



## 5:

### REDES DE BANDA ANCHA INALÁMBRICAS

El día 3 de noviembre de 2004, en la sede del Ministerio del Interior, el Círculo de Tecnologías para la Defensa y la Seguridad organizó la Jornada sobre "Redes de Banda Ancha Inalámbricas". La jornada fue una puesta al día sobre estas nuevas tecnologías donde participaron expertos procedentes de la Administración, la Universidad y la Empresa.

## 10:

### XI JORNADAS DE TECNOLOGÍAS PARA LA DEFENSA Y LA SEGURIDAD

El CESEDEN fue el lugar elegido para celebrar la cita bienal que dió origen a la fundación del Círculo de Tecnologías para la Defensa y la Seguridad. En esta ocasión el encuentro estaba titulado "Conocimientos y aplicaciones emergentes".

## 15:

### PROGRAMA EUROPEO DE INVESTIGACIÓN EN SEGURIDAD

La presentación del "Programa Europeo de Investigación en Seguridad" tuvo lugar el pasado mes de enero en el CDTI. Una jornada organizada por el Círculo en colaboración con el Centro para el Desarrollo Tecnológico e Industrial.

## 18:

### CURSO DE FORMACIÓN EN ETSI

El pasado mes de noviembre el salón de actos de la Escuela Técnica Superior de Ingenieros de Telecomunicación de la UPM acogió el acto conjunto de apertura y clausura de los cursos de formación continua organizada por el Círculo, la Inspección General CIS y la UPM.

## 21:

### NOMBRAMIENTOS

Durante la Junta Directiva celebrada el pasado mes de marzo se aprobaron las nuevas incorporaciones a los órganos de gobierno del Círculo de Tecnologías para la Defensa y la Seguridad.

## 2:

### TRIBUNA

### AGENDA

## 24:

## “LA SEGURIDAD DE LA UNIÓN EUROPEA: UNO DE LOS GRANDES RETOS DEL SIGLO XXI”



Antonio Vizcaíno Camacho  
Secretario de Estado de  
Seguridad  
Ministerio del Interior.

Vivimos un momento de grandes transformaciones sociales y tecnológicas y en ese entorno, todos los actores públicos y privados que desempeñan un papel en la tarea de garantizar la seguridad integral de los ciudadanos, y especialmente las Fuerzas y Cuerpos de Seguridad del Estado, deben prepararse; no sólo para afrontar esos cambios, sino también para responder a las nuevas situaciones relevantes para la seguridad pública. Los avances tecnológicos deben servir para mejorar la eficacia en la actuación de todos los agentes de la Administración en sus múltiples parcelas, desde la información y la inteligencia hasta el diseño y ejecución operativos.

### **Nuevo terrorismo**

Los atentados del 11 de septiembre en Estados Unidos y del 11 de marzo en Madrid, y, de manera más genérica, las nuevas amenazas a la seguridad, han empujado a la Unión a desarrollar procedimientos de actuación contra las nuevas manifestaciones de criminalidad. Las que se aprovechan de los avances tecnológicos y científicos para vulnerar la ley y optimizar sus actividades ilícitas.

El desarrollo del Programa Europeo de Investigación en Seguridad (ESRP) es uno de esos instrumentos con los que contamos para lograr el objetivo fundamental en la lucha contra las nuevas formas de criminalidad global: la modernización de nuestros sistemas de seguridad, que se han mostrado vulnerables frente a las nuevas amenazas, y el desarrollo de políticas de seguridad y defensa basadas en nuevas estrategias y nuevas tecnologías que permitan una prevención más eficaz y una respuesta más efectiva. Es decir, el desarrollo de nuevos instrumentos que nos permitan adelantarnos a los enemigos de la libertad, la democracia y la justicia.

Las nuevas amenazas a las que nos enfrentamos son producto directo de los importantes y profundos cambios que el mundo ha vivido en las dos últimas décadas y que se han condensado bajo el término globalización. Hoy no podemos enfrentarnos a ningún reto con garantías de éxito si no somos conscientes de que los instrumentos que debemos utilizar deben ser globales. Esas respuestas integrales han hecho que la frontera entre la Seguridad y la Defensa, entendidas de manera tradicional, sea cada vez menos clara. El Ministerio del Interior es consciente de esa realidad y de la necesidad de aprovechar las capacidades de los dos ámbitos, tanto en el aspecto operativo como en el desarrollo de sistemas basados en la tecnología.

El Programa Europeo de Investigación en Seguridad es, sin duda, un gran paso adelante, que nos permitirá potenciar las sinergias entre la Defensa y la Seguridad Civil. Sólo respuestas integrales servirán para hacer frente a los problemas globales. Los sistemas de seguridad nacional se han mostrado impotentes e ineficaces a la hora de hacer frente a las nuevas amenazas. Esa reflexión es compartida tanto en Europa como en Estados Unidos. Así, el Gobierno español, entre sus primeras actuaciones, analizó los fallos en los sistemas de seguridad que no permitieron evitar la masacre del 11-M y diseñó un paquete de medidas para subsanar esas carencias. Lo mismo ocurrió en Estados Unidos tras el 11 de septiembre.

En ambos casos la respuesta pasó por parámetros similares. El fortalecimiento de los sistemas de seguridad nacionales desde una perspectiva mucho más amplia, que tiene como uno de sus ejes básicos la proyección de la labor de las Fuerzas y Cuerpos de Seguridad del Estado más allá de nuestras fronteras nacionales. No sólo a su trabajo en el exterior para prevenir acciones criminales en nuestro territorio, sino también a las misiones de mantenimiento de la paz por parte de los mismos cuerpos que garantizan la seguridad nacional, en nuestro caso el Cuerpo Nacional de Policía y la Guardia Civil. El Programa Europeo de Investigación en Seguridad contempla misiones de ambos tipos, un enfoque que, desde nuestro punto de vista, es muy positivo.

#### **Armonización europea**

Junto a esa nueva perspectiva, la Unión debe hacer frente a uno de los grandes déficits que presenta la política de seguridad Europea y que requiere realizar un importante esfuerzo para coordinar más y mejor las diferentes políticas nacionales. Es indudable que en este aspecto tenemos claras deficiencias estructurales políticas e institucionales que no favorecen la explotación efectiva de las capacidades científicas, tecnológicas e industriales de las que

disponemos los países europeos. Por ello, es imprescindible avanzar hacia la consecución de una mayor armonización en las políticas y, especialmente, en los requerimientos operativos entre los responsables y los usuarios finales de los sistemas basados en la tecnología más avanzada.

El Programa Europeo de Investigación en Seguridad debe convertirse en un instrumento eficaz en este campo, además de contribuir significativamente a cumplir los objetivos de las políticas de crecimiento y de competitividad de la Unión Europea definidas en Lisboa y Barcelona.

Para que todos estos objetivos se cumplan los gestores del programa no deben olvidar que es imprescindible que los proyectos que se financien estén orientados de manera esencial a resolver las necesidades y problemas concretos de los usuarios finales de los nuevos instrumentos. En este sentido, y puesto que la Comisión Europea está formando un grupo asesor de alto nivel que ayude a orientar y gestionar el programa de la forma más adecuada posible, me parece obligado que en ese

grupo asesor estén representadas las opiniones de estos usuarios finales, en nuestro caso esencialmente las Fuerzas y Cuerpos de Seguridad del Estado.

