

TECNIMAP 2010

ZARAGOZA- DEL 6 AL 9 DE ABRIL

XI Jornadas sobre Tecnologías de la Información para
la Modernización de las Administraciones Públicas

***RED NACIONAL DE EMERGENCIAS:
ENTORNO COLABORATIVO
DE
GESTIÓN DE CRISIS***

Ponente: Rodolfo Arroyo de la Rosa.

Organización: Unidad Militar de Emergencias – Ministerio de Defensa - España

TECNIMAP 2010

ZARAGOZA- DEL 6 AL 9 DE ABRIL

XI Jornadas sobre Tecnologías de la Información para
la Modernización de las Administraciones Públicas

INDICE

1. OBJETO.....	1
2. INTRODUCCIÓN.....	1
3. ANTECEDENTES	2
4. NECESIDAD OPERATIVA DE LA RENEM	2
5. GENERALIDADES.	3
5.1. CONCEPTO DE LA RENEM	3
5.2. MISIÓN DE LA RENEM.....	3
5.3. DESPLIEGUE	3
6. ARQUITECTURA PROPUESTA	3
6.1. NODOS CIS DE LA RENEM	3
6.2. VISTA DE SISTEMA	4
6.2.1. SOPORTE DE TELECOMUNICACIONES	4
6.2.2. SEGMENTO TERRESTRE	5
6.2.3. SEGMENTO SATÉLITE	5
6.3. SERVICIOS.....	5
6.4. MATRIZ DE SISTEMAS DE LOS POSIBLES USUARIOS	6
7. ANÁLISIS DE LA ARQUITECTURA PROPUESTA.....	8
8. PUNTOS DE FRICCIÓN PARA UNA POSIBLE IMPLANTACIÓN.....	10
8.1. FALTA DE UN REFERENTE INTERNACIONAL	10
8.2. ASPECTO ECONÓMICO	11
9. CONCLUSIONES	11
ANEXO A. GLOSARIO.....	¡Error! Marcador no definido.

TECNIMAP 2010

ZARAGOZA- DEL 6 AL 9 DE ABRIL

XI Jornadas sobre Tecnologías de la Información para
la Modernización de las Administraciones Públicas

LISTA DE FIGURAS

Figura 1.	Integración de Sistemas en la RENEM.....	3
Figura 2.	Capacidades de Telecomunicaciones de la RENEM.	4
Figura 3.	Redes de Telecomunicaciones de la RENEM.	5

LISTA DE TABLAS

Tabla 1.	Sistemas de Organismos del Estado.	7
Tabla 2.	Sistemas de Comunidades Autónomas.....	8
Tabla 3.	Sistemas de Corporaciones Privadas	8

1. OBJETO

El objeto de este documento es el **análisis** de la Arquitectura Propuesta para la constitución del Sistema que será en su día la Red Nacional de Emergencias (RENEM). Trataremos de analizar los **sistemas propuestos** y las **razones operativas** que los sustentan. Finalizaremos con un estudio de los **posibles candidatos** a formar parte como afiliados de la red y el papel que pueden jugar. Finalizaremos con una exposición de los **problemas para llevar a cabo su implantación**.

2. INTRODUCCIÓN

Las situaciones de crisis, catástrofes o emergencias, provocadas por fenómenos naturales, instalaciones o infraestructuras tecnológicas o del origen humano más pernicioso, han puesto de manifiesto la urgente necesidad de crear y fortalecer lazos para conseguir una coordinación eficaz entre los organismos gubernamentales, civiles y militares, y asociaciones humanitarias, corporativas o voluntarias, llamadas a participar en la **Gestión de Crisis**, operaciones de apoyo a la defensa civil y en todas las actividades de ayuda humanitaria en general.

En la Directiva de Defensa Nacional del año 2008 (DDN-2008) se reafirma en este sentido marcando ex profeso en el apartado PLANTEAMIENTOS ESTRATÉGICOS que en el ámbito nacional, las Fuerzas Armadas deben responder a una demanda cada vez mayor de la sociedad española de que las administraciones públicas respondan eficazmente ante situaciones graves de emergencia.

Las Fuerzas Armadas pueden contribuir a paliar en gran medida sus efectos, aportando capacidad de reacción rápida, disponibilidad y preparación para afrontar este tipo de situaciones. En este escenario, destacó la creación de la Unidad Militar de Emergencias (UME) en octubre de 2005 que viene a ampliarse con la DDN 2008 en la que la aportación de la Defensa a la Seguridad Nacional trata de promover la plena **integración de la Unidad Militar de Emergencias en el sistema nacional de Protección Civil**, sobre la base de la cooperación entre Administraciones Públicas en esta materia.

Para contribuir a preservar la seguridad y el bienestar de los ciudadanos y de sus bienes, cuando una catástrofe o calamidad los ponen gravemente en peligro, se exige una gestión eficaz de las situaciones de emergencia. En este sentido, se requieren Sistemas de Información y Telecomunicaciones (CIS) avanzados que faciliten una respuesta rápida, enérgica y eficaz, a los riesgos afrontados, que den servicio a redes y sistemas de vigilancia, alerta y gestión coordinada, y que solventen, entre otros problemas, la indisponibilidad de medios y la vulnerabilidad de infraestructuras y sistemas de telecomunicaciones en estos casos.

