Jornadas sobre tecnologías de la información para la modernización de las Administraciones Públicas.

TECNIMAP 2010. Zaragoza

Sesión 3- **SALA B** 7 de abril de 2010. 16,00 a 18,00 h

El papel de las TIC en la Defensa y la Seguridad ciudadana. Organización Ministerio Defensa.		
Moderadora: Dª Mónica Melle Hernández. Directora General de Infraestructura de Defensa. Ministerio de Defensa.		
Ponente	**Cargo**	**Organización**
D. Antonio Gibert Oliver	General de Brigada del Cuerpo General del Ejército del Aire (JDSIT)	Ministerio de Defensa
D. Federico Colás Rubio.	Subdirector General del Centro Criptológico Nacional	Ministerio de Defensa
D. Pedro Martín Jurado	Inspector General CIS	Ministerio de Defensa
D. Esteban Cueva Álvarez.	Subdirector General de Servicios Técnicos y Telecomunicaciones	Ministerio de Defensa
D. Manuel Ruiz Sánchez	Director Programas y Sistemas Terrestres	Asociación Española de Empresas Tecnológicas de Defensa, Aeronáutica y Espacio

RESUMEN PRESENTACIONES:

La primera ponencia presentada por el Sr Martín trató del gran reto de alinear el negocio con la tecnología en una organización.

La eterna duda: ¿Son las tecnologías son las que deben de adaptarse/alinearse con el negocio?, o por el contrario ¿Es el negocio el que debe adaptarse/alinearse con las tecnologías? . Negocio y TIC no son entes independientes tienen que encajar. Ciertamente el negocio es complejo y debe afrontarse con planes directores, desde la visión sistémica a servicios tecnológicos, de estos a servicios de negocio y a usuarios finales.

La forma de resolver el dilema es el PLANEAMIENTO, que partiendo de las necesidades, las estandarice y analice en un modelo de referencia (TIC-CIS), del cual emane un Plan Director, que se concretará en un programa Anual de Recursos y en su ejecución. Pero el Planeamiento requiere control de todo el proceso, aportación continuada de financiación, recursos humanos y soporte de la organización. Hay que actuar desde una posición organizativa que permita la observación y actuación en los dos mundos objeto del alineamiento (negocio y tecnología), por ello toda la inversión TIC se realiza en aras de objetivos de negocio. En todo caso son esenciales las políticas de recursos humanos que dimensionen y garanticen la competencia, y las políticas de recursos financieros que garanticen el ciclo de vida del recurso.

La segunda ponencia presentada por el General Gibert y de las capacidades CIS en las FAS

Las CIS (TIC en Defensa) son de dos tipos de propósito general (similares a las de cualquier Ministerio y las de Mando y Control (específicas de las Fuerzas Armadas).
El Sistema de mando y Control Militar (SMCM) tiene por objeto proporcionar a la JEMAD (Junta Estado Mayor de la Defensa) de un conjunto de capacidades básicas para poder desempeñar su misión

El SMCM tiene dos partes: El STM (Sistema de Telecomunicaciones Militares) y el SIM (Sistema de Información Militar). El STM tiene por objetivo satisfacer necesidades de telecomunicaciones precisas para la preparación y conducción de las operaciones militares, en paz, crisis y guerra. Es por tanto un sistema 24x7.

EL STM consta de un segmento terrestre y otro satelital, los satélites son el Spainsat y el XTAR , con vida útil hasta el 2023-24.,la cobertura del segundo abarca desde California a Singapur. La gestión del STM se basa en una Dirección centralizada, pero en una ejecución descentralizada.

La actividad CIS en operaciones expedicionarias exteriores implica una gestión centralizada en el centro gestor del Sistema al que reportan los enlaces terrestres y satelitales. La constante evolución de los terminales satélite posibilita ya enlaces en movimiento y despliegues rápidos de infraestructura. La operativa de las misiones expedicionarias tiene, entre otras posibilidades, las de enlaces cifrados, integración de voz y datos, y posibilidad de aprovechar satélites civiles.