### **Empresa y mundo científico**

Es imprescindible que las empresas españolas y el mundo científico de nuestro país participen activamente en las distintas convocatorias que se realicen para el Programa Europeo de Investigación en Seguridad. España debe tener un retorno adecuado en este programa, tanto económico como científico y tecnológico. Desde los distintos ministerios con responsabilidad en el programa se harán todos los esfuerzos necesarios para apoyar y promover esa necesaria participación. En el caso del Ministerio del Interior se estudiarán, además, todas las posibilidades que se abran para que las Fuerzas y Cuerpos de Seguridad y los usuarios finales de las tecnologías y sistemas que se desarrollen, puedan participar activa y directamente en las propuestas que se consideren más próximas a sus necesidades operativas.

El desarrollo de la Sociedad del Conocimiento ha creado nuevos riesgos que hacen que nuestras sociedades sean menos seguras. Estos riesgos son menos visibles e ignoran las fronteras nacionales e incluso las de la Unión Europea. Europa es consciente de esta realidad y en los últimos tiempos, en buena medida gracias al impulso español, ha dado importantes pasos que permiten ser más eficaces contra el terrorismo internacional y la delincuencia organizada, dos de las amenazas que los ciudadanos sufren directamente. Ese avance no puede frenarse y los europeos debemos aprovechar todas las capacidades que hemos desarrollado en los últimos años.

Por un lado la ampliación de la Unión ha creado una zona de paz garantizada de la que disfrutan 25 países y más de 450 millones de personas y nos brinda la oportunidad de desarrollar políticas armonizadas y nuevos instrumentos para combatir la multiplicación de las nuevas amenazas en este amplio

territorio. De otro lado, la Constitución Europea, en pleno proceso de ratificación, nos permitirá consolidar un espacio de Libertad, Seguridad y Justicia dotado de excelentes instrumentos jurídicos y políticos para hacer frente a las nuevas amenazas.

En ese escenario, el Programa Europeo de Investigación en Seguridad cobra una especial importancia: servirá para que Europa saque el máximo partido a su potencial humano, tecnológico y científico en el ámbito de la seguridad. Una de las principales preocupaciones de la ciudadanía. Estamos ante la oportunidad de situar a la Unión Europea en el lugar que le corresponde, que no es otro que el liderazgo de la respuesta global ante las nuevas amenazas desde los valores de la libertad, la justicia y la paz.

Para ello, la modernización de nuestros sistemas de Seguridad y Defensa y el desarrollo de políticas basadas en nuevas estrategias y nuevas tecnologías que permitan una prevención más eficaz y una respuesta más efectiva deben ser nuestras prioridades. No les quepa duda de que en esa tarea no regatearemos ningún esfuerzo. ☺

### **Antonio Vizcaíno Camacho**

Secretario de Estado de Seguridad  
*(Discurso de apertura de la Jornada sobre el "Programa Europeo de Investigación en Seguridad (ESRP)" celebrado el pasado 14 de enero.)*

## “REDES DE BANDA ANCHA INALÁMBRICAS: WI-FI, WI-MAX”



Julio Martínez Meroño, en la sesión de apertura.

La jornada de “Redes de Banda Ancha Inalámbricas: Wi-Fi, WIMAX” se celebró en el salón de actos del Ministerio del Interior, el día 3 de noviembre de 2004, asistiendo numerosas personas de la Administración, la Universidad y la Empresa.

A lo largo de la jornada se efectuó una puesta al día sobre el estado del arte de estas nuevas tecnologías, a cargo de los principales expertos en la materia. Se analizó el impacto que este tipo de redes está teniendo en el sector de las telecomunicaciones, y se dió un repaso a las diferentes características tecnológicas inherentes a la tecnología Wi-Fi tales como: estándares WLAN, frecuencias utilizadas, escenarios de actuación, aplicaciones públicas y un aspecto tan crítico en este tipo de redes como es la seguridad.

La sesión de apertura corrió a cargo de **Julio Martínez Meroño**, director general de Infraestructuras y Material de la Seguridad del Ministerio del Interior, que dio la bienvenida y agradeció la asistencia a los presentes en su discurso se refirió a la importancia de los avances tecnológicos en materia de telecomunicación e informática (Tecnologías de la Información) que permiten acceder a la información en cualquier momento y lugar.

Particularmente destacó el hecho de que con las redes inalámbricas, se puedan simplificar las complejas estructuras de cableados de telecomunicaciones en los edificios. También precisó que hay que estar atentos a las posibles aplicaciones que estas tecnologías puedan tener en materia de Seguridad.

En la primera ponencia Jorge Pérez Martínez, catedrático de la ETS de Ingenieros de Telecomunicación de Madrid, analizó el impacto de las redes WLAN en el sector de las telecomunicaciones.

Comenzó la ponencia refiriéndose a las diferentes normas IEEE 802 existentes y en desarrollo. Las que junto con las normas HiperLAN del ETSI reproducen la batalla entre el mundo de la informática (802.11e) y el mundo de las telecomunicaciones (HiperLAN). Y es que la industria informática, es fundamentalmente norteamericana mientras que la industria de telecomunicaciones muy desarrollada en Europa. **Pérez Martínez** señalaba la posibilidad de llegar a un estándar único y a la

conectividad permanente ubicua multimedia (IEEE 802.20).

La itinerancia en la WLAN hace necesaria una armonización a nivel internacional de las bandas de frecuencias utilizadas, todo tanto por criterios económicos y como tecnológicos.

El catedrático continuó hablando de la tecnología WIMAX, la tecnología de última milla, que ofrece mayor ancho de banda y alcance que la familia de estándares Wi-Fi. Presentó un estudio comparativo entre ambas tecnologías desde el punto de vista de la cobertura, alcance y calidad de servicio.

Finalmente se centró en el impacto de las redes WLAN en el sector, analizando las incertidumbres de estas redes frente a otras redes fijas (ADSL y cable) y móviles (2G y 3G) desde el punto de vista de las inversiones.

Según Jorge Pérez el Wi-Fi puede considerarse una tecnología de éxito, que ha permitido la ubicuidad en la conexión a LAN en áreas de hasta unos centenares de metros, aunque coexistirá con otras tecnologías inalámbricas. Destacó que en España no existe una industria Wi-Fi nacional y la regulación tampoco ha favorecido la inversión y la innovación.

Los grandes beneficiarios del desarrollo de la tecnología Wi-Fi son los fabricantes de equipos y componentes WLAN. No obstante, los operadores de fija y móvil se están posicionando en la tecnología Wi-Fi, ya que en el momento actual ven en ella un claro complemento a sus negocios naturales en el plano de la banda ancha.

En la siguiente ponencia **Ricardo Alvariño Álvarez**, subdirector general de Planificación y Gestión del Espectro Radioeléctrico, analizó la "Regulación del espectro radioeléctrico" en relación con las Redes de Banda Ancha Inalámbricas.

Ricardo Alvariño se refirió a estas redes como complemento de acceso a banda ancha en recintos públicos, ya que permiten la portabilidad; y es que utilizan el espectro radioeléctrico en bandas de uso común bajo ciertas condiciones, sin causar interferencias ni reclamar protección.

A continuación dio un repaso a la Normativa nacional del Espectro Radioeléctrico, tipos de uso del Dominio Público Radioeléctrico, Títulos Habilitantes para el uso del Dominio Público Radioeléctrico y el Cuadro Nacional de Atribución de Frecuencias. Hizo especial hincapié en las frecuencias de uso común utilizadas para las redes WLAN: en la banda de frecuencias 2,4 GHz, (2400 a 2483,5 MHz) y en la banda 5 GHz, (5150 – 5350 MHz) y (5470 – 5725 MHz).

**Ricardo Alvariño** terminó su intervención haciendo referencia a la "Recomendación de la Comisión Europea de 20-03-2003" aplicable a este tipo de redes.

