Trabajo practica pericias informaticas

ALUMNOS:

● Kevin Veliz

● Brian Suarez

● Leandro Torrez

● Yober Vasquez

● Micaela Vázquez

● Juan Tulis

PROFESORA:

Analía Buratovich

CURSO: 4A

Pericias Informáticas

[¿Qué es una pericia? 1](#_Toc166534256)

[¿Qué es un perito judicial? 1](#_Toc166534257)

[Tipos de peritos 1](#_Toc166534258)

[Perito Oficial 1](#_Toc166534259)

[Perito de oficio 2](#_Toc166534260)

[Perito de parte 2](#_Toc166534261)

[Consultor Técnico 3](#_Toc166534262)

[Asesor Técnico 3](#_Toc166534263)

[Especialista Consultor 4](#_Toc166534264)

[Responsabilidades 4](#_Toc166534265)

[Responsabilidad civil: 4](#_Toc166534266)

[Responsabilidad penal: 5](#_Toc166534267)

[Responsabilidad administrativa: 6](#_Toc166534268)

[Remuneración 6](#_Toc166534269)

[¿Qué es un perito Informático? 7](#_Toc166534270)

[¿Qué tareas realizan? 8](#_Toc166534271)

[Delitos que investigan 9](#_Toc166534272)

[Elementos que se analizan 10](#_Toc166534273)

[¿Qué se estudia para ser perito informático? 12](#_Toc166534274)

[Proceso de una pericia informática 12](#_Toc166534275)

[Casos de ejemplo 14](#_Toc166534276)

[Hackeo a Sony Pictures 14](#_Toc166534277)

[El enemigo en casa 16](#_Toc166534278)

[Crimen de Fernando Báez Sosa - Perito informático 18](#_Toc166534279)

[Trabajando para tu competencia 19](#_Toc166534280)

# ¿Qué es una pericia?

Una pericia puede ser un estudio que desarrolla un perito sobre un asunto encomendado por un juez, un tribunal u otra autoridad, que incluye la presentación de un informe (el informe pericial o dictamen pericial). Este informe puede convertirse en una prueba pericial y contribuir al dictado de una sentencia.

# ¿Qué es un perito judicial?

Un perito es una persona experimentada, hábil o entendida en una ciencia o arte. El perito es el experto en una determinada materia, que, gracias a sus conocimientos, actúa como fuente de consulta para la resolución de conflictos.

# Tipos de peritos

## Perito Oficial

Es el profesional que trabaja en relación de dependencia del Poder Judicial. A este cargo se accede únicamente a través de un concurso de oposición y antecedentes.

## Perito de oficio

Para ejercer esta función, el experto debe registrarse en los registros que, con ese propósito, se establecen en cada ámbito judicial.

Su relación con el Poder Judicial es contractual, para intervenir en un caso específico, siendo convocado por el magistrado.

En el ejercicio de esta función, el profesional deberá adecuar su actuación a las disposiciones que establecen los códigos de procedimiento del ámbito en el que participe. Además, debe mantener una imparcialidad y objetividad estrictas, garantizando la integridad y credibilidad de su análisis.

## Perito de parte

Son expertos contratados por una de las partes, que le ayudan a dar soporte técnico a su defensa legal. Suelen ser especialistas elegidos por su experiencia y conocimientos técnicos en el caso, y ayudan a la parte a preparar el caso.

## Consultor Técnico

Su intervención está regulada por el Código de Procedimiento Civil, y, por ende, opera en todos los ámbitos judiciales que se rigen procesalmente bajo este código. Es designado por el juez a solicitud de cualquiera de las partes (quien será responsable de cubrir sus honorarios). No está legalmente obligado a aceptar formalmente el cargo ni a presentar informes (aunque conserva el derecho de presentarlos).

Además, su función implica brindar asesoramiento especializado en cuestiones técnicas relacionadas con el caso en cuestión, garantizando la precisión y relevancia de sus opiniones para el proceso judicial.

## Asesor Técnico

Este especialista no participa de forma directa en un litigio, sino que es convocado por los abogados o las partes para proporcionar asesoramiento técnico especializado.

