f., <https://goo.gl/wi785m>). Lo importante aquí es poder distinguir entre el buen uso, es decir, utilizar esos datos responsablemente para determinado caso, y el mal uso, que está destinado a lograr ventaja de las debilidades con que cuenta la víctima.

Según un gran *hacker* conocido en el mundo, Kevin Mitnik, todos tenemos la capacidad de colaborar con el otro, y este es el primer movimiento de confianza. Por otro lado, también juega un factor psicológico importante: no nos gusta decir que no y, por sobre todas las cosas, al ser humano le gusta que lo elogien constantemente. Por todo ello, es importante conocer las fases de la Ingeniería Social:

- Recolectar información.
- Incrementar el vínculo.
- Aprovechamiento de la conexión con la víctima.
- Llevar a cabo la maniobra a fin de lograr el cometido.

Como se puede ver, cada una de estas fases tiene una función determinada dentro del proceso, es decir, conlleva cumplir cada una en un espacio de tiempo determinado para poder lograr el cometido. Veámoslo en un ejemplo:

Primero, se comenzaría por obtener información de un objetivo determinado a través de llamados, mails o fuentes abiertas de recolección de información. Luego de esto, se accedería al objetivo. Ya sea presentándose como consultor o de otra manera, se procedería a incrementar la confianza con la víctima. Una vez que se llegue a una mayor cercanía en cuestiones íntimas, será el momento de poner en acción la búsqueda de la información sensible que esta posea y que sirva para el interés final. Una vez que se logre obtener la información, se logrará cualquier objetivo.

Con base en este simple ejemplo, se observa cómo, a través de un proceso—que puede llevar días, semanas, meses o años—, se puede lograr obtener información personal, sensible o informatizada de una o varias personas. Es decir, estamos hablando de datos que son clave y que se encuentran dentro de la esfera de la intimidad de la persona.

Siguiendo con el estudio, debemos entender que este tipo de técnicas existen y son de las que los ciberdelincuentes se sirven para poder lograr sus objetivos, es decir, al aprovecharse de las debilidades de los seres humanos. En efecto, debemos tener presente cuáles son las herramientas que utilizan, que encontraremos en todo ciberdelito:

- **Phishing:** práctica de manipulación que consiste en el envío de correos electrónicos que simulan originarse en fuentes de buena reputación con el objetivo de influir u obtener información personal de la víctima. Hoy en día es uno de los grandes problemas que se deben contrarrestar, ya que se mueven millones de dólares.
- **Smishing:** práctica de manipulación que consiste en el envío de mensajes de texto que simulan originarse en números de personas reales y de buena reputación, con el objetivo de influir u obtener información personal de la víctima.
- **Vishing:** es una práctica que tiene como fin obtener información o pretender influir en la acción a través del uso telefónico.

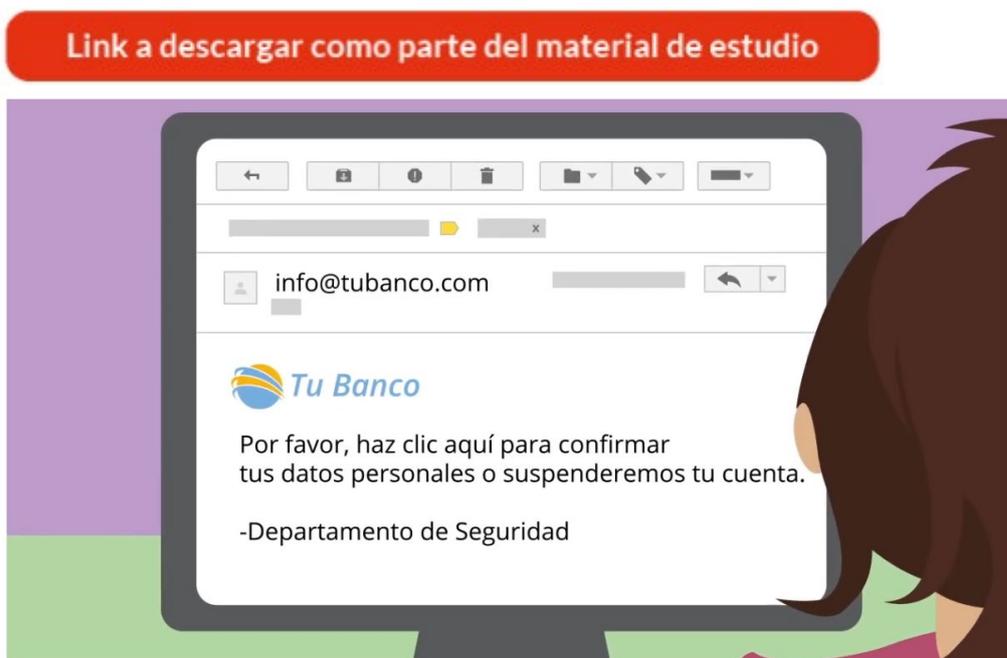
- **Suplantación de identidad:** Es la habilidad de simular ser otra persona con el objetivo de obtener información o acceso a una persona, empresa o sistema informático.

c. **¿Cómo evitar un ataque de ingeniería social?**

<https://youtu.be/cGbfi7AV6hA>

d. **Buenas prácticas en Seguridad Informática**

3.4.2. **Buenas prácticas en Seguridad Informática**



VIDEO ¿Cómo evitar un ataque de ingeniería social?

3.5. **Google Drive. Documentos, hojas de cálculo y presentaciones.**

Google Drive es un servicio web que te permite almacenar, modificar, compartir y acceder a tus archivos y documentos en la nube (plataforma en línea de Google a la que se accede desde cualquier dispositivo con conexión a Internet). Puedes subir al servicio más de 30 tipos de archivos. El servicio dispone de 15Gb de almacenamiento gratuito, ampliables mediante un pago. Dispone de versiones móviles tanto para Android como para IOS para poder acceder a través de nuestro dispositivo a nuestros datos, editar documentos etc. Este

servicio se integra con otros servicios de Google como por ejemplo Gmail (Gestor de correo vía web) y de otras aplicaciones de terceros que se integran casi de forma nativa con Google Drive (por ejemplo, Power Point, Excel, Word).



En el siguiente link de acceso a soporte de google, vamos a centrarnos y considerar como material obligatorio de estudio los tres títulos marcados, y todos aquellos subtítulos que lo contengan, desplegando las flechas hacia abajo.

<http://support.google.com/drive/?hl=es>

Los títulos son:

Guardar archivos en google

Organizar y encontrar tus archivos

Compartir archivos en Google Drive

Link a descargar como parte del material de estudio



Consultar los temas de ayuda

| | |
|---|---|
| Cómo empezar a utilizar Google Drive | ▼ |
| Drive para ordenadores | ▼ |
| Guardar archivos en Google Drive | ▼ |
| Organizar y encontrar tus archivos | ▼ |
| Compartir archivos con Google Drive | ▼ |
| Acerca de Google Drive para Mac/PC | ▼ |
| Documentos, hojas de cálculo, diapositivas y otras aplicaciones | ▼ |
| Privacidad, políticas y uso inadecuado | ▼ |
| Cómo solucionar problemas | ▼ |