**José Casado Meléndez**, de CISCO SYSTEMS España, disertó sobre los "Escenarios de utilización de redes Wi-Fi", destacando en primer lugar que la utilización de redes Wi-Fi en las empresas, incrementa la productividad ya que proporciona acceso a las aplicaciones de negocio (respuesta rápida, colaboración) en zonas donde no lo había anteriormente gracias a la disponibilidad de conexión fuera del ámbito de la empresa.

WLAN es otra tecnología que habrá que tener en cuenta en el camino de la convergencia a IP de las redes empresariales, planteando una fórmula "IP + Movilidad = Ubicuidad + Productividad".

El ponente también trató otros aspectos como la evolución de las WLAN, integración con las redes fijas, seguridad de WLAN, programa CCX y la presencia de la tecnología Wi-Fi en cada vez más dispositivos (PDA's, PC's portátiles, teléfonos etc.).

**Carlos Jiménez Suárez**, presidente de SECUWARE, habló de la seguridad en el puesto de trabajo. El objetivo es un control de acceso seguro al sistema, para evitar que la información, el software de la compañía sean robados o manipulado.

El presidente de SECUWARE destacó la importancia de reducir el impacto económico de la pérdida o robo de equipos portátiles (laptops). Según sus palabras hay que reducir el TCO (Total Costo of Ownership) ya que los usuarios no pueden instalar su propio software no corporativo y garantizar la seguridad y estabilidad del sistema en cualquier entorno.

**David Zafrilla González**, Gestor de Soluciones Senior de Ericsson, desarrolló una ponencia sobre las Redes WLAN y la 3ª Generación de Comunicaciones Móviles desde el punto de vista del fabricante. Comenzó con los conceptos básicos sobre Wireless LAN y la situación creciente del mercado, destacando el crecimiento del número de PC's portátiles en uso con WLAN y del número de ubicaciones WLAN públicas (hotspots). Esto es debido a que se permite el uso de aplicaciones ya conocidas, a los avances tecnológicos, al bajo coste y a ser una tecnología complementaria de otras.

Tras dar un repaso detallado a los diferentes estándares WLAN existentes y a su evolución, que permitirá el acceso a servicios 3G desde WLAN o el "roaming" entre redes 3G y WLAN, **David Zafrilla** analizó el papel de los operadores móviles en relación con WLAN y estableció una comparativa entre la tercera generación (3G) y las redes WLAN, que pueden incluso compartir emplazamientos, para llegar a la conclusión de que son complementarias. Para ello presentó el concepto de arquitectura MOWLAN como el complemento perfecto para Redes Móviles.

Otro aspecto importante analizado fue la seguridad en comunicacio-



Ricardo Alvarío.

nes WLAN, la seguridad en el interfaz aire y la seguridad en el acceso a la red: Usuario y password estático, autenticación OTP (One Time Password) y autenticación por SIM.

Dentro de la demanda de servicios el ponente hizo hincapié en las Comunicaciones Móviles de Interior (Cobertura Celular Dedicada IN-BUILDING) que permiten acceder mediante WLAN a la Red Corporativa y a Estaciones Base de Radio en aeropuertos, estaciones de tren, edificios de oficinas, hoteles, centros comerciales, hospitales, etc.

**Javier Pedernal Rubio**, Jefe del Dpto. de Radio y Planta Interna de Telefónica, desarrolló la ponencia "Prospectiva sobre el impacto de las Redes de Acceso Inalámbrico en la Redes Públicas de Telecomunicación: la visión de un Operador"

**Javier Pedernal** presentó los servicios Wi-Fi que presta actualmente el operador, describiendo la operativa y arquitectura de cada servicio:

- Zona ADSL Wi-Fi: Servicio de acceso a Internet en lugares públicos como hoteles, restaurantes, ... (Hot Spots) basado en tecnología Wi-Fi (802.11) con movilidad entre los Hot Spots de Telefónica y

acceso a la red mediante línea ADSL.

- Solución ADSL Zona Wi-Fi: Servicio muy similar al anterior, pero sin movilidad entre Hot Spots.
- Soluciones ADSL LAN Wi-Fi Básica: Servicio orientado a empresas para dar conectividad a la Red Local del cliente, permitiendo movilidad entre ubicaciones del cliente, con encriptación y autenticación Wi-Fi. El cliente puede gestionar sus usuarios.
- Soluciones ADSL LAN Wi-Fi Premium: Orientado a visitantes, sólo permite conectividad con Internet.
- Wi-Fi en Ibercom: en fase de implementación y que tiene como objetivo proporcionar extensiones móviles de cada PABX, con numeración integrada y facilidades de usuario, utilizando teléfonos Wi-Fi, PDA con softphone u ordenadores portátiles.

También se refirió a las variantes y mejoras de servicios en fase de realización y a nuevos servicios como el *Roaming* Wi-Fi Nacional e Internacional.

Por último, **Javier Pedernal** analizó la evolución del Wi-Fi al WIMAX que tiene como objetivo extender la Banda Ancha como acceso por defecto, para todos los clientes y como soporte a todos los servicios, mediante acceso permanente entre casa y la oficina o acceso fijo.

En cuanto a la disponibilidad, se prevé la siguiente evolución: Acceso (2005) — Nomadicidad (2006) — Movilidad (2007).

**Francisco Javier García Vieira**, Subdirector Adjunto de Tecnología de RED.ES, desarrolló la ponencia: “Aplicaciones Públicas de las WLAN”, presentando en primer lugar las funciones asignadas a Red.es, Entidad Pública Empresarial, adscrita al Ministerio de Industria, Turismo y Comercio:

- Gestión de los dominios “.es”.
- Creación del “Observatorio de las Telecomunicaciones y de la Sociedad de la Información”.
- El asesoramiento a la Administración General del Estado en el ámbito de las telecomunicaciones y la sociedad de la información.
- El fomento y desarrollo de la Sociedad de la Información.
- Actuando como catalizador entre los proveedores de Tecnología y Servicios y las diferentes Administraciones.

García Vieira también pasó revista a los Programas de desarrollo de la Sociedad de la Información:



Asistentes a la jornada de redes de banda ancha durante la conferencia de Jorge Pérez.

Dentro de las Actuaciones en educación destacó el “Internet en la Escuela” cuyo objetivo es la introducción de las TIC en los centros educativos (Aula de Informática), y que lleva a cabo la “Red de centros educativos pilotos”. La “segunda fase, “Internet en la Escuela” tiene como objetivo la integración del uso de las TIC en todo el ámbito educativo.

“Internet Rural” tiene como objetivos lograr que los ciudadanos de zonas rurales dispongan de acceso, público y de calidad, a Internet mediante la creación de centros de Acceso Público.

Con “Internet en las Bibliotecas” se pretende que todas las bibliotecas públicas tengan conexión de acceso a Internet de Banda Ancha y con redes de área local.

Según **Francisco Javier García**, el uso de WLAN´s en los Programas de desarrollo de la SI, presenta múltiples ventajas, inherentes a la tecnología utilizada.



El uso de WLAN en los programas “Internet Rural e Internet en las Bibliotecas” ha posibilitado la instalación de Hot Spots que han permitido extender el alcance de los proyectos y multiplicar su impacto. En el programa “Internet en la Escuela” se ha aprovechado la movilidad y flexibilidad de las WLAN para dar cobertura a la totalidad de los centros educativos sin necesidad de cablear todas las aulas.