Su conocimiento y experiencia son solicitados para brindar orientación sobre aspectos técnicos relevantes para el caso en cuestión, aportando análisis detallados y recomendaciones fundamentadas que contribuyan al desarrollo estratégico de la defensa o la argumentación legal. Además, su colaboración puede extenderse a la preparación de informes técnicos que respalden los argumentos presentados ante el tribunal.

## Especialista Consultor

Es un profesional altamente capacitado y con una amplia experiencia, comúnmente requerido en el ámbito penal para brindar claridad al tribunal durante juicios orales sobre temas específicos.

Su prestigio y dominio en su campo lo convierten en una figura destacada cuya opinión es valorada por su capacidad para explicar temas complejos de manera comprensible. Además de su participación en juicios, puede ser llamado para colaborar en la preparación de estrategias legales y en la evaluación de evidencia técnica.

# Responsabilidades

El experto puede enfrentar responsabilidad al presentar su evaluación; no obstante, hay distintos tipos de responsabilidad dependiendo del contexto específico en el que se haya requerido su participación. Estos tipos son los siguientes:

## Responsabilidad civil:

La responsabilidad civil del perito implica que será responsable por los daños causados a las partes debido a falta de atención, culpa, negligencia o ignorancia en su actuación.

Esta responsabilidad puede surgir de acciones o omisiones, como la pérdida del objeto a examinar o el hecho de no ser experto en la materia que supone que lo es. Resolver la responsabilidad civil del perito es complejo, ya que suele requerir que su informe haya influido directamente en la decisión judicial y el daño resultante. Es importante destacar que la sentencia que resuelva este proceso no modificará la decisión judicial previa que tuvo en cuenta el informe pericial.

La parte afectada por la decisión judicial es la encargada de reclamar la responsabilidad civil del perito. Para eso, debe demostrar primero la influencia del dictamen en la decisión del juez y, en segundo lugar, que esa impacto resultó en un perjuicio para la parte que busca la responsabilidad civil de perito.

## Responsabilidad penal:

Podemos definir la responsabilidad penal del perito como la obligación de responder penalmente al cometer conductas delictivas en el ejercicio de su profesión, que se van a traducir en una sanción penal consistente con los delitos en que se haya incurrido, derivada en una multa, una pena privativa de la libertad y la suspensión o inhabilitación para su ejercicio profesional.

## Responsabilidad administrativa:

El perito incurre en responsabilidad administrativa cuando este profesional se

 encuentra designado por una autoridad judicial o administrativa, cuenta con un

 nombramiento y deja de cumplir con lo establecido en la Ley Federal de

 Responsabilidades Administrativas de los Servidores Públicos, lo que le puede

 ocasionar, generalmente con amonestaciones, suspensión del empleo, cargo o

 comisión, destitución del puesto, sanciones económicas o la inhabilitación para

 desempeñar el cargo, por lo que es obligado que el perito que cuente con

 nombramiento oficial cumpa con lo establecido en el artículo 8 de la Ley Federal de

 Responsabilidades Administrativas de los Servidores Públicos.

# Remuneración

En la República Argentina un perito puede trabajar de oficio para el Poder Judicial, en cuyo caso sus honorarios serán decididos por el magistrado en base a la Ley N°27.423 o trabajará de forma independiente y por tanto podrá fijar sus propios honorarios.

Desde 2017, la Ley N° 27.243 ha sido una pieza fundamental en la regulación de los honorarios en el ámbito judicial argentino. Esta normativa no solo establece pautas para abogados y procuradores, sino que también abarca a otros actores, incluidos los peritos informáticos. Su objetivo es garantizar que los honorarios sean justos y equitativos, especialmente para aquellos profesionales cuyo trabajo técnico es crucial en casos judiciales que involucran evidencia digital o tecnológica. Así, esta ley proporciona un marco claro para la fijación de honorarios, asegurando la transparencia y la adecuada remuneración de los peritos informáticos por su valiosa contribución en el sistema judicial.

# ¿Qué es un perito Informático?

El perito informático es un perito judicial, que en su carácter de auxiliar de la justicia tiene como tarea primordial la de asesorar al juez respecto a temas relacionados con la informática.

