

El Foro de las Evidencias Electrónicas ha popularizado este término que procede de la denominación inglesa y que se enmarca en la disciplina más amplia de la Prueba Judicial.

Los documentos electrónicos pueden ser sometidos a los criterios de los peritos informáticos para determinar su autenticidad y ser aportados como prueba en juicio. Cuando se emplea la firma electrónica, su eficacia probatoria es singularmente importante por el contexto normativo que determina la presunción de los aspectos de integridad y atribuibilidad, pero sin tomar en cuenta ciertos aspectos técnicos (como las formas avanzadas AdES-XL) pueden perderse elementos tan importantes como la databilidad (situar la firma en el tiempo) o la verificación de su validez (respecto a la inclusión o no del certificado, en el momento de la firma, en la lista de certificados revocados).

Leyes como la LAECSP (Ley 11/2007) y LMISI (Ley 56/2007) generalizan las gestiones por vía electrónica en el sector privado y en el sector público, pero quienes tienen que implantarlas, se preguntan sobre la forma de presentar las evidencias electrónicas en los procesos jurisdiccionales, si fuera el caso. La Ley de Enjuiciamiento Civil española es muy avanzada en el uso de medios electrónicos, y en su marco se han creado los mecanismos para presentar pruebas electrónicas en juicio.

Por otro lado, los incidentes de seguridad dejan tras de sí un conjunto de rastros y vestigios que puestos en relación unos con otros y vinculados a otras fuentes de investigación favorecen la recreación del relato fáctico del suceso, gracias a la capacidad de los investigadores forenses que los analizan. Añadimos así la valoración de las pruebas no estructuradas a las estructuradas que se gestionan en las transacciones electrónicas, completando el marco de las que se pueden presentar, con los procedimientos previstos en las instancias procesales.

Conceptos como logs, hash, timestamping, bases de datos, diplomática digital, firma electrónica, cadena de custodia, se manejan en estos contextos y son algunos de los que se presentarán en este seminario impartido por reconocidos profesionales. Yo tendré el privilegio de presentarlos y confío en tener la oportunidad de saludarle el día del evento.

Cordialmente  
Julián Inza  
Codirector del Foro de las  
Evidencias Electrónicas  
Presidente de la Jornada

¡Reserve en su agenda el próximo 29 de septiembre!

## Horario

9:00 - 9:30 Acreditaciones  
9:30 -11:00 Ponencias y Sesiones de Trabajo  
11:00-11:30 Coffe Break  
11:30-14:30 Ponencias y Sesiones de Trabajo  
14:30-16:00 Pausa Comida  
16:00-18:30 Ponencias y Sesiones de Trabajo  
18:30-19:00 Coloquio y Clausura

## Dirigido a...

- Responsables tecnológicos y de asesoría jurídica de banca y seguros
- Cuerpos y fuerzas de seguridad del estado
- Abogados en ejercicio, especialmente en áreas tecnológicas
- Fiscales, jueces y magistrados
- Peritos judiciales
- Ingenieros recién titulados que prevean dedicarse a la actividad forense

## Objetivos

- Proporcionar una visión global de qué es una evidencia electrónica.
- Explicar cuál debe ser la actuación de los peritos para la obtención de evidencias electrónicas.
- Analizar desde el punto de vista jurídico y tecnológico el sector de las evidencias electrónicas.
- Estudio de la posición de los tribunales en este ámbito.
- Examen de los principales problemas que en la actualidad existen ante la ausencia de una regulación legal específica.
- Resolver las dudas posibles acerca de las evidencias electrónicas en cada orden jurisdiccional.
- Conocer los niveles de seguridad y confidencialidad en el procedimiento pericial.
- Entender el funcionamiento de cada fase en la obtención de evidencias electrónicas.
- Conocer las soluciones más apropiadas para cada empresa en función de sus necesidades, a efectos de prevenir posibles vulneraciones por parte de los trabajadores.
- Estar al día de las normativas legales españolas y europeas que regulan y afectan a las evidencias electrónicas.

## Inscripción e Información

Fecha: 29 de septiembre de 2011

Lugar: Centro de formación de Atenea Interactiva  
C/ Métrida, 6 – 28043 Madrid

Coste: 450 € + IVA (18%). Total 531 € por asistente  
Bonificable por la Fundación Tripartita

Inscripción:

-Mediante el formulario web accesible en:

<http://www.ateneainteractiva.com>

-Por teléfono: 902 365 612. Contacte con el Departamento de Eventos

-Por e-mail: Envíenos sus datos a:

[inscripciones@ateneainteractiva.com](mailto:inscripciones@ateneainteractiva.com)

# EVIDENCIAS ELECTRÓNICAS



Madrid, 29 de septiembre de 2011

# Programa de la Jornada

## Introducción y presidente de la jornada

Julián Inza

## 9:30-11:30 El valor de las evidencias informáticas: Problemática actual

Javier Pagès López

- El valor de las evidencias informáticas.
- Algunos criterios de validez.
- Normas de actuación pericial.
- Principales problemas actuales - Ejemplos prácticos:
  - Entorno Civil.
  - Entorno Mercantil.
  - Entorno Laboral.
  - Entorno Penal.
- Algunas Soluciones Existentes:
  - Custodia Certificada de Evidencias.