El director general de Telecomunicaciones y Tecnologías de la Información, del Ministerio de Industria, Turismo y Comercio, **Bernardo Lorenzo Almendros**, clausuró la jornada. En su discurso destacó la utilidad de la jornada donde se trataron aspectos regulatorios y se hizo referencia al desarrollo reglamentario de la Ley General de Telecomunicaciones. Una Ley estructurada en dos grandes reglamentos: uno relativo a los mercados y otro relativo a los servicios, en el cual se tratan aspectos que afectan a la colaboración de los operadores con la Administración en cuestiones de seguridad pública y defensa nacional. ☁

# “XI JORNADAS DE TECNOLOGÍAS PARA LA DEFENSA Y LA SEGURIDAD”

El Centro Superior de Estudios de la Defensa Nacional (CESEDEN) fue la sede, durante los días 24 y 25 de noviembre, de las “XI Jornadas de Tecnologías para la Defensa y la Seguridad”. La cita bienal del Círculo de Tecnologías para la Defensa y la Seguridad y que dio origen a su creación.

En esta undécima edición el encuentro estaba titulado “**Conocimientos y aplicaciones emergentes**” y fue inaugurado por el jefe del Estado Mayor del Ejército, general de Ejército, **José Antonio García González** y por el presidente del Círculo de Tecnologías para la Defensa y la Seguridad, **Arsenio Huergo Fernández**, a quienes acompañó el director del CESEDEN, Teniente General **Domingo Marcos Miralles**.

La primera Jornada estuvo dedicada a “**TÉCNICAS DE DETECCIÓN Y VIGILANCIA**” (Sensores heterogéneos, ubicuos y



De izq. a drcha. Marisol Martínez Tirado, Domingo Marcos, José Antonio García González y Arsenio Huergo.



De izq. a drcha. José Luis Orts, Félix Simón, Antonio Cieza, Antonio Cabello y Vicente Sánchez Gálvez.

conectados en red para obtener más información, de mayor eficiencia y en tiempo real) y fue presidida por **Julio Ángel Martínez Meroño**, director general de Infraestructuras y Material de la Seguridad del Ministerio del Interior

En ella se expusieron y debatieron las diferentes técnicas empleadas, incluyendo tecnologías tan diversas como las aplicadas en la detección de agentes químicos y biológicos, los biosensores y los diversos sensores electromagnéticos.

Los sensores electromagnéticos, químicos y biológicos serán uno de los elementos fundamentales de los presentes y futuros sistemas para la seguridad y la defensa por su papel en la obtención de los datos básicos que permiten el funcionamiento de los sistemas de armas, de mando y control, inteligencia, etc. Las nuevas amenazas requerirán la conexión de los sensores mediante redes que permitan disponer de la información en cualquier punto y en tiempo real, facilitando la rápida y eficaz toma de decisiones.

La segunda Jornada tuvo por objeto tecnologías emergentes más significativas en "**Sistemas de protección y armas**", y estuvo presidida por el general de división del Ejército del Aire, **Antonio Cieza González**, subdirector general de Tecnología y Centros del Ministerio de Defensa. En ella se describieron los nuevos enfoques en sistemas de protección y los desarrollos actuales en materiales para este fin. Las armas no letales, las nuevas tendencias en robótica y las tecnologías emergen-

tes (MEMS y nanotecnologías) para realizar los sistemas de armas completaran la Jornada. Nuevos conceptos y materiales para la protección frente a armas de precisión y adaptadas a la amenaza:

Para enfrentarse a las nuevas armas inteligentes, caracterizadas por su precisión y capacidad de destrucción limitada y concentración de sus efectos sobre objetivos aislados en entornos sensibles, las tecnologías de nuevos materiales pondrán a disposición del combatiente modernos y eficaces sistemas de protección que deberán disponer de nuevas armas, incluidas las no letales, adaptadas a conflictos asimétricos. De este modo aparece un nuevo combatiente que hace uso extensivo de las tecnologías disponibles y se convierte en un elemento más de los sistemas de comunicación e información desplegados en el escenario del conflicto y un usuario privilegiado de los mismos.

La última Jornada se dedicó al "**Mando y control, comunicaciones y gestión de la información**" (Tecnologías digitales en los futuros escenarios de conflicto, hacia las batallas de la información) y fue presidida por el Contralmirante **Manuel Otero Penelas**, jefe de la División de Sistemas de Información y Telecomunicaciones del Estado Mayor Conjunto.

A lo largo de la misma se analizaron las tecnologías esenciales para conservar una posición de ventaja con respecto a potenciales adversarios en los presentes y futuros escenarios de conflicto.

La adquisición de información, su procesado, protección y distribución en tiempo real; la prevención de ataques sobre las redes y sistemas propios; y la capacidad de acceder y destruir los sistemas de comunicación e información del enemigo serán objetivos prioritarios para las fuerzas armadas y cuerpos de segu-

ridad del Estado. Las tecnologías digitales ampliarán las dimensiones del campo de batalla convencional a nuevos escenarios caracterizados por combates físicos y lógicos a larga distancia sobre tierra, mar, aire, espacio y ciberespacio.

Las Jornadas se completaron con dos conferencias magistrales, de inauguración y cierre, a cargo de los Ministerios de Industria y Defensa.

En la primera de ellas, a cargo de **Salvador Luis Soriano Maldonado**, subdirector general de Servicios de la Sociedad de la Información, del Ministerio de Industria y Turismo y Comercio, se presentó **“El papel de las tecnologías de Seguridad y Defensa en el desarrollo de la Sociedad de la Información. Iniciativas en el Ministerio de Industria”**.

Por otra parte, el general de división del Ejército del Aire, **Antonio Cieza González**, subdirector general de Tecnología y Centros, describió el **Observatorio Tecnológico** que recientemente ha creado el Ministerio de Defensa.

Las jornadas fueron clausuradas por el Secretario de Estado de Seguridad del Ministerio del Interior, **Antonio Camacho Vizcaíno**, quien puso de relieve la idoneidad de la convocatoria, así como el apoyo de su departamento a este tipo de iniciativas que fomentan la investigación en Defensa y en Seguridad, tanto desde la Administración como desde la universidad y las empresas.

Esta undécima edición de las Jornadas de Tecnologías para la Defensa y la Seguridad, destacó especialmente por la importante presencia académica y del mundo de la investigación con participación de representantes de la Universidad Complutense de Madrid, Universidad Autónoma de Madrid, Universidad Politécnica de Madrid, Universidad de Sevilla, Universidad Politécnica de Cataluña, Consejo Superior de Investigaciones Científicas e Instituto Nacional de Técnica Aeroespacial.

Como también es habitual en estos encuentros del “Círculo” participaron representantes de los ministerios de Defensa: Interior, Industria, Turismo y Comercio y Educación y Ciencia, tanto como del Ministerio de Defensa de Suecia, y de las Fuerzas y Cuerpos de Seguridad del Estado.

Y las industrias del sector participaron dentro de la denominada “sesión Póster”, en la que presentaron sus productos:

ALCATEL, AMPER, CETECOM, CISCO, EADS TELECOM, GMV, PAGE IBÉRICA, ROHDE & SCHWARZ ESPAÑA, SECUWARE, SENER, SGI, SIMAVE, SOFTWARE AG, TECNOBIT y TECOSA.

Todas las ponencias presentadas en las jornadas, junto con las exposiciones de las industrias, serán recogidas en un libro, que constituirá el XI volumen de la colección Fórum de Electrónica Militar, y que se presentará próximamente. ☺



De Izq. a drcha. Domingo Marcos, Antonio Camacho, Jose Antonio García González y Marisol Martínez Tirado.

# “SEMINARIO INTERNACIONAL RAMSS”

Métodos y Tecnología organizó el Seminario Internacional RAMSS (*Reliability, Availability, Maintainability, Safety and Supportability*) el pasado 2 de Diciembre de 2004 en el Hotel Westin Palace de Madrid con el objetivo de acercar experiencias y técnicas empleando la ingeniería de sistemas de empresas europeas para mejorar la fiabilidad de los productos.