Función: La función del perito informático consiste en el análisis de elementos informáticos, en busca de aquellos datos que puedan constituir una prueba o indicio útil para el litigio jurídico al que ha sido asignado.

# ¿Qué tareas realizan?

Dentro de las principales funciones tenemos:

* Un perito informático se encarga de analizar las pruebas informáticas y presentarlas de forma clara y comprensible para los jueces.
* Intervienen, almacenan, documentan y estudian las pruebas digitales para elaborar informes periciales detallados.
* Después acuden a los tribunales para aclararlo y preparar la refutación por las partes.
* Además, asesora a los abogados sobre las estrategias de acusación y defensa en relación con las pruebas digitales.
* Apoyan a la parte que les ha contratado en la presentación de argumentos técnicos en el escrito inicial.
* Preservar y justificar toda la información que pueda estar presente en el soporte técnico manipulado.

Además de llevar a cabo su peritaje, los peritos también deben interactuar con quienes lo utilizan. Esto se hace a través del intercambio de conocimientos, con el objetivo de convertirse en partícipe del proceso judicial. El deber del perito es mantener la confidencialidad para proteger los datos e informaciones sensibles de los implicados en el proceso.

# Delitos que investigan

El peritaje informático se usa en aquellos casos en los que se sospecha o se tiene la certeza de que se ha producido en uso inadecuado de la tecnología, se ha producido una brecha de seguridad en un sistema informático, o de que los soportes informáticos han sido el vehículo para la constitución de un delito. Por ejemplo:

* Casos de espionaje, revelación de secretos o violación de la propiedad industrial.
* Delitos contra la propiedad intelectual.
* Intromisiones ilegítimas en la intimidad de la persona.
* Accesos ilegales a documentos o ficheros de la empresa.
* Competencia desleal por parte de un empleado.
* Despidos por uso inadecuado de la tecnología.
* Interceptación de comunicaciones.
* Protección de datos personales sensibles o datos jurídicos.
* Difusión de datos privados o reservados.
* Acceso o manipulación ilegítima de software.
* Uso ilegítimo de servidores, hardware, redes o sistemas informáticos.
* Daños en equipos informáticos provocados por un uso abusivo.
* Delitos económicos realizados a través de medios informáticos.
* Delitos contra los consumidores o el mercado realizados a través de medios informáticos.
* Estafas y fraudes a través de soportes digitales.
* Acceso, posesión o divulgación de pornografía infantil.

# Elementos que se analizan

En un peritaje informático, se analizan diferentes elementos relacionados con dispositivos electrónicos y los datos que contienen. Algunos de estos elementos incluyen:

* **Dispositivos de almacenamiento:** Como discos duros, USB, tarjetas de memoria, etc. Se busca archivos relevantes, su eliminación o recuperación, y se evalúa cualquier manipulación.
* **Registros de actividad:** Esto incluye eventos del sistema, accesos a servidores y aplicaciones, revelando quién accedió, cuándo y qué acciones se realizaron.
* **Correos electrónicos:** Se identifican mensajes relevantes, se recuperan correos eliminados, se rastrea la dirección IP de origen y se autentica la autenticidad de los mensajes.
* **Historial de navegación web:** Información sobre sitios visitados, fechas y horas de acceso, y actividades en línea.
* **Archivos y documentos:** Se examinan para detectar modificaciones, creaciones o eliminaciones sospechosas.
* **Metadatos:** Información sobre creación, modificación y ubicación de un archivo para verificar su autenticidad.
* **Registros de comunicaciones:** Registros de llamadas, mensajes de texto y mensajes instantáneos relevantes en casos de acoso o comunicación ilegal.
* **Redes sociales:** Examinar perfiles, mensajes, fotos y contenido en redes sociales para recopilar evidencia.
* **Transacciones financieras:** Análisis de registros de transacciones electrónicas y cuentas bancarias en casos de fraude o lavado de dinero.
* **Vulnerabilidades de seguridad:** Buscar vulnerabilidades en sistemas y redes en casos de violaciones de seguridad.
* **Ubicación y localización:** Registros de ubicación de dispositivos móviles relevantes en investigaciones de ubicación.
* **Registros de aplicaciones:** Analizar registros de actividad de aplicaciones para identificar eventos significativos o actividades sospechosas.

