

Planes de Seguridad y Protección de Datos en AA.PP.

El martes, 15 de marzo, tuvo lugar el seminario sobre "Planes de Seguridad y Protección de Datos en Administraciones Públicas", organizado por "Sociedad de la Información" y patrocinado por Deloitte, T-Systems y

Siemens. Como era de esperar por la generalidad del tema, atrajo nada menos que 287 inscripciones, con 181 asistentes finales. La presidencia también estuvo nutrida, con once ponentes. *Por Jorge Heredia.*

Para las próximas semanas están previstos los siguientes seminarios:

- "*Ciudades Digitales*" (17 de mayo).

- "*10 años de e-Government: Experiencias y retos*" (1 de junio).

- "*Gestión de recursos humanos en las AA.PP.*" (14 de junio).

LA presencia en el evento por parte de la Agencia Española de Protección de Datos fue notoria, tanto por la intensidad como porque contaron con dos ponentes. Abrió el seminario José Luis Piñar Mañas, director de la Agencia Española de Protección de Datos, quien se centró en los principios generales de la ley, y lo cerró Inmaculada Gómez Barduzal, inspectora de Datos de la misma agencia, quien enfatizó los aspectos legales de la seguridad de la información, los incumplimientos típicos y las sanciones correspondientes.

Domingo Laborda, director general de Modernización Administrativa, del Ministerio de Administraciones Públicas, habló sobre "Políticas y herramientas de Seguridad en la Administración General del Estado". Entre sus conclusiones, recordó que "la seguridad es un proceso, no una meta. Es un camino que tenemos que recorrer juntos: Administraciones Públicas, investigación, empresas y usuarios".

José Luis Yanguas, director del Servicio de Organización, del Departamento de Economía y Hacienda, del Gobierno de Navarra, habló sobre "El Plan Director de Seguridad del Gobierno de Navarra". Como conclusiones de su puesta en ejecución, mencionó las siguientes: mejora de la seguridad en marcha; necesidad de contar con recursos internos cualificados; aparición de nuevos aspectos técnicos

Pedro Alberto González, responsable de Sistemas del Consejo General del Poder Judicial, habló sobre la "Protección de datos en la Justicia: una reforma pendiente". Repasó el marco legal actual y los problemas existentes que impiden un cumplimiento total de la ley, la prevista reforma del reglamento 5/1995, y las actuaciones desarrolladas, especialmente la auditoría de seguridad.

Las presentaciones utilizadas por los ponentes están disponibles gratis en la web www.socinfo.info/seminarios/datos.htm.

y organizativos; aparición de nuevas funciones y responsabilidades relacionadas con la organización de la seguridad que es necesario asignar; se necesita invertir en sistemas de información que soporten los modelos de gestión; y hay que desarrollar programas de formación continua.

Juan Miguel Ramos, socio de Deloitte, habló de "La seguridad de las aplicaciones web", con los defectos de seguridad, el cibercrimen, y la conveniencia de un test de vulnerabilidades para identificar y corregir los riesgos.

Carolina de Oro, responsable de Área de Seguridad de Siemens, versó



Aspecto parcial del público asistente y vista general de la primera mesa de los ponentes.



De izda a dcha, José Luis Piñar, Domingo Laborda, José Luis Yanguas, Pedro Alberto González y Juan Miguel Ramos.

sobre "Puntos clave a la hora de abordar un plan de continuidad de negocio" y sus aspectos básicos, como son el análisis de impacto en el negocio, el análisis de riesgos, la propia estrategia de continuidad de negocio, las operaciones y respuesta de emergencia (que incluye un Centro Operativo de Emergencia), y los planes de recuperación.

Juan José Gilsanz, director de Mobile Solutions de T-Systems, se centró en "Los nuevos riesgos de seguridad introducidos por la movilidad", entre los que se cuentan: *Denial of service* (DoS), el ataque produce la imposibilidad por parte de la víctima de acceder y/o permitir el acceso a un recurso determinado; el escaneo de puertos; el robo de información crítica; el *spoofing* (IP falseadas); el acceso no autorizado a datos y dispositi-



Detalle de un momento del café descanso.

vos; y un largo etcétera, lo que obliga a la implantación de un sistema de seguridad que describió en sus principales características.

Luis Arróspide Urbieto, responsable de Seguridad de la Sociedad Foral de Servicios Informáticos, de la Diputación Foral de Gipuzkoa, habló sobre "El Plan de Seguridad Integral de los Sistemas de Información de la Diputación Foral de Gipuzkoa", con el resumen de los

proyectos, los factores críticos de éxito (necesidad de apoyo del consejo, comité de dirección, etc.; necesidad de un marco metodológico sólido) y los próximos pasos a dar.

Vicent Andreu, técnico superior de Organización de la Universidad Jaime I, tituló su ponencia: "Hacia un Sistema de Gestión de la Seguridad de la Información: la experiencia de la Universitat Jaume I",

lo que ha implicado: la incorporación de la sistemática *Plan-do-check-act* a la seguridad de la información; mayores necesidades de mejora, con clasificación de la información y control de accesos; y un énfasis en las áreas más fuertes: Organización, Recursos Humanos, Continuidad y Conformidad.

Por último, Carlos Fernández, responsable de Seguridad de Sistemas de Información, de Aenor, habló sobre "La certificación del Sistema de Gestión de la Seguridad de los S.I." (con 127 controles). Entre las ventajas de la certificación, señaló las siguientes: Integrar la gestión de la seguridad de la información con otras modalidades de gestión empresarial; mejorar la imagen de confianza y competitividad empresarial; cumplimiento de la legislación, y satisfacción de los accionistas. ☒



De izda a dcha, Luis Arróspide, Vicent Andreu, Carlos Fernández, Carolina de Oro, Juan José Gilsanz, e Inmaculada Gómez.