La amplísima participación, que alcanzó el centenar de asistentes de las principales empresas del mercado español confirma que existe una gran inquietud técnica por este tema.

**Santiago Jaraba** y **Luis Redondo**, de Métodos y Tecnología, en sus respectivas ponencias de “**Vista general de la tecnología empleada en RAS**” y “**Fiabilidad y Disponibilidad en Sistemas Intensivos en Software**”, expusieron todo un conjunto de métodos y técnicas perfectamente aplicables en organizaciones dedicadas al diseño de sistemas HW/SW. Técnicas que están empleando con sus actuales clientes en prácticamente todos los sectores del mercado como telecomunicaciones, energía, banca, industria y ferroviario.

En su intervención **Luis Redondo** resaltó que en general todos los usuarios exigen software más fiable, desarrollado más rápidamente y más barato. Tres características que tienen claros conflictos entre ellas mismas.



De izq. a drcha. Marisol Martínez Tirado, Paul Mann, Teodoro Bajo y Santiago Jaraba.

Por otra parte existen numerosas razones por las que debemos asegurar un mínimo de fiabilidad en los productos, tanto tangibles como intangibles.

La *reputación* de una compañía está muy relacionada con la fiabilidad de sus productos. Cuanto mayor es la fiabilidad de sus productos, más posibilidades tendrá de tener una buena reputación.

También son importantes los *costes de las garantías*. Si los productos fallan durante el periodo de garantía, los beneficios de la compañía se verán significativamente reducidos por los costes de reparación y reemplazo de los productos defectuosos.

Además también hay que tener en cuenta los efectos medioambientales, económicos y de vidas humanas que puede ocasionar un sistema que no funcione como se tenía previsto.

A lo largo de la jornada se hizo referencia a un Proyecto PROFIT I+D+i, cofinanciado por el Ministerio de Industria, Turismo y Comercio y por el Fondo Social Europeo, de diseño e implementación de un banco de pruebas para Sistemas Intensivos en Software, denominado RAMSes (“RAMS español”). Actualmente, dicho proyecto se está realizando en un consorcio de empresas y universidades españolas liderado por Métodos y Tecnología. Las principales características innovadoras de este banco de pruebas son que permitirá inyectar defectos hardware y errores software en los sistemas bajo prueba con el objeto de poner a los mismos en situaciones extremas y poder comprobar su comportamiento antes de pasarlos a explotación. El producto resultante de este proyecto se convertirá en una herramienta indispensable en las empresas de diseño de sistemas TIC para predecir y asegurar la fiabilidad y la disponibilidad de sus sistemas.

**Paul Mann**, de la empresa PMSC, en su ponencia de **The Application of RAMS in large scale Complex Railway Projects**, hizo ver cómo es imprescindible gestionar sistemática y organizadamente la seguridad en el desarrollo de los sistemas ferroviarios mediante la utilización de la técnica de los *Safety Case*.

**Ramón Somoza**, de la empresa EADS-CASA, en su conferencia de **“Requisitos de Fiabilidad y Safety”** en sistemas de Aviónica, presentó todo un conjunto de normativas aplicables en el desarrollo y operación de los sistemas de aviónica cuyo objetivo es aumentar su fiabilidad, disponibilidad y *safety*.

**Michelle Penny**, de la empresa ISOGRAPH, en su ponencia de **“Moving RAMS theory into practice”**, recomendó emplear herramientas software para poder realizar los análisis de fiabilidad y disponibilidad. ☺

# “PROGRAMA EUROPEO DE INVESTIGACIÓN EN SEGURIDAD (ESRP)”

El salón de actos del Centro para el Desarrollo Tecnológico e Industrial (CDTI) del Ministerio de Industria, fue la sede el pasado 14 de enero de la presentación del Programa Europeo de Investigación en Seguridad (ESRP), en un acto organizado por el Círculo de Tecnologías para la Defensa y la Seguridad en colaboración con el CDTI.

La jornada fue abierta por el director general del CDTI, **Maurici Lucena**, quién después de dar la bienvenida a los asistentes, presentó y dio la palabra a los ponentes invitados en la mesa inaugural.

Habló en primer lugar **Arsenio Huergo**, presidente de la Fundación Universidad-Empresa. Resaltó en su discurso lo oportuno de la convocatoria de la jornada y de su adecuación a la línea de actuación del Círculo, al plantear un debate en torno a algo tan próximo a las inquietudes de los ciudadanos y de los profesionales en particular, como es el concepto de seguridad.

A continuación habló **Javier Monzón**, presidente de INDRA, quien agradeció la invitación a participar en la jornada.



De izq. a drcha. Arsenio Huergo, Maurici Lucena, Antonio Camacho, Javier Monzón y Marisol Martínez Tirado.

nada. Donde participó desde su posición de primer ejecutivo de una empresa española con importante actividad en el área de seguridad. y como miembro que fue del Grupo de Personalidades convocado por la Comisión Europea (CE), para sugerir las acciones que esta debería emprender para avanzar en el campo de la investigación en Seguridad.

**Monzón** aportó algunas de las ideas clave desarrolladas por el Grupo de Personalidades en su informe final, haciendo hincapié en la necesidad de poner en marcha urgentemente un programa de investigación en seguridad, suficientemente dotado económicamente por la CE, que aunase los esfuerzos de las empresas, centros de investigación y universidades, sin olvidar la fundamental participación de los usuarios finales.

Asimismo expresó la necesidad de que, aunque los proyectos pudiesen tener carácter precompetitivo, deberían estar principalmente pensados en ayudar a resolver necesidades específicas de dichos usuarios finales.

Por último tomó la palabra. **Antonio Camacho**, Secretario de Estado de Seguridad, quién expresó el gran interés que existe en su Ministerio por todas las iniciativas que se están tomando en torno al concepto de la seguridad, y en particular por el programa Europeo de Investigación en Seguridad (ESRP), objeto de la presente jornada.

Insistió en la necesidad de que los usuarios finales, y en concreto las Fuerzas y Cuerpos de Seguridad del

Estado, participen activamente en las propuestas y en el desarrollo de los proyectos dentro del ESRP, para asegurar la utilidad del esfuerzo tanto humano como económico, qué el programa va a exigir.

Significó la importancia del concepto de investigación ya que sin ella no se podrán dominar las tecnologías necesarias para dar respuesta a las amenazas que se plantean a nuestra sociedad.

Finalmente, el Secretario de Estado animó a las empresas, centros de investigación y universidades a participar activamente en el ESRP y a conseguir el retorno económico y tecnológico que le corresponda a España en el mismo.

Después de una pausa en el programa, le correspondió a **Herbert Von Bose**, Jefe de Unidad en la CE, presentar los objetivos, situación y próximas acciones del ESRP.

Tras recordar las iniciativas políticas que estaban detrás de la idea de desarrollar un programa de estas características, **Von Bose** explicó las áreas que la CE estaba estudiando para ponerlo en marcha.

En primer lugar habló del área de "Consulta y Cooperación". La CE está estableciendo un grupo asesor en investigación de seguridad para orientar debidamente el desarrollo del ESRP. También se está estudiando fórmulas para coordinar debidamente este programa con otros pro-



Herbet von Bose.



Asistentes a la jornada (ESRP).

gramas nacionales o intergubernamentales del mismo dominio de actividad.

Una segunda área se refería al lanzamiento del propio ESRP, que se pretende hacer en enero del 2007, como un subprograma específico del VII Programa Marco Comunitario de I+D. La CE está estudiando el nivel apropiado de financiación que se deberá arbitrar para alcanzar los objetivos propuestos.