# ¿Qué se estudia para ser perito informático?

Para convertirse en un perito informático, es fundamental tener un profundo conocimiento en dos áreas principales: informática y derecho. En el ámbito de la informática, es necesario entender tanto el funcionamiento de los equipos y programas informáticos como los procedimientos asociados. Además, en el campo del derecho, se requiere comprensión tanto de cuestiones relacionadas con la ciberseguridad como del derecho procesal.

Esto implica estar al tanto de los últimos avances en tecnología informática, así como de las normativas y regulaciones que afectan al mundo de la ciberseguridad.

# Proceso de una pericia informática

El proceso de un peritaje informático es una combinación de recopilación de evidencia y análisis técnico respecto a la disputa legal, siempre relacionada a la tecnología. Por norma general, se siguen los siguientes pasos:

1. **Recolección de Información:** el perito informático y el cliente se reúnen y discuten sobre el caso, incluyendo los detalles del incidente, los dispositivos involucrados y los objetivos del peritaje.
2. **Planificación:** Según la información, el perito informático planea cómo proceder. Esto puede incluir la identificación de los dispositivos que necesitan ser examinados, las herramientas y técnicas a utilizar, y los plazos para completar el trabajo.
3. **Recopilación de datos y evidencias:** El perito toma en cuenta cualquier tipo de evidencia digital que considere importante. Esto puede implicar la extracción de datos de dispositivos como computadoras, celulares y dispositivos de almacenamiento.
4. **Análisis forense:** Se realiza un análisis forense digital exhaustivo. Esto implica examinar archivos, registros, metadatos y otros elementos para identificar patrones, anomalías o cualquier otra información relevante para el caso.
5. **Documentación:** Durante el análisis, el perito documenta el proceso de la forma más detallada posible. Crea informes que describen los métodos utilizados, los resultados obtenidos y las conclusiones alcanzadas.
6. **Presentación de resultados:** Una vez completado el análisis, el perito debe informar lo descubierto. La información presentada puede estar en formato de texto, imágenes o gráficos.

1. **Testimonio en el tribunal:** No siempre es el caso, pero puede que el perito sea llamado a testificar en el tribunal como testigo experto.
2. **Seguimiento y apoyo continuo:** Finalizada la presentación de resultados, el perito informático puede seguir brindando apoyo y asesoramiento adicional según sea necesario para el caso.

# Casos de ejemplo

## Hackeo a Sony Pictures

El caso del **hackeo a Sony Pictures** en 2014 fue uno de los incidentes de seguridad informática más impactantes en la industria del entretenimiento. Aquí tienes más detalles sobre el caso:

1. El Ataque: En noviembre de 2014, los sistemas informáticos de Sony Pictures Entertainment, la división de entretenimiento de Sony Corporation, fueron comprometidos por un grupo de hackers que se autodenominan "Guardians of Peace" (Guardianes de la Paz). Los hackers lograron acceder a una gran cantidad de información confidencial, incluyendo correos electrónicos, documentos internos, planes de películas futuras, datos financieros y detalles de empleados.
2. Filtración de Datos Sensibles: Los hackers filtraron gran parte de la información robada en Internet, lo que generó una enorme repercusión mediática y afectó la reputación de Sony. Entre los datos filtrados se encontraban correos electrónicos entre ejecutivos de alto nivel, detalles sobre la remuneración de empleados, información personal de celebridades y datos financieros confidenciales.
3. Amenazas y Coacción: Además de la filtración de datos, los hackers también amenazaron con llevar a cabo ataques terroristas en cines que proyectarán la película "The Interview", una comedia satírica que involucra un complot ficticio para asesinar al líder de Corea del Norte, Kim Jong-un. Estas amenazas llevaron a Sony a cancelar el estreno de la película en cines, aunque finalmente se lanzó en plataformas digitales.
4. Investigación Forense: Después del ataque, Sony contrató a empresas de seguridad cibernética y expertos en informática forense para investigar el incidente. Se llevaron a cabo análisis exhaustivos de los sistemas comprometidos para determinar el alcance del ataque, identificar a los perpetradores y fortalecer la seguridad de la red de Sony.
5. Atribución y Sospechas de Corea del Norte: Aunque inicialmente se especuló sobre la autoría del ataque, investigaciones posteriores, incluida una evaluación del FBI, sugirieron que el gobierno de Corea del Norte estaba detrás del hackeo en represalia por la película "The Interview". Corea del Norte negó su participación, pero el FBI afirmó que existían pruebas suficientes para respaldar esta afirmación.