Las catástrofes producen consecuencias múltiples y simultáneas en los sistemas de información y telecomunicaciones, ya que se producen necesidades temporales adicionales en un momento en el que las redes y sistemas permanentes están menos disponibles y soportan una sobrecarga. En estas situaciones el suministro de servicios de telecomunicaciones e información a los **organismos responsables en la gestión de emergencias** debe estar garantizado y coordinado, para lo que se precisa obtener el máximo partido de los recursos disponibles creando al mismo **entornos colaborativos** entre los organismos implicados.

La aparición de la UME en escena exige al Ministerio de Defensa mirar al CIS desde un prisma hasta la fecha desconocido. La **necesidad de colaboraciones online y compartición de recursos con organismos civiles** que tiene la Unidad Militar de Emergencias, implica necesariamente una revisión.

Es en este contexto donde aparece la **Red Nacional de Emergencias (RENEM)**, como un conjunto de capacidades que faciliten una coordinación eficaz entre los elementos civiles y militares que participen en operaciones de gestión de crisis y de apoyo a autoridades civiles.

Por tanto se ha identificado la necesidad de crear una **red colaborativa de gestión de emergencias** que integre los Centros Operativos existentes en aquellos órganos responsables, para intercambiar información, para facilitar la toma de decisiones y lo que es más importante, para poder sincronizar acciones durante la gestión de los recursos empleados para aliviar a la población.

El Objetivo es fácil de imaginar: disponer de información en tiempo oportuno, contar con un foro de coordinación y de expertos, y no menos importante, facilitar la conducción de la emergencia.

3. ANTECEDENTES

La Ley Orgánica 2/1985 de Protección Civil, en su disposición final tercera, indica que el Gobierno creará la Red de Alarma Nacional, dependiente de los órganos de Protección Civil del Estado, que a estos efectos se coordinarán con los órganos correspondientes del Ministerio de Defensa.

La Ley 32/2003 General de Telecomunicaciones, en su artículo 4.2., indica que corresponderá al Ministerio de Ciencia y Tecnología (actual Ministerio de Ciencia e Innovación) ejecutar la política de Defensa Nacional en el sector de telecomunicaciones. A tal efecto coordinará con el MINISDEF a fin de asegurar la compatibilidad con los servicios civiles. Además en el artículo 4.3. señala que en el ámbito de Protección Civil el Ministerio de Ciencia y Tecnología cooperará con el MININT y con los órganos de las CCAA competentes. Por último, en esta ley en su artículo 4.4 advierte que los bienes afectos a la explotación de redes de los servicios de telecomunicaciones dispondrán de los medios y sistemas que se determinen a propuesta del MINISDEF, MININT y MINCyT.

La Ley Orgánica de la Defensa Nacional 5/2005, de 17 de noviembre, da un paso más convirtiendo esta "colaboración" en una misión más de las FAS, al establecer en su artículo 15.3 que "Las Fuerzas Armadas, junto con las Instituciones del Estado y las Administraciones Públicas, deben preservar la seguridad y bienestar de los ciudadanos en los supuestos de grave riesgo, catástrofe, calamidad u otras necesidades públicas, conforme a lo establecido en la legislación vigente".

El 7 de octubre de 2005, el Consejo de Ministros adopta el Acuerdo por el que se aprueba la creación de la Unidad Militar de Emergencias (UME). Establece que la misión principal de la UME es intervenir en cualquier lugar del territorio nacional para contribuir a la seguridad y bienestar de los ciudadanos, junto con el resto de las instituciones del Estado y las Administraciones Públicas.

4. NECESIDAD OPERATIVA DE LA RENEM

Es incuestionable que en la sociedad de la información y de las nuevas tecnologías la coordinación y control exige el **establecimiento de un sistema común** mediante el cual los organismos implicados puedan cumplimentar las misiones asignadas. El acceso a las redes y sistemas de alerta y emergencias existentes, tanto de la Administración General del Estado y Comunidades Autónomas, como de otros organismos responsables de la gestión de infraestructuras críticas, parece indicar el modelo más idóneo para lograr que tanto la Unidad Militar de Emergencias como el resto de participantes, dispongan de la información necesaria para la gestión de la emergencia en el momento de su intervención.

A tenor de lo expuesto en los párrafos precedentes parece obvia la necesidad de crear esa red que permitirá **interconectar a los organismos relacionados con la gestión de emergencias y proveedores de alertas**, con el propósito de intercambiar información con otros sistemas para obtener datos relevantes, o para recibir información sobre la gestión realizada sobre las emergencias en curso.

5. GENERALIDADES.

5.1. CONCEPTO DE LA RENEM

La **Red Nacional de Emergencias (RENEM)** será un Sistema de Sistemas de Información y Telecomunicaciones que integrará sistemas de información y telecomunicaciones pertenecientes a organizaciones nacionales de la Administración General del Estado (AGE), las Comunidades Autónomas (CCAA) y corporaciones privadas a cargo de infraestructuras críticas del Estado.