Por último citó un área de carácter institucional, recordando la importancia de desarrollar la cooperación con otros organismos activos en la Unión Europea, y en concreto con la Agencia Europea de Defensa.

En su presentación, Herbert von **Bose** explicó el estado de la llamada "acción preparatoria", previa al lanzamiento del ESRP, definiendo en primer lugar los objetivos de la misma. Son fundamentalmente el verificar la adecuación de los procedimientos de gestión existentes a los objetivos planteados para el programa definitivo e ir orientando las tecnologías que serán prioritarias en su desarrollo.

Después de afirmar que el presupuesto total para la acción preparatoria sería de 65 millones de euros con una financiación de hasta el 75 % de los gastos totales de los proyectos, **Von Bose** explicó el estado de las dos primeras convocatorias. Para la primera hay ya aprobados siete proyectos y cuatro actividades de soporte, que están poniéndose en

marcha en estos momentos. En los consorcios seleccionados hay dos empresas españolas, GMV e INDRA Espacio.

La segunda convocatoria puesta en marcha a comienzos de febrero, y cuenta igual que la primera, con 15 millones de euros de ayuda por parte de la CE.

Al final de la presentación tuvo lugar un animado debate entre el ponente y la sala.

**Javier Cañizares**, representante Nacional de aeronáutica y Espacio del CDTI, habló sobre las modalidades de participación en el Programa Marco, en el que, como se ha dicho anteriormente, se encuadrará el ESRP.

**Javier Cañizares** explicó en términos prácticos las normas establecidas por la CE para regular y facilitar la participación de las empresas, universidades y centros de investigación en los consorcios que obligatoriamente deben establecerse para proponer y, en su caso, desarrollar, los proyectos concretos de I+D. También habló del papel de los usuarios finales en estas iniciativas.

A continuación, y en una corta mesa redonda moderada por la directora del Círculo de Tecnologías para la Defensa y la Seguridad, las dos empresas españolas protagonistas en la primera convocatoria de la





Javier Cañizares

acción preparatoria, expresaron sus experiencias particulares.

En primer lugar fue **Alberto de Pedro**, de la empresa GMV, quién explicó los antecedentes de la convocatoria y como la misma se adecua perfectamente a las estrategias de la empresa en actividades de seguridad. GMV participa en uno de los proyectos seleccionados, el proyecto ISCAPS (vigilancia integrada de zonas con afluencia masiva de personas para la seguridad pública), y en la acción de soporte Geo Crew, (estudio sobre la utilización de información geo-espacial para la mejora del conocimiento de las situaciones y concepto de arquitectura para la alerta temprana de crisis).

En segundo lugar, **Victoriano Moreno**, de la empresa INDRA Espacio, presentó el proyecto ASTRO + de tecnologías espaciales avanzadas para soporte a actividades de seguridad. Detalló la génesis del mismo y la contribución de INDRA Espacio al desarrollo del proyecto dentro del consorcio seleccionado.

Las dos presentaciones fueron muy prácticas, en el sentido de que los ponentes aportaron experiencias reales habidas en el largo periodo de preparación y aprobación de las propuestas, y consejos muy claros

sobre donde y como poner el énfasis para hacer lo más atractivas posibles las propuestas. De cara a su evaluación por los responsables de la CE a conseguir la participación más interesante posible, en cuanto a su contenido tecnológico dentro de los consorcios.

La jornada finalizó con una nueva mesa redonda sobre “El punto de vista de los usuarios. Las necesidades operativas y la respuesta tecnológica”, en la que el general de la Guardia Civil, **Ángel García-Fraile**, subdirector de Planificación del Ministerio del Interior, llevó a cabo una interesante presentación en relación con la “Lucha contra el terrorismo y la delincuencia organizados. Acciones y proyectos”.



Asistentes a la jornada.

En su intervención empezó repasando las medidas en curso en el ámbito europeo para afianzar la cooperación, tanto de índole legislativo como operativo, con especial énfasis en los sistemas de información.

Continuó describiendo los objetivos estratégicos del plan de la Unión Europea para la lucha antiterrorista, y relacionó los mismos con la iniciativa de la CE de poner en marcha el ESRP. Enfatizando de esta manera la importancia de la tecnología para poder alcanzar dichos objetivos.

**José Luis Díez Aguado**, jefe de Servicio del Área de Seguridad del Ministerio del Interior, habló de la “Confidencialidad y utilización del PKI por las fuerzas y cuerpos de seguridad del estado”.

La necesidad de compartir información para conseguir una mayor efectividad en la lucha contra el terrorismo y el crimen organizado, debe hacerse compatible con la seguridad de los procesos y los sistemas utilizados.

**Díez Aguado** habló de la plataforma de servicios de seguridad y de las aplicaciones y tecnologías con ella relacionados.

La jornada terminó con un cóctel en el que los asistentes tuvieron ocasión de profundizar con los ponentes en algunos de los temas desarrollados a lo largo de la sesión. ☺

# CLAUSURA 2ª EDICIÓN CURSOS DE FORMACIÓN CONTINUA Y APERTURA 4ª EDICIÓN ESPECIALIDAD EN SISTEMAS DE COMUNICACIÓN E INFORMACIÓN PARA LA SEGURIDAD Y LA DEFENSA

Entre los objetivos marcados en el Plan Director CIS se incluye el mejorar la cualificación del personal técnico del MINISDEF. Por ello la Inspección General CIS está trabajando activamente en este sentido con el Círculo de Tecnologías para la Defensa y la Seguridad y la Universidad Politécnica de Madrid (UPM).

Entre las acciones que se han llevado a cabo hasta la fecha se encuentra la de potenciar y aumentar la participación del personal del Departamento en las sucesivas ediciones que se viene impartiendo del Curso de Postgrado – Especialidad en Sistemas de Comunicación e Información para la Seguridad y la Defensa. Dicho curso es organizado por la Escuela Técnica Superior de Ingenieros de Telecomunicación (ETSIT) de la Universidad Politécnica de Madrid, a través del “Círculo”, y que cuenta con el patrocinio de la Inspección General CIS y de diversas empresas del sector. Gracias a la intervención de la Inspección se ha incrementado el número de becas previstas para alumnos del MINISDEF, que han

pasado de 14 en la 1ª edición a las 22 de la 2ª, 3ª y 4ª (en la práctica realizan el curso más alumnos, puesto que hay becas de otros organismos y empresas que nos ceden).

En línea con lo anterior y con objeto de profundizar en los campos concretos de actividad que fueron tratados o apuntados en la Especialidad citada, la Inspección General ha patrocinado las 2 ediciones que hasta la fecha se han impartido de una serie de cursos de formación continua.

Todo ello está orientado a la posible configuración en un futuro de un Master en Sistemas de Comunicación e Información para la Seguridad y la Defensa. Un máster incluiría en su programa, entre otras, las materias impartidas en estos cursos; por lo que las enseñanzas recibidas podrían convalidarse por créditos del futuro Master.

En sintonía con estos objetivos, el pasado 16 de noviembre, en el salón de actos de la Escuela Técnica Superior de Ingenieros de Telecomunicación, de la UPM, se celebró un acto conjunto de apertura y clausu-

ra de los cursos, presidido por el Inspector general CIS del Ministerio de Defensa, vicealmirante **Simeón Cantó Antolí**, y por el director de la Escuela, **Guillermo Cisneros**, contando asimismo con la presencia del director del Postgrado, **Juan Riera** y del director de la Especialidad **Félix Pérez**.

#### **CLAUSURA 2ª EDICIÓN CURSOS DE FORMACIÓN CONTINUA AÑO 2004**

Los cursos de formación continua impartidos durante el año 2004 han constado de 60 horas lectivas, estructuradas en 3 módulos independientes

- **Servicios y Redes TCP/IP.**

Fechas: 7 al 16 de junio.