La tercera ponencia presentada por el Sr Cueva trató de las Infraestructuras y Sistemas de Información en la Red Corporativa del Ministerio de Defensa.

El Ministerio de Defensa (MINISDEF) dispone de un entorno tecnológico muy complejo con 180.000 Registros en Directorio Corporativo, 86.000 Usuario, 67.000 PCs en red. Su dispersión es enorme con 664 emplazamientos, 9 emplazamientos en Misiones de Paz, y 40 emplazamientos en el extranjero.
La red de telecomunicaciones global del Ministerio tiene dos partes bien diferenciadas:

1º.- Telecomunicaciones de propósito general. Con Servicio de voz y datos a todos los usuarios del MINISDEF. Contratados a operadores públicos. Se basa en RPV para voz, fija y móvil, y para datos.
2º.-Telecomunicaciones de Mando y Control. Servicio de telecomunicaciones a los usuarios de mando y control. Es propiedad del MINISDEF.

La red corporativa de datos está basada en tecnología MPLS. La Confidencialidad e integridad de las comunicaciones están aseguradas mediante túneles IPSec. Otro aspecto clave es la cuestión de la Identidad digital en el Departamento, que se logra mediante 3 proyectos, a saber: PKIDEF: Emisión de certificados según Ley 11/2007; TEMD: Dispositivo seguro de creación de firma según Ley 59/2003; PSSDEF: Servicio de validación de certificados y firma para aplicaciones

El Ministerio de Defensa en su calidad de Prestador de Servicios de Certificación Electrónica proporciona: Certificado de firma de entidad final (persona), certificado de firma de entidad final (no persona), para tratamientos automatizados, y servicio de sellado de tiempo coordinado con el ROA. Se dispone de más de 57.000 tarjetas criptográficas en uso.

Cabe mencionar también el sistema de propósito general Sistema de Información de Mensajería de Defensa (SIMENDEF) que automatiza el procedimiento administrativo de registro, firma, archivo y envió de la correspondencia oficial. El sistema interconecta registros con transmisión de documentos firmados electrónicamente, con repositorio único y gestión documental.

La cuarta ponencia presentada por el Sr Colás del CNN trató del papel del Centro Criptológico Nacional, Organismo que tiene por misión garantizar la seguridad de los sistemas de información y comunicaciones de las administraciones públicas.

El CNN interviene y participa en tres grandes ámbitos de trabajo: 1.- Sistemas de la Administración, 2.- Sistemas de Seguridad y Defensa, 3.- Infraestructuras críticas y sectores estratégicos.
Una de sus actividades más conocidas del CNN es elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los Sistemas de las tecnologías de la información y las comunicaciones de la Administración.
Y también la de formar al personal de la Administración especialista en el campo de la seguridad de las TIC
Asimismo, realiza tareas de evaluación criptológica, auditorías funcionales de seguridad conforme a Common Criteria e ITSEC, y mediante el servicio TEMPEST es posible efectuar la medición de equipos, plataformas y locales, así como la validación mediciones realizadas por Laboratorios. El objetivo final de estas tareas de evaluación es facilitar el desarrollo de la Sociedad de la Información.
El CNN tiene una labor poco conocida en lo referente a sus tareas de coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad.
Un servicio a resaltar del CNN es su servicio/ equipo de respuesta ante incidentes y situaciones delicadas, en este caso su misión es ser el centro de alerta y respuesta de incidentes de seguridad, ayudando a las AAPP a responder de forma más rápida y eficiente ante las amenazas de seguridad que afecten a sus sistemas de información. En este apartado sus servicios se clasifican en proactivos, reactivos y de gestión.
La red interadministrativa SARA posee un Sistema de Alerta Temprana proporcionado por el CNN y tiene ya ultimado un proyecto de sensores en las salidas de Internet de las Administraciones Públicas, para detectar y atajar amenazas con este origen (se examinan los logs). Para usar este servicio hace faltar firmar Convenio con el CNN.