5.2. MISIÓN DE LA RENEM

La RENEM tendrá como misión **asegurar el intercambio de información relevante** para la gestión y coordinación de las emergencias en España.

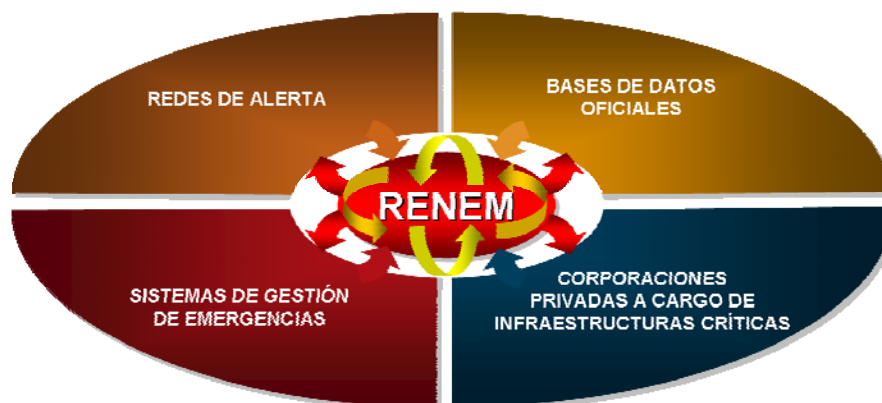


Figura 1. Integración de Sistemas en la RENEM.

5.3. DESPLIEGUE

La RENEM se desplegará a nivel nacional **ofreciendo** un conjunto de **servicios de información y telecomunicaciones** a los organismos **afiliados**. Dicho despliegue será el resultado de los convenios de interconexión/afiliación a la RENEM que los organismos realicen tanto con el MINISDEF como los que puedan realizar entre sí.

6. ARQUITECTURA PROPUESTA

6.1. NODOS CIS DE LA RENEM

Un Nodo CIS es el conjunto de capacidades CIS que proporcionan servicios de intercambio e integración de información, de sistemas de alerta y/o gestión de emergencias, para el enlace con otros nodos. Los Nodos más relevantes son los que se relaciona a continuación:

- **Nodos CIS de la UME (NCU)**. Nodos de UME en la RENEM.
- **Nodos CIS FAS (NCF)**. Resto de FAS que pueden apoyar en la emergencias.
- **Nodos de Redes de Vigilancia y Alerta (NRA)**. Este tipo de nodos se implantarán en los organismos de Alerta de la Administración Central del Estado,

los Centros 112 de las CCAA que generen alertas en el ámbito de su responsabilidad y en corporaciones privadas responsables de infraestructuras críticas del Estado.

- **Nodos CIS de Organismos de Gestión de Emergencias (NGE).** Este tipo de nodos se implantarán en aquellos organismos de la AGE, CCAA y corporaciones privadas que disponen de sistemas de Gestión de Emergencias que son susceptibles de compartir e intercambiar información.
- **Puestos de Mando Avanzados (PMA).** Centros de mando desplegados que se sitúan en lugares próximos a las zonas de emergencia.
- **Nodo Principal de Servicios (NCU-NP).** Ofrecerá los servicios RENEM de forma centralizada.
- **Otros Nodos:** No se detallan por no ser relevantes en este trabajo.

6.2. VISTA DE SISTEMA

El sistema interconectará a todos los integrantes mediante una “arquitectura en estrella” en cuyo nodo central se proporcionarían los servicios comunes y los nodos periféricos serán cada uno de los organismos y entidades que se integren en la RENEM. Es decir, la RENEM ofrecerá un “Bus de Servicios” al que accederían todos los usuarios del sistema con los privilegios correspondientes.

Todos los usuarios se conectarían al bus de servicios a través de los recursos de telecomunicaciones de la RENEM

6.2.1. SOPORTE DE TELECOMUNICACIONES

La diversidad de organismos con responsabilidad en la gestión de emergencias implica que los Nodos de la RENEM estarán geográficamente distribuidos por todo el territorio nacional teniendo alguno de ellos incluso capacidad de proyección internacional. Esto implica disponer de capacidades de telecomunicaciones con cobertura global.

Para dotar a la RENEM de alta disponibilidad y redundancia se basará en la combinación de redes de telecomunicaciones agrupadas en dos segmentos: Terrestre y Satélite.