## 12:00 -14:00 El cibercrimen y la inseguridad 2.0

Antonio Ángel Ramos Varón

- El cibercrimen como una arquitectura empresarial alrededor del delito en la red.
- Visitando en línea los canales de intercambio de: datos personales y bancarios.
- La venta y adquisición de material para cometer delitos en la red.
- Nunca ha sido tan fácil rastrear a una persona u organización.
- Usando herramientas para rastrea a personas o infraestructuras.
- Analizando las comunicaciones interferidas en una red.
- La geolocalización vista como una brecha de seguridad.

## 15:30-17:00 Evidencias: ¿forenses o certificadas?

Jacobo van Leeuwen

- La contradicción de la "evidencia" electrónica.
- ¿Qué se quiere demostrar?
- Modos de impugnar los medios de prueba.
- Pre-construir: certificando evidencias.
- Algunas técnicas para demostrar voluntad, origen o contenido.

- Adecuación en función del riesgos vs usabilidad/costes.
- Análisis de la validez legal.
- Casos prácticos: email, web y redes sociales.

## 17:00-18:30 Diplomática digital y gestión de documentos con carácter probatorio

Fernando Pino

- Autenticidad de los Documentos Electrónicos. Diplomática digital.
- Documentos privados. Documentos públicos.
- Custodia de documentos a largo plazo.
- La Prueba Electrónica en la Ley de Enjuiciamiento Civil.
- Cadena de custodia.

## Ponentes

D. Julián Inza

Actualmente es Presidente del **Grupo Interactiva**.

Pionero de la Certificación Digital, ha sido director general de Camerfirma, director de Estrategia Tecnológica de Banesto, Technology Senior Vicepresident de Mobipay International y director Gerente de FESTE. Es coordinador del Foro de la Firma Electrónica, coordinador del Foro de las Evidencias Electrónicas, profesor del Instituto de Empresa y miembro del Comité Editorial de Financial Tech Magazine.

En ASIMELEC es Presidente del Esquema de Certificación de PSCs y Coordinador del Grupo de Trabajo de eFactura de ASIMELEC. En OASIS es co-Chairman de Firma Electrónica en UBL-Security-SC.

**Blog:** *"Todo es Electrónico"*

**Twitter:** @albalia

D. Fernando Pino

Licenciado en Derecho en la Universidad Complutense de Madrid y Máster en Informática y Derecho por el Instituto Español de Informática y Derecho, desarrollando su especialidad en criptología y seguridad informática. Ha participado en diferentes jornadas relativas a la protección de datos, firma electrónica y seguridad de la información. Ha trabajado en AC Camerfirma durante cuatro años, desarrollando labores de consultoría y formación en PKI.

Actualmente, Fernando es auditor CISA y desarrolla su carrera en **Albalia Interactiva** como Director de Tecnología Legal.

**Twitter:** @fpinosola

D. Antonio Ramos Varón

Titulado por la Universidad Complutense de Madrid. Profesor de postgrados y masters universitarios como: el título propio de la Universidad Complutense de Madrid "Experto en técnicas estadísticas aplicadas a las seguridad informática de redes de ordenadores", "Master Universitario en ingeniería de seguridad de la información y las comunicaciones" Universidad Alfonso X el sabio (UAX) y el "Postgrado de Seguridad informática y hacking de sistemas" editado por la Escuela Universitaria Politécnica de Mataró.

Autor de libros como: Hacker 2006, Hacking Práctico, Hacking y Seguridad en Internet, entre otros, publicados por las editoriales Anaya Multimedia y Ra-Ma. Director de contenidos del programa de TV en Internet "Mundo Hacker TV" programa divulgativo sobre seguridad e inseguridad informática dirigido a usuarios y empresas.

D. Jacobo van Leeuwen

Experto en seguridad e Internet, CISA, CISSP e ITIL, con 15 años de experiencia en proyectos y servicios gestionados de seguridad para gran parte del IBEX 35. Ha asumido distintos cargos en empresas como Telefónica, IP6 Seguridad y el Grupo SIA.

Especialista en la seguridad de documentos y procesos electrónicos, con especial foco en administración electrónica, eHealth (receta e historia clínica) y B2B/EDI (contratación, facturación y cobro).

Actualmente es fundador de Evicertia, un servicio que mediante correo electrónico, un móvil o por web, ofrece una nueva forma rápida, funcional y económica de dejar las cosas por escrito, con plenas garantías legales, sin tener que usar el papel.

D. Javier Pagès López

Director de la empresa *Informática Forense S.L.*, es licenciado en Informática por la Universidad de Valladolid, experto en Desarrollo de sistemas para Comercio Electrónico, por la Universidad de Salamanca (2010) y Auditor Jefe ISO/IEC 27001:2005, por el British Standards Institution (2010).

Con más de 20 años de experiencia en el sector informático, es colaborador con las Fuerzas y Cuerpos de Seguridad del Estado en la lucha contra la ciberdelincuencia y miembro del Comité Técnico Normalizador de AENOR AEN/CTN197, sobre Informes Periciales.

Presidente de AI2, Presidente-Fundador, y actual Tesorero, de ISSA-España y Vocal de CCII - Consejo General de Colegios Profesionales de Ingeniería en Informática, es formador y ponente habitual en cursos y seminarios sobre Peritaje, Informática Forense y Seguridad