Duración: 20 horas (2 créditos).

Alumnos matriculados: 32

- **Seguridad de Redes de Comunicaciones**

Fechas: 20 al 30 de septiembre.

Duración: 20 horas (2 créditos).

Alumnos matriculados: 29

- **Comunicaciones, localización y radionavegación por satélite.**

Fechas: 4 al 18 de octubre.

Duración: 20 horas (2 créditos).

Alumnos matriculados: 40

#### **ACTO DE APERTURA 4ª EDICIÓN ESPECIALIDAD EN SISTEMAS DE COMUNICACIÓN E INFORMACIÓN PARA LA SEGURIDAD Y LA DEFENSA 2004-2005.**

La 4ª Edición de la Especialidad se estructura, de forma similar a ediciones anteriores, en un total de 130 horas lectivas, distribuidas en 6 módulos de 20 horas cada uno y una serie de conferencias que completan los créditos totales. Las clases se imparten a razón de 3 horas diarias (de 17:00 horas a 20:00 horas) de lunes a jueves.

Como novedad con respecto a ediciones anteriores significar que se han incorporado 2 nuevas empresas patrocinadoras: ALCATEL e INDRA, que se añaden a las ya habituales AMPER, GMV, ISDEFE, ROHDE SCHWARZ, TECNOBIT Y TELEFÓNICA.

El calendario previsto y número de alumnos matriculados son los siguientes:

- Fechas: 17 de noviembre de 2004 al 24 de febrero de 2005.
- Alumnos matriculados: 40



Acto conjunto de apertura, clausura y entrega de diplomas de la 4ª edición de la de Especialidad en Sistemas de Comunicación e Información para la Seguridad y la Defensa y 2ª Edición de los cursos de Formación Continua.

# CLAUSURA DE LA JUNTA DIRECTIVA

**El secretario de Estado de Defensa, Francisco Pardo, clausura la Junta Directiva del Círculo de Tecnologías para la Defensa y la Seguridad**

La Junta Directiva del Círculo de Tecnologías para la Defensa y la Seguridad celebró, el 7 de marzo, su reunión anual en la Cámara Oficial de Comercio e Industria de Madrid, presidida por Arsenio Huergo Fernández, presidente de la Fundación Universidad-Empresa.

En la asamblea se aprobaron el informe de gestión de 2004, la agenda de actividades de 2005, así como el presupuesto y la renovación de miembros en el Comité Ejecutivo y la Junta Directiva, tras las elecciones celebradas el 24 de febrero.

En su intervención, el presidente resaltó el gran número de actividades realizadas durante el Ejercicio y la importante y también numerosa respuesta por parte de los asistentes.

El vicepresidente Humberto Figarola, puso de relieve la destacada actividad del "CÍRCULO", por el número de actos celebrados, así como por el poder de convocatoria y el buen ambiente creado y mantenido entre la Universidad, la Administración y las empresas.

Al almuerzo de clausura de la Junta asistió como invitado de honor el secretario de Estado de Defensa, (SEDEF) Francisco Pardo Piqueras, quien felicitó al "CÍRCULO" por su trabajo. En su discurso, el SEDEF tendió la mano a las empresas asistentes recordando que el aumento

presupuestario del Ministerio de Defensa para operatividad, tendrá continuidad en los próximos años.

Acompañando al secretario de Estado en esta sesión de clausura, estuvieron presentes, Fernando Fernández-Tapias, y José María Isardo, presidente y director general de la Cámara de Comercio e Industria de Madrid; el jefe del Estado Mayor de la Defensa (JEMAD), general de ejército, Félix Sanz Roldán; el jefe del Estado Mayor del Ejército (JEME), general de ejército, José Antonio García González; el almirante jefe del Estado Mayor de la Armada (AJEMA), almirante general, Sebastián Zaragoza Soto; el jefe del Estado Mayor del Aire, general del Aire, Francisco José García de la Vega; el director general de la Guardia Civil, teniente general del Ejército del Aire, Carlos Gómez Arruche y el presidente de la comisión de Defensa del Congreso de los Diputados, Joaquín Leguina Herrán, además de presidentes y consejeros delegados de las empresas del sector.

Por parte del Círculo de Tecnologías para la Defensa y la Seguridad, asistieron el presidente Arsenio Huergo Fernández; el director gerente de la Fundación Universidad-Empresa, Fernando Martínez Gómez; los vicepresidentes: Violeta Demonte Barreto, directora general de Investigación del Ministerio de

Ciencia y Tecnología; Carlos Villar Turrau, director general de Armamento y Material del Ministerio de Defensa; Julio A. Martínez Meroño, director general de Infraestructuras y Material de la Seguridad del Ministerio del Interior; Humberto Figarola Plajà, vicepresidente de INDRA y la directora del "CÍRCULO", Marisol Martínez Tirado.



De izq. a drcha., Francisco Pardo, Fernando Fernández Tapias, Joaquín Leguina y Humberto Figarola.



El JEMAD y los tres Jefes de Estado Mayor de los tres ejércitos.

La Junta Directiva del Círculo de Tecnologías para la Defensa y la Seguridad, en su reunión del pasado 7 de marzo aprobó la incorporación a sus órganos de gobierno, de los siguientes vocales:

Por parte de ISDEFE, se incorpora a la Junta Directiva, **Miguel Ángel Panduro Panadero**, Consejero Delegado de ISDEFE, en sustitución de Luis Julve Guerrero. De INDRA, se une a la Junta Directiva y al Comité Ejecutivo **Francisco Navarro Rodríguez**, en sustitución de Antonio de Carvajal Salido.

Además este año, tal y como contempla nuestro Reglamento, corresponde renovar la las vocalías de la Junta Directiva. Tras las elecciones celebradas el pasado 24 de febrero de 2005, resultaron elegidas las siguientes empresas que mantendrán sus cargos durante cuatro años, los dos primeros en la Junta Directiva y los dos últimos, además, en el Comité Ejecutivo.

Dentro de la Categoría B se incorporan **SENER** y **TELEFÓNICA MÓVILES** y en la Categoría C **SIMAVE**.

En consecuencia se unen a la Junta Directiva **Jorge Deza Enríquez**, de SENNER, **Antonio Mora Villanova**, de TELEFÓNICA MÓVILES y **Adolfo Ferreiro Martín**, de SIMAVE.

Además, pertenecerán al Comité Ejecutivo los próximos dos años, los representantes de AMPER, **Francisco Soler Pozuelo**; de GMV, **Manuel Pérez Cortés** y de PAGE, Ramiro **Sánchez Reviriego**, en sustitución, este último, de Carlos Borrego Díaz. ☺



Los vicepresidentes del "Círculo", Humberto Figarola, Violeta Demonte, Julio Martínez Meroño y Carlos Villar, en la Junta Directiva.



## LOCKHEED MARTIN ESPAÑA

Lockheed Martin España S.A., recientemente establecida como subsidiaria de Lockheed Martin Corporation, con la que se pretende reforzar la creación de alianzas industriales con empresas españolas, con el fin de servir y apoyar mejor a sus clientes nacionales explorando nuevas oportunidades de exportación de productos desarrollados conjuntamente y producidos en España.

Esta oficina es continuadora de una dilatada colaboración con las autoridades y empresas españolas cuyos primeros resultados se remontan a unos 50 años atrás.

Lockheed Martin suministra el sistema de combate AEGIS con el radar SPY-1 y el sistema de lanzamiento vertical MK 41 para las cuatro nuevas Fragatas F-100 de la Armada Española. Como resultado de la cooperación en este programa, el Ministerio de Defensa de Noruega seleccionó al equipo Izar-Lockheed Martin para el suministro de cinco nuevas fragatas para la Armada Noruega Real.