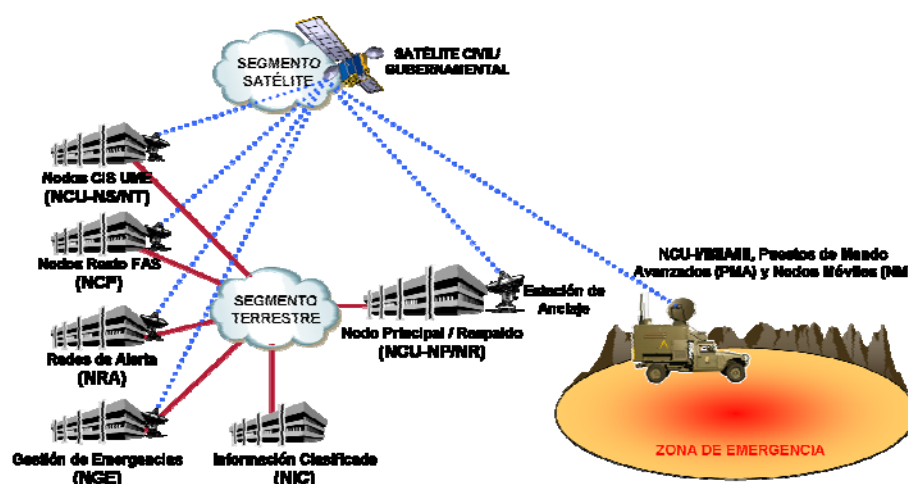


Figura 2. Capacidades de Telecomunicaciones de la RENEM.

6.2.2. SEGMENTO TERRESTRE

Las redes candidatas de telecomunicaciones que formarán este segmento son:

- **Red IRIS.** Es la red española para Interconexión de los Recursos Informáticos de las universidades y centros de investigación. Gestionada por la Entidad Pública Empresarial Red.es del Ministerio de Industria, Turismo y Comercio.
- **Red SARA** (Sistema de Aplicaciones y Redes para las Administraciones) pertenece al Ministerio de Administraciones Públicas (MAP).
- **WAN PG.** Red de Propósito General de MINISDEF.
- **Internet.** Accesos Remotos con protocolos seguros. (Solución limitada).

6.2.3. SEGMENTO SATÉLITE

Materializará las conexiones de los organismos a través de redes de telecomunicaciones vía satélite gubernamental/civil. La ventaja primordial es que puede garantizar el enlace de los elementos que participan en una emergencia, independientemente del lugar y del estado de las infraestructuras.

Las redes de telecomunicaciones vía satélite que formarán este segmento son:

- **SATÉLITE GUBERNAMENTAL.** Red Satélite con carga espacial gubernamental.
- **SATÉLITE CIVIL.** Red satélite civil de operadores públicos.
- **RETUME.** Parte de la Red Táctica de la UME.

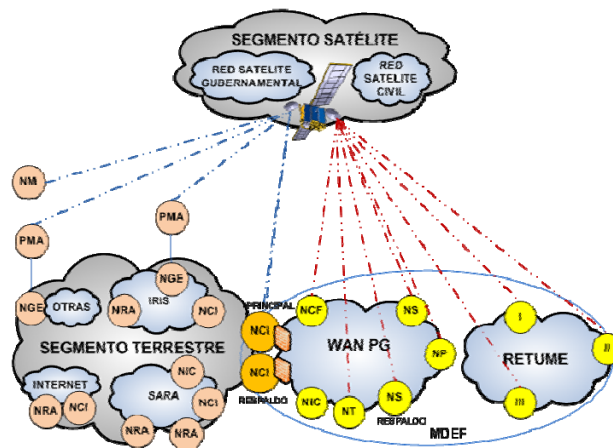


Figura 3. Redes de Telecomunicaciones de la RENEM.

6.3. SERVICIOS.

La RENEM proporcionará una serie de servicios, sobre la base de la conectividad proporcionada por las diferentes redes de comunicaciones que la forman, conformando una arquitectura global (grid) que interconectará un conjunto de capacidades de información end-to-end, con sus procesos y personal a demanda de los diferentes Organismos que lo necesiten. La interoperabilidad necesaria entre Organismos conectados a la RENEM debe basarse en el concepto de servicios. Hasta la fecha los servicios funcionales a implementar en la RENEM son los siguientes:

- Servicios Intercambio de Datos.
- Réplica de Bases de Datos.

- o Servicios de Coordinación de Operaciones.
- o Herramientas Colaborativas.
- o Servicios de Mensajería oficial de Emergencias (MOEMER).
- o Servicios de Telefonía y Videoconferencia de Emergencias.
- o Servicios Seguridad y Sellado de Tiempo.
- o Servicios de Acceso a Sistemas.

6.4. MATRIZ DE SISTEMAS DE LOS POSIBLES USUARIOS

La RENEM está destinada a ser una sola red de intercambio de información, con **diferentes niveles de seguridad**, para uso por parte de los diferentes organismos. Los Sistemas que inicialmente, se han identificados como susceptibles de interconectarse a la RENEM, ya sea mediante suministro o consumo de información alertas o relativa a la gestión de emergencias se indican en las siguientes tablas.