La quinta ponencia presentada por el Sr Ruiz de TEDAE (Asociación Española de Empresas de Tecnologías de Defensa, Aeronáutica y Espacio) trató de la visión del sector privado. Para ello basó su exposición y como hilo conductor el caso de la UME (Unidad Militar de Emergencias)

Nuevos retos en la coordinación

1. La proliferación de tecnología ha generado progreso, pero también sistemas de información disjuntos en los diversos organismos. Existen sistemas de información previos, no diseñados generalmente para poder interactuar con otros.
2. Interacción para compartir información, análisis, saber donde se encuentran las unidades de los otros actores, misiones que está realizando cada medio, como se asignan tareas/responsabilidades...
3. En coordinaciones OPERATIVAS donde el tiempo es un factor clave y decisivo, el tiempo real o tiempo útil.
4. La Información a integrar proviene de muchas fuentes, lo que provoca: Repetición de la información: Es necesario realizar una fusión de la misma. Recepción de informaciones contradictorias. Información parcial: Es necesario recopilar la información de todas las fuentes para determinar la foto global.
5. Toma de decisiones: Es fundamental contar con una idea clara, precisa y a tiempo de la situación. Diferentes actores pueden necesitar diferente información para la toma de decisión. Problemas por la saturación de información.

Retos de coordinación de emergencias

1. Gran diversidad de actores presentes, Tiene aun más importancia el posicionamiento de medios y conocer qué está realizando cada medio (misiones).

2. Evolución de emergencias: Ante determinadas emergencias (ej: incendios) es vital disponer de herramientas de apoyo que permitan estimar la evolución.

3. En el ámbito de la Defensa se han desarrollado conceptos y tecnologías para la coordinación efectiva de operaciones tales como: CROP: Common Relevant Operational Picture; NEC: Network Enabled Capability. Estas tecnologías, originalmente pensadas para Defensa, tienen su aplicación directa en áreas civiles.

Red Nacional de Emergencias RENEM

Objetivos de la RENEM son: Intercambio de información actual sobre incidentes; Sincronizar acciones durante la gestión de la crisis; Soporte a la toma de decisiones
Abarca y comprende a todos los operadores y agentes implicados (AA.PP, Protección Civil, Infraestructuras básicas, etc).La idea subyacente es la integración y coordinación de todas las redes de alerta. A RENEM se puede acceder vía red SARA o red IRIS.
El acceso a la RENEM se materializa de dos formas no excluyentes: Mediante portal web RENEM (con acceso restringido y con SSL), o mediante el protocolo CESAR (utiliza XML sobre web services), consistente en: Intercambio manual/automático de alertas y recursos mediante un lenguaje común. El Portal proporciona servicios tales como: Comunicación de Alertas y Recursos, Common Relevant Operational Picture (CROP), Herramientas Colaborativas, y Mensajería Oficial de Emergencias con firma digital. El portal dispone de un área de emergencia y de un área colaborativa de expertos.
RENEM cuenta con el soporte que le da el SIMGE (Sistema Integrado Militar de Gestión de Emergencias). Este sistema da soporte a la UME en las distintas fases operativas de la gestión de emergencias. Su arquitectura informática es tipo SOA.

Conclusiones de esta ponencia:

1.- La proliferación de tecnologías/sistemas en Defensa diversos genera problemas de coordinación que la propia tecnología es muy capaz de resolver.
2.-En el sector de la Defensa se han desarrollado tecnologías para la coordinación efectiva de operaciones.
3.- La RENEM proporciona un entorno cooperativo para la coordinación de los diferentes sistemas de emergencias.
4.- El SIMGE proporciona a la RENEM capacidades de procesamiento de información y predicciones.