El caso del hackeo a Sony Pictures demostró la vulnerabilidad de las grandes corporaciones ante los ataques cibernéticos y la importancia de la pericia informática en la investigación y mitigación de estos incidentes. Además, planteó preguntas sobre la seguridad cibernética en la industria del entretenimiento y las implicaciones de la censura en la libertad de expresión.

## El enemigo en casa

Lorenzo Martínez, informático forense, también, director de la empresa Securizame, especializada en ciberseguridad y peritaje forense, nos cuenta un caso complicado al que tuvo que hacer frente.

El nos relata: “En una empresa, había alguien que contactaba con ellos indicándoles que tenía acceso a sus sistemas, dando prueba de ello. La falta de evidencias nos llevaba a varios callejones sin salida”. Detalla, hasta un indicio los llevó a pensar que la máquina estaba, en realidad, dentro de la propia empresa.

“Solicité analizar el ordenador de una persona del departamento de sistemas, que curiosamente me conocía, realizando toda la cadena de forma correcta; es decir, que el trabajador entregó de su propia mano el equipo a un notario”. Tras llevar a cabo, una imagen del disco y analizar esta, acorralando con evidencias de otros equipos, se determinó, que, efectivamente, este empleado estaba saboteando desde dentro a la empresa para la que trabajaba.

“Se marchó antes de que la despidieran”, aclara Martínez, quien reconoce que, técnicamente hablando, tenía conocimientos de hacking, aunque no los suficientes de forense. “De hecho, en el análisis del ordenador descubrimos que, desde justo la fecha en la que se enteró que le iba a analizar el caso, empezó a ejecutar una herramienta de limpieza y borrado de evidencias en su ordenador todos los días” añade.

## Crimen de Fernando Báez Sosa - Perito informático

El perito informático, en este caso Rodríguez Romeo, realizó un análisis detallado de los archivos digitales incorporados al expediente. Esto incluyó revisar la cadena de custodia de los teléfonos secuestrados y examinar la integridad de los datos contenidos en ellos.

El perito puso en duda la integridad de la cadena de custodia de los teléfonos secuestrados, señalando que no se siguieron los protocolos adecuados y que no se proporcionó información detallada sobre el estado de los dispositivos y cómo fueron resguardados.

Rodríguez Romeo señaló que no pudo verificar la integridad de los archivos digitales incorporados a la causa, ya que encontró mensajes eliminados después del secuestro de los teléfonos y diferencias en las fechas de creación y modificación de los archivos.

El perito informático aclaró que su expertise se limita al análisis de archivos digitales y que no tiene la capacidad de corroborar la autenticidad de las filmaciones, ya que su enfoque se basa en verificar la integridad de los archivos a través de sus hashes.

## Trabajando para tu competencia

David Olmo tuvo un caso de un empleado directivo de una gran empresa tecnológica que iba a ser despedido. “Se negaba entregar los medios tecnológicos que le proporcionó la empresa (portátil y disco externo)”, por lo que la empresa empieza a sospechar qué está realizando proyectos para otra de la competencia.

Para intentar corroborar esta tesis, se cita al empleado en una notaría mediante un burofax, para que el notario pudiera dar fe de lo que allí iba a ocurrir. “El representante legal de la empresa preguntó a este empleado si hacía entrega de todos los datos y si había borrado algo”. ¿La respuesta delante del notario? Que no había borrado nada.

Sin embargo, y una vez realizada la clonación del disco y la posterior recuperación de datos, obtuve un “timeline” del usuario donde conseguí demostrar que el usuario durante la madrugada previa había borrado archivos de la empresa y correos electrónicos”. De hecho, se había levantado a las 5 de la mañana para proceder a toda esta eliminación de archivos antes de presentarse en la notaría donde, probablemente, no se esperaba la presencia de un perito.