Rodolfo Arroyo de la Rosa

FUERTE Y CLARO

El enlace en las emergencias

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DIRECCIÓN GENERAL DE PROTECCIÓN CIVIL Y EMERGENCIAS

FUERTE Y CLARO

El enlace en las emergencias

Rodolfo Arroyo de la Rosa

Catálogo de Publicaciones de la Administración General del Estado
http://publicacionesoficiales.boe.es

EDITA:
Secretaría General Técnica. Ministerio del Interior

Autor: Rodolfo Arroyo De la Rosa
Acuarelas: Carlos Torres Cabrera
Ilustraciones: Manuel Pizarro Artola y Juan Martínez Rivas
NIPO (papel): 126-14-012-3
NIPO (en línea): 126-14-011-8
Depósito Legal: M 7975-2014
Impreso en España / Printed in Spain
Diseño, maquetación e impresión: Tórculo Comunicación Gráfica, S. A.


EL ENLACE EN LAS EMERGENCIAS
FUERTE Y CLARO

A mis hijas
Sofía, Clara y Eva,
por todo lo que me dan.

ÍNDICE

PROEMIO

JUAN ANTONIO DÍAZ CRUZ

Director General
de Protección Civil y Emergencias
Ministerio del Interior

La gestión de las emergencias consiste, en general, en una evaluación de la situación, previsión de su evolución, establecimiento de objetivos estratégicos a alcanzar, elección de tácticas adecuadas para conseguirlos, organización de los recursos disponibles y control continuo de la intervención para readaptar el plan cuando sea necesario

En todas las emergencias que he tenido ocasión de seguir como Director General de Protección Civil, he podido constatar que una de las prioridades a resolver, para llegar a compatibilizar los recursos disponibles en cada momento y minimizar los fatales resultados de aquellas, es la de procurar un eficaz enlace, entre todos los agentes implicados en dar respuesta a las mismas. Este enlace debe asegurarse desde el inicio de la emergencia y deberá llevarse a cabo durante el tiempo en que continúe activa y hasta que finalice.

Podemos afirmar por ello, sin temor a equivocarnos, que para que se produzca una adecuada gestión de cualquier emergencia, será necesario que el enlace funcione de forma correcta, coordinada y continua. Valiéndose para ello, de los medios disponibles en cada momento y solventando de forma ágil, y rápida, las causas de indisponibilidad que las estructuras de telecomunicaciones, a raíz de la propia situación, puedan llegar a producirse.

El libro que tienen ahora entre sus manos, precisamente trata, como su título hace expresa mención, a "El enlace en las emergencias", que como define su autor, es "El conjunto de acciones, procedimientos y medios que debemos poner en práctica para establecer el canal de comunicación entre usuarios, con el fin de que puedan tratar y transmitir la información necesaria para asegurar la coordinación, fundamentar las decisiones y llevarlas a cabo durante todas las fases de dicha emergencia".

El presente libro, escrito por el Comandante de Transmisiones, Diplomado de Estado Mayor, Rodolfo Arroyo de la Rosa, excelente profesional con amplia experiencia en el campo de las telecomunicaciones de las Fuerzas Armadas y en el de la gestión de emergencias, tanto por su contenido como por su redacción, amena pero no carente de rigor metodológico, puede constituir un excelente apoyo para la formación de los componentes de los equipos de intervención en emergencias.

Por el amplio espectro de los temas abordados, será también una estimable ayuda como texto de consulta para aquellas personas, que ostentando algún tipo de responsabilidad en la gestión de emergencias, dentro del ámbito de la Protección Civil, ya sea a nivel local, autonómico ó Estatal, desee ilustrarse sobre las comunicaciones en emergencias. Así como también, a cualquier persona interesada en la Protección Civil, que como todos sabemos, es cosa de todos.

No quiero terminar sin agradecer al Comandante Arroyo de la Rosa su contribución al Sistema Nacional de Protección Civil.

Madrid, 7 de abril de 2014

PRÓLOGO

JOSÉ LUIS GOBERNA CARIDE[1]

General de Brigada del CG ET (Transmisiones) DEM

Este libro, que me cabe el honor de prologar, es el resumen de un esfuerzo colectivo, vivo y dinámico, de un grupo de profesionales de las Fuerzas Armadas que supo comprender el problema del apoyo e integración de la Unidad Militar de Emergencias en la estructura de la Protección Civil en España, y darle la mejor de las soluciones posibles.