ÁMBITO ESTATAL		
ORGANISMO		SISTEMA
Ministerio de Defensa	UME	Sistema de Posicionamiento de Vehículos y Aeronaves.
	Ejército Tierra	IGSAN, SIGLE, DICODEF, SIPERDEF, SISANDEF, SICISFAS
	Ejército del Aire	SL2000, CESAEROB (SIGESTREDI)
	EMAD/MOPS	- Sistema de Información de JEMAD - Sistemas de Información de Mando y Control (SIM del SMCM): SICONDEF, SINTEFAS, SILOGFAS, etc. - Medios y Sistemas de apoyo de las FAS en emergencias.
	INTA	Servicios de Teledetección
	IGSAN	Red De Alerta Sanitaria
Ministerio de la Presidencia del Gobierno	DISSC	Sistema Nacional de Conducción de Crisis.
Ministerio del Interior	DGPCyE	RAR, SIGE, SIGAME.
	DGT	ARENA Incidencias de Tráfico. Cámaras de Tráfico.
	Policía Nacional	Sistema de información.
	Guardia Civil,	Sistema SIGO (Sistema Integrado de Gestión Operativa). Sistema SIVE (Sistema Integrado de Vigilancia del Estrecho).
	CNPIC	ERMES Base de datos que contiene el catálogo de Infraestructuras Críticas.
Ministerio de Medio Ambiente	DGA	Información sobre cuencas hidrográficas, Riesgos de inundaciones y nevadas. SAIH. Sistemas Automáticos De Información Hidrológica.
	INM	Meteoalerta.
	DGBD	RED INFO. Baco de datos de Biodiversidad. Mapa Forestal, Inventario Forestal Nacional, Incendios Forestales, Espacios Protegidos, Erosión de Suelos, Productividad Potencial Forestal, Vías Pecuarias, Red Natura, Modelos Combustibles.
Ministerio de Sanidad y Consumo	INSCIII	Redes de Alerta Sanitaria y Biológica.
Ministerio de Educación y Ciencia	IEO	Instituto Español de Oceanografía.
	IGME	Instituto Geográfico y Minero de España
Ministerio de Fomento	DGC	Dirección General de Carreteras.
	IGN	Información sísmica y volcánica.
	AENA	SIGRA Sistema de Información Geográfica de AENA. SACTA Sistema Automatizado de Control de Tráfico Aéreo.
Ministerio de Industria, Turismo y Comercio	INTECO	Centro de respuestas de incidentes de seguridad en Internet, CATA, RED.ES.
Consejo de Seguridad Nuclear	CSN	SALEM.

ÁMBITO ESTATAL	
ORGANISMO	SISTEMA

Tabla 1. Sistemas de Organismos del Estado.

ÁMBITO AUTONÓMICO		
	CONSEJERÍA / DEPARTAMENTO	SISTEMA
Andalucía	Consejería de Gobernación	Emergencias 112: SENECA.
	Dirección General de Gestión del Medio Natural Consejería de Medio Ambiente	Incendios forestales: INFOGIS.
Aragón	Departamento de Política Territorial, Justicia e Interior	112 SOS Aragón.
	Dirección General del Medio Natural Departamento de Medio Ambiente	Incendios Forestales
Asturias	Consejería de Presidencia, Justicia e Igualdad	SMARTCICU
	Bomberos del Principado de Asturias Consejería de Justicia, Seguridad Pública y Asuntos Exteriores	Incendios Forestales.
Canarias	Dirección General de Seguridad y Emergencias	112 Canarias, Incendios Forestales.
Cantabria	Consejería de Presidencia y Justicia (Dirección G. Protección Civil)	SENECA.
	Dirección General de Montes y Conservación de la Naturaleza Consejería de Ganadería, Agricultura y Pesca	Incendios Forestales.
Castilla La Mancha	112	112 Castilla La Mancha: SITREM.
	Dirección General del Medio Natural Consejería de Medio Ambiente y Desarrollo Rural	Incendios Forestales: FIDIAS.
Castilla León	Consejería de Interior y Justicia	112.
	Dirección General del Medio Natural Consejería de Medio Ambiente	Incendios Forestales.
Cataluña	Departamento de Interior, Relaciones Institucionales y Participación	112.
	Dirección General de Prevención, Extinción de Incendios y Salvamento Departamento de Interior, Relaciones Institucionales y Participación	Incendios Forestales.
Ceuta	Centro Proceso de Datos	112
	Viceconsejería de Calidad Ambiental	Incendios Forestales.
Extremadura	Consejería de Presidencia	112 Extremadura: SITREM.
	Dirección General de Desarrollo e Infraestructuras Rurales Consejería de Desarrollo Rural	Incendios Forestales: INFOGIS.
Galicia	Consellería de Presidencia, Administraciones Públicas e Xustiza	112 Galicia: XEOCODE.
	Dirección General de Montes e Industrias Forestales Consejería del Medio Rural	Incendios Forestales: X-LUMES.
Islas Baleares	Consejería de Interior (Dirección General de Emergencias)	112 Baleares.
	Dirección General de Biodiversidad	Incendios Forestales.