La Armada Española también cuenta con helicópteros SH-60B LAMPS Mk III para proteger a sus buques de ataques submarinos. En 1998 la Armada Española adquirió seis helicópteros multi-misión adicionales del tipo LAMPS Mk III y actualizó sus aviones existentes con la misma configuración.

Los aviones de transporte y de patrulla marítima Hércules C-130 y P-3 Orion han estado al servicio de las fuerzas aéreas españolas duran-

te muchos años. El sistema de combate Mark 92 y el sonar SQR-19 están en servicio a bordo de las fragatas Santa María desde los años 80 y los ordenadores UYK-43 son elementos fundamentales del sistema de combate del portaviones Príncipe de Asturias.

En la industria espacial Lockheed Martin ha contribuido al desarrollo de la industria de las telecomunicaciones españolas con tres satisfactorios lanzamientos de satélites Hispasat. La división espacial de EADS-CASA fue seleccionada para el suministro de adaptadores Inter-Stage y otros componentes para el lanzador Atlas V de la fuerza aérea norteamericana construido por Lockheed Martin.

EADS-CASA fue seleccionada por Lockheed Martin para suministrar los aviones de patrulla marítima de los guardacostas norteamericanos, los conocidos CN-235. También se seleccionó el sistema de la dirección de tiro Dorna de Izar, para la configuración básica del buque proyectado por Lockheed Martin que compite en el programa del Litoral Combat Ship de la U.S. Navy.

### LOCKHEED MARTIN GLOBAL INC.

Edf. Iberia Mart II  
c/. Orense 34, 7º  
28020 Madrid  
Telf.: 91 598 12 90



Izar e INDRA son importantes suministradores del programa AEGIS de Lockheed Martin en Japón, Corea y Estados Unidos. Recientemente INDRA fue seleccionada para el desarrollo del Módulo de Prueba F 18 para el CASS de la Armada Estadounidense y TECNOBIT ha ganado un contrato de suministro de cables y racks para el programa de Lockheed Martin SH-60R LAMPS de la Armada Estadounidense.

Lockheed Martin España tiene su sede central en Madrid, el consejero delegado es James R. Nelson, anteriormente vicepresidente de Operaciones Internacionales para Lockheed Martin Corporation. ☺

# NOTICIAS


## NAVANTIA, LA NUEVA EMPRESA ESPAÑOLA DE CONSTRUCCION NAVAL MILITAR

La nueva empresa española de construcción naval militar, fruto de la segregación de actividades de Izar, se llama Navantia. De esta manera la SEPI quiere garantizar la viabilidad de parte de los astilleros públicos ya que se ha fijado el objetivo de facturar anualmente en torno a los 1.400 millones de euros. Además se ha avanzado el programa anual de inversiones que gira en torno a los 90 millones de euros. La compañía tiene una cartera de pedidos por valor de unos 3.600 millones de euros.

En el acto de presentación de Navantia, el pasado 2 de marzo, estuvieron presentes el vicepresidente segundo del Gobierno y ministro de Economía y Hacienda, Pedro Solbes y el presidente de la Sociedad Estatal de Participaciones Industriales (SEPI), Enrique Martínez Robles.

Navantia seguirá operando en las instalaciones de Ferrol, Fene, Puerto Real, San Fernando, Cartagena y las oficinas administrativas de Madrid.

Las líneas de actividad girarán entorno a la construcción naval, fundamentalmente militar, aunque en sus competencias figura un 20% de actividad en materia civil. La nueva empresa también participará en líneas de actividad de propulsión y energía, reparaciones y sistemas y armas, todo ello con un alto componente tecnológico ya que de los más de 5.500 empleados de la nueva compañía, un millar son ingenieros o adscritos a las tareas de Investigación y Desarrollo (I+D).

El catálogo de productos de Navantia, ofrece la más amplia variedad de buques militares y de guardacostas con el fin de suministrar con plena fiabilidad tanto a la Armada Española, como a la de cualquier otro país. 

## JORNADA:

### “SISTEMAS DE AERONAVES NO TRIPULADAS”

Jueves 26 de Mayo

Instituto Nacional de Técnica Aeroespacial  
Ctra. de Ajalvir, km. 8 • 28850 Torrejón de Ardoz (Madrid)  
Horario de 10,00 a 18,30

Evitar bajas en cualquier conflicto es uno de los principales objetivos a los que se enfrentan los combatientes hoy en día. Un objetivo que se intenta alcanzar, entre otros muchos caminos, a través de los desarrollos tecnológicos. La investigación avanza y uno de las soluciones hacia las que apunta es la investigación y fabricación de aeronaves no tripuladas. Unas aeronaves que han alcanzado con éxito un alto nivel técnico y han permitido su aplicación operativa en todos los ámbitos militares y civiles.

Ciertos países con alta experiencia en su utilización en escenarios reales han alcanzado un alto desarrollo en estos sistemas y continúan investigando para obtener desarrollos en un amplio espectro de vehículos aéreos no tripulados que van desde los micro UAV a los futuros aviones de combate sin tripulación.

Todo ello induce a pensar que este campo tendrá una fuerte demanda y gran aplicación, a corto y medio plazo, lo que obliga a nuestra industria a posicionarse adecuadamente en esta carrera tecnológica, de aplicación dual y que socialmente será muy aceptada ya que evitará los riesgos y las limitaciones del factor humano. Por este motivo, por la fuerte demanda empresarial que los avances tecnológicos en materia de autotripulación, el Círculo de Tecnologías para la Defensa y la Seguridad ha organizado esta jornada. Demostrando una vez más el interés por estar apoyando el desarrollo de tecnológico dentro de la industria y la empresa.

#### PROGRAMA

- Sistemas de UAV's.
- Concepto de sistema.
- Aplicaciones.
- UAV's como Elemento de C<sup>4</sup> I
- UAV's como Elemento de combate
- Aplicaciones civiles
- Elementos del sistema
- Vehículo Aéreo
- Categorías y prestaciones.
- Tecnologías específicas.
- Cargas útiles
- Tipos y aplicaciones.
- Sensores diversos.
- Enlace de datos. Estación de Control en Tierra.
- Categorías y estrategias.
- Tratamiento de la información.
- Sistemas relacionados con la operación
- Despegue y aterrizaje.
- Lanzamiento y recuperación.
- Operaciones sobre el mar.
- Programas
- Programas españoles y europeos.
- Perspectivas para el próximo futuro.

El pasado 13 de abril, en el Salón de Actos de la Dirección General de la Guardia Civil, tuvo lugar la celebración de la jornada “**Internacional Protección de Infraestructuras Críticas**”, organizado por el “Círculo de Tecnologías para la Defensa y la Seguridad” y con la colaboración del Ministerio de Defensa, Ministerio de Industria, Turismo y Comercio, el Ministerio del Interior y el Ministerio de Educación y Ciencia.



Toda la información sobre esta jornada aparecerá en el número 55 del Boletín del Círculo de Tecnologías para la Defensa y la Seguridad.

## BOLETÍN DEL CÍRCULO DE TECNOLOGÍAS PARA LA DEFENSA Y LA SEGURIDAD

**Directora:** Marisol Martínez Tirado

**Sede:** Fundación Universidad-Empresa

c/ Santa Cruz de Marcenado, 33 - 1º 6

www.fue.es

secretaria@circulodefensa.com - 28015 Madrid.

Tel.: 91 540 02 06

Fax: 91 559 12 47

**Fotografía:** Jorge Brichette.

**Impreme:** Imprenta Gómez y González

**Depósito Legal:** M-18.835-1984.