La obra del Comandante Arroyo de la Rosa, miembro ilustre de aquel equipo, que concibió, ensayó y puso en servicio con grandes dotes de entusiasmo, imaginación y acreditada experiencia todos los CIS/TIC de la UME, es sencilla y de fácil lectura, porque se pone en el lugar del lector, porque es amena y porque trata de cautivarle desde el primer párrafo; y doy fe de que lo consigue. Sin embargo, ese estilo llano, sencillo y comprensible no es óbice para tratar todos los temas con rigor y profundidad, y por ello la convierte en un referente en esta materia del que pronto veremos su huella en foros, conferencias, congresos y allá donde se trate de la gestión de emergencias.

No es sólo un libro sobre los sistemas de información y telecomunicaciones en emergencias, es mucho más, porque aborda el problema del enlace, de la información, de su tratamiento, de los equipos terminales más modernos, de los diversos sistemas de información básicos y específicos, de cómo hay que organizar un puesto de mando y cómo se ha afrontado el reto del mando y control en otros países y situaciones diferentes.

Es un libro de un Ingeniero Militar y de un profesional de los CIS/TIC de las Fuerzas Armadas, que conoce como nadie las emergencias en España. Al mismo tiempo, es un actualizado referente tecnológico y didáctico, diría que incluso muy pedagógico, un libro que pronto veremos en los centros de enseñanza porque viene a cubrir una laguna que clamaba por ser cubierta desde hace años a nivel nacional.

Solo me queda dar las gracias al Comandante D. Rodolfo Arroyo de la Rosa, que hago extensible a su familia, por este excelente trabajo, de tanto provecho para el sector de las emergencias en España, felicitarle por una obra tan completa y trabajada, y desearle todos los éxitos profesionales y personales que se merece su entrega al Ejército, a la UME y a España.

Torrejón de Ardoz,
7 de octubre de 2013

Día de la Virgen del Rosario,
Patrona de la Unidad Militar
de Emergencias en la celebración
del VIII Aniversario de su creación.

1. El General Goberna fue la persona encargada en el Ministerio de Defensa de diseñar el Sistema de Telecomunicaciones e Información de la Unidad Militar de Emergencias (UME) como base del Sistema de Mando y Control que debiera sustentar la Dirección Operativa de una Emergencia declarada de Interés Nacional en España. Para ello contó con el apoyo inestimable de los Ingenieros David Fernández Bermejo y Javier Bermejo Higuera, ambos ligados al Ministerio de Defensa, y para siempre a la Unidad Militar de Emergencias.

DEL AUTOR

Rodolfo Arroyo de la Rosa es Comandante del Arma de Ingenieros (Transmisiones) del Ejército de Tierra.

Es Diplomado de Estado Mayor y posee el Título de Ingeniero en Informática de Sistemas por la UNED.

Posee un Máster en Paz, Seguridad y Defensa por el Instituto Universitario Gutiérrez Mellado y realizó el VIII Máster Ejecutivo en Dirección de Sistemas de Emergencias por la Universidad Camilo José Cela. En la actualidad presta sus servicios en la Unidad Militar de Emergencias donde fue destinado en el año 2008 a la Sección de Sistemas de Información y Telecomunicaciones del Estado Mayor de la UME.

Además es Técnico Superior en Prevención de Riesgos Laborales especialidad Ergonomía y Psicología Aplicada, Técnico Superior en Prevención de Riesgos Laborales especialidad Seguridad en el Trabajo y Técnico Superior en Prevención de Riesgos Laborales especialidad Higiene Industrial.

Ha estado destinado en la Brigada Paracaidista, en la Unidad de Transmisiones de la Fuerza de Acción Rápida, y en la Brigada Multinacional de Apoyo al Mando del Eurocuerpo en Estrasburgo (Francia), donde estuvo al mando de la Compañía de Sistemas Información de la OTAN. En 2004 vuelve a España siendo destinado por el Diploma de Transmisiones a la