ÁMBITO ESTATAL		
ORGANISMO	SISTEMA	
	Consejería de Medio Ambiente	
La Rioja	Consejería de Administraciones Públicas y Política Local	112 La Rioja.
	Dirección General del Medio Natural Consejería de Turismo, Medio Ambiente y Política Territorial	Incendios Forestales.
Madrid	Consejería de Sanidad y Consumo	112 Madrid.
	Consejería de Medio Ambiente y Ordenación del Territorio (Dirección General del Medio Natural)	Incendios Forestales.
Melilla	112	
	Viceconsejería de Medio Ambiente	Incendios Forestales.
Murcia	Dirección General de Protección Civil	112 Murcia: COORDCOM.
	Dirección General de Medio Natural Consejería de Industria y Medio Ambiente	Incendios Forestales.
Navarra	Dirección General de Interior	112.
	Dirección General del Medio Ambiente Departamento de Medio Ambiente, Ordenación del Territorio y Vivienda	Incendios Forestales.
País Vasco	Departamento de Interior	112.
	Dirección de Medio Ambiente Departamento de Urbanismo y Medio Ambiente Diputación Foral de Alava	Incendios Forestales
Valencia	Consejería de Gobernación	112: COORDCOM
	Dirección General de Gestión del Medio Natural Consellería de Medio Ambiente	Incendios Forestales

Tabla 2. Sistemas de Comunidades Autónomas.

ÁMBITO PRIVADO	
CORPORACION PRIVADA	SISTEMA
Compañía Logística de Hidrocarburos (CLH)	Sistema de control de la red de transporte de hidrocarburos.
Res Eléctrica Española (REE)	SIOS. Sistema de Información de Operación del Sistema
Red Nacional de Ferrocarriles Españoles	COPERNICO.
Empresa nacional del Gas (ENAGAS)	SIGE Sistema de Información y Gestión Energética.

Tabla 3. Sistemas de Corporaciones Privadas

7. ANÁLISIS DE LA ARQUITECTURA PROPUESTA

Comencemos por estudiar la vista de sistema en la cual se hace referencia a una **arquitectura en estrella**. Hoy día ningún ingeniero de sistemas utilizaría una estrella como base del diseño de una red de alta disponibilidad. Es evidente que el HUB sobre el que se conectan los organismos que configuran la estrella es precisamente el elemento más sensible.

Las razones esgrimidas son dos. La primera apunta a que el bus de servicios se debe situar en una "zona segura". Esta zona no es otra que la red del Ministerio de Defensa

denominada WAN de Propósito General en la que se ubicarán los servidores de servicios.

La segunda razón señalada es que al ser la UME la impulsora de la RENEM, "de momento" debe ser su personal la que desde sus instalaciones gestione el sistema.

La RENEM debería satisfacer las necesidades de telecomunicaciones derivadas de la interconexión e interoperabilidad de los sistemas de alerta y gestión de emergencias de diferentes organismos, tanto de forma permanente con los centros destinados a tal efecto como extraordinaria con unidades desplegadas en casos de emergencia. Esto significa que **debe operar en todo tiempo**, 24 horas al día, 365 días al año.

Es evidente por ello que por esta razón se decide duplicar en **segmentos terrestres y satélite**, para garantizar por un lado la supervivencia en caso de fallo múltiple, pero por otro lado se pretende igualmente garantizar el enlace en aquellos puntos que no tengan accesos a infraestructura terrena. Por tanto se puede decir que el **planteamiento** es bastante **lógico**.

Los "peros" los podríamos plantear en las redes candidatas a formar parte de uno y otro segmento.

En el **segmento terrestre** por el que se opta son principalmente las dos redes pertenecientes a la AGE, SARA y RedIRIS. Ambas son redes que ofrecen a su favor una capacidad tecnológica enorme, Centros de Alerta Temprana y Personal de servicio.

El disponer de estas redes obliga a los organismos interesados en la afiliación a realizar importantes inversiones para extender desde los asentamientos más próximos de SARA o RedIRIS hasta sus instalaciones.

¿Se plantea entonces una solución alternativa? Un rápido análisis apunta a la adquisición o **alquiler de circuitos punto a punto** a teleoperadores de sistemas de telecomunicaciones para realizar la arquitectura en estrella mencionada con anterioridad. Sin duda esta alternativa sería mucho más rápida de implementar y más flexible, teniendo en su contra el coste implícito que debería ser asumido por el organismo o entidad candidato a formar parte de la RENEM.

El **segmento satélite** es sin duda la característica que marca la diferencia. No tanto el civil, que hoy día es accesible por cantidades aceptables de dinero, sino el llamado satélite con carga gubernamental (SpainSat y X-Start).

La capacidad de poder dotar con terminales satélite terrestres en Banda X, gestionado por la AGE, es sin duda de un gran valor añadido con respecto a las entidades que se entregan empresas comercializadoras que ofrecen este tipo de servicios civiles.

Además por otro lado la AGE realizó una inversión enorme a través del consorcio HISDESAT que ofrece la posibilidad a organismos ajenos a la propia AGE de contar con parte de la **carga gubernamental** que es estos momentos no se encuentra utilizada. Es decir esta inclusión en la arquitectura se considera fundamental ya que es el verdadero respaldo a las redes terrenas y la que garantiza el futuro funcionamiento de la RENEM, de un modo independiente de l estado de la infraestructura terrena y con una flexibilidad desconocida hasta la fecha en las redes de emergencia que permite desplegar en el mismo lugar de la catástrofe.

No obstante el no excluir los accesos mediante terminales **satélite comerciales civiles** facilita la integración de organismos que ya cuentan con estos medios y da redundancia y robustez a este segmento.

La RENEM debe facilitar la coordinación eficaz entre los elementos civiles y militares que participen en operaciones de gestión de crisis y de apoyo a autoridades civiles. La integración de la información de los sistemas de alertas y gestión de emergencias para

proporcionar los datos necesarios para ofrecer una **visión global** y compartida sobre riesgos y situaciones de emergencia a los diferentes organismos afiliados se pretende hacerla mediante un **bus de servicios** fundamentalmente basado en WEB. Esto sin duda se debe estimar como un acierto. El **"Share Information"** tan de moda al otro lado del Atlántico tras los ataques del 11 de Septiembre es vital. El recurrir a entornos Web tiene muchas ventajas.

Herramientas Colaborativas que permitan intercambio de datos y recepción e intercambio de alertas, y un servicio de Mensajería Oficial de Emergencias deberían ser las prioridades.

Mención específica merece el tema de los **diferentes niveles de seguridad** relacionados con la red de intercambio de información. En la RENEM se pretende integrar a una **gran cantidad de sistemas** de Ministerios, Comunidades Autónomas y organismos responsables de infraestructuras críticas muy diferentes entre sí. Además la RENEM nace con vocación de aglutinar bases de datos de diverso tipo, que normalmente son de carácter reservado.

El condicionante de seguridad no es cuestión baladí, pues si un sistema se debe acreditar para tratamiento de determinada información sensible, eso implica un concienzudo diseño y control de los elementos que pueden tener acceso a él. Esto es fácil de decir pero tremendamente difícil de cumplimentar.

En cuanto a la relación de organismos y sistemas a integrar en la RENEM, se concluye que es sin duda ambiciosa. ¿Irrealizable? Esperemos que no. Es por ello que uno de los principales requisitos es la **interoperabilidad**. La RENEM garantizará la interoperabilidad de los sistemas CIS de los organismos que formen parte de ésta. Pero para que esto sea real deberá ofrecer diferentes grados de interoperabilidad en función de las necesidades.

8. PUNTOS DE FRICCIÓN PARA UNA POSIBLE IMPLANTACIÓN

Hasta este apartado nos hemos limitado a exponer parte de las soluciones dadas al problema de la implantación y al análisis de las mismas. A continuación trataremos de hacer un breve recorrido por los impedimentos o trabas más reseñables con los que nos podremos encontrar.

8.1. FALTA DE UN REFERENTE INTERNACIONAL

Como ya se ha señalado anteriormente, **no existe** ninguna referencia ni en Europa ni en Estado Unidos **que reúna todas las capacidades que se han expuesto**.

Esto sin duda es un handicap ya que no se tiene referencia alguna que esgrimir para reivindicar la existencia de este tipo de red en España, pero por otro lado tiene la gran ventaja de que al partir de cero se puede ser todo lo ambicioso que se quiera para dotarnos de una gran herramienta a nivel Gobierno Central para contribuir a la gestión de crisis provocadas por emergencias de cualquier índole.

Los referentes más próximos se pueden buscar en **Francia y EEUU**. En el caso del país galo su organización centralista le permite una gestión de las situaciones de crisis y emergencias mucho más simple que el que pueda adoptar un país descentralizado como es nuestro caso o el de EEUU. En el 2008 entró en funcionamiento la llamada **Red ISIS (Intranet Sécurisé Interministériel pour la Synergie gouvernementale)**. Esta red es similar a nuestra Red SARA del Ministerio de Administraciones Públicas, pero centrada en las situaciones de crisis. Además no contempla elementos desplegados.

En **Estados Unidos** el 11 de septiembre de 2001 marca un punto de inflexión en la concepción de la seguridad interior en EEUU. En 2002 se nombra al **USNORTHCOM**

(Mando Norte) como Mando de Combate contra ataques aéreos, terrestres, navales, espaciales y cibernéticos en el territorio nacional continental. El mayor reto al que se enfrenta este Mando es el de realizar un enfoque integral para que todos los participantes concierten sus estrategias y acciones desde el primer momento. Esto implica adquirir la capacidad de “**compartir información**”.

El Mando Norte tiene acceso al sistema CIS del DoD. No ocurre lo mismo con el resto de agencias civiles y tampoco se dispone de medios estatales o federales para desplegar y permitir el C4 en el lugar donde ocurra un incidente.

Por otro lado la **Guardia Nacional** se encuentra desplegada en todos los estados y tiene asignadas tanto misiones estatales como federales, dependiendo directamente o por delegación del Presidente de los EEUU del Gobernador del Estado. Ésta fuerza es la primera encargada de auxiliar a los estados y posee capacidades CIS desplegables.

En ese momento se considera imprescindible contar con información de primera mano proveniente del lugar donde se ha producido la emergencia para conformar una COP sobre la que sustentar el C4 de todos los organismos. Detectada esta carencia el Jefe de la Guardia Nacional propone crear un área de intercambio de información basada en un sistema de comunicaciones en todo el territorio continental sobre el que sustentar el C4. Este sistema se pasa a denominar **JCCSE (Joint Connus Communications Support Environment Concept for Joint C4)**. Es decir el JCCSE pasa a ser la aportación del DoD al NRF.

El **Concepto JCCSE**, es lo que de modo aproximado más se asemeja con el concepto español de **Red Nacional de Emergencias**, aunque con marcadas diferencias en el alcance, participante, objetivos y tipo de redes utilizadas. Primero porque en ambas hay un componente militar (Guardia Nacional en EE.UU. y UME en España), segundo porque ambas usan redes militares para alcanzar a cubrir todo el territorio nacional, y sobre todo porque ambas soluciones contemplan un componente CIS desplegable en base a los medios militares.

8.2. ASPECTO ECONÓMICO

La red se podría haber diseñado a base de fibra óptica oscura (de la mucha existente e infrautilizada) instalada en España. Con el fin de evitar los precios de alquiler o compra de este servicio que además tuviera cobertura nacional, se ha optado por tratar de utilizar redes pertenecientes a la administración general del estado. Red SARA, Red IRIS o las redes del MINISDEF son redes ya existentes con capacidad suficiente para soportar los servicios.

El aspecto del personal para operar y sustentar esa red queda sobradamente cubierto por el personal TIC del MINISDEF, con lo cual el gasto en este aspecto ya está pagándose.

En resumen que la única componente que llevaría un gasto sería el “enganche” del organismo en cuestión a una de las redes ofertadas.

9. CONCLUSIONES

Se ha identificado la necesidad de crear una red de gestión de emergencia a nivel nacional que integre los centros operativos para intercambiar información y facilitar la toma de decisiones durante la gestión de catástrofes

Una red que debe asegurar su funcionamiento en condiciones “todo tiempo” debe asegurar su operatividad con soluciones backup en términos de soporte de telecomunicaciones, nodos de respaldo y condiciones de seguridad garantizada dado el tipo de datos que podrá correr en su interior.

Se ha señalado que no es fiable una arquitectura en estrella tal y como se encuentra definida en estos momentos, por la debilidad que representa un único punto desde el que se proveen los servicios a los organismos afiliados. La solución pasaría por duplicar este HUB que será el Nodo proveedor de servicios con un Nodo CIS adicional o centro de respaldo del primero.

El proyecto se ha mostrado viable y ejecutable siempre cuando esté basado en la colaboración entre todos los posibles organismos y administraciones participantes. Sin duda que contar con el respaldo de dos grandes redes como SARA y RedIRIS ya de por sí indica el alto grado de colaboración de distintas partes.

El segmento satélite basado en terminales gubernamentales es vital para lograr la flexibilidad y robustez del sistema.

Es un buen negocio, porque todos los que accedan a afiliarse ganarán. Pero además el buscar realizarlo a través de WEB, es sin duda un hecho que facilitará el lanzamiento y la implementación. De entrada son estándares abiertos que no exigen instalaciones de ningún software específico para acceder a la RENEM y que por tanto facilitará el mantenimiento de la propia red y lo que es si cabe más importante: el usuario conoce el negocio y el rechazo a nuevas innovaciones y uso de software desconocido debe ser mínimo.

El resultado de la red dependerá del grado de participación y coordinación entre todos los organismos responsables de las alertas y gestión de emergencias. Esto debe materializarse en una realidad útil y tangible. Es decir los servicios que se ofrezcan deben estar limitados en las pretensiones iniciales para evitar retardos innecesarios. Dar un foro de intercambio de información seguro y una mensajería común para los organismos implicados en el mundo de las emergencias es básico para poder posteriormente ir subiendo en el nivel de ambición.

Hemos señalado la dificultad que supone crear diferentes dominios de seguridad en una misma red integrada por organismos tan dispares. Quizás se debiera optar por un único nivel y sacar fuera de esta red toda la información que sobrepase el nivel de seguridad admisible de acuerdo a las medidas implementadas.

La interoperabilidad con la ingente cantidad de sistemas identificados no está ni mucho menos garantizada. Por lo tanto se estima que se deberían marcar diferentes niveles que no obliguen a los organismos a realizar fuertes inversiones en desarrollo de aplicaciones que permitan un intercambio fluido de información entre sistemas. El protocolo TSO (estándar XML de la UE para emergencias) es sin duda una buena base para lanzar el intercambio de información a diferentes grados de interoperabilidad.

La RENEM es consecuencia de la necesidad de ejercer la dirección y coordinación operativa de las emergencias declaradas de interés nacional. Esta función, de la mayor exigencia, debe considerarse como el cometido distintivo y esencial para el que la Unidad Militar de Emergencias fue creada.

La falta de referentes internacionales es un handicap que debe ser reconducido y transformarlo en ventaja ya que no impone ninguna restricción.

El condicionante económico no debe ser un impedimento al menos para echar a andar. Si se limitan los servicios iniciales, los gastos son perfectamente asumibles por los participantes.

Los objetivos de la RENEM no se deben identificar con objetivos de la UME. Se trata de objetivos globales que pueden y deben repercutir en el bienestar de los españoles. No viene a sustituir a nada ni a nadie...La RENEM viene a sumar.

La RENEM es un proyecto ambicioso pero alcanzable, que de finalizarse con éxito se convertiría en una referencia internacional en la gestión de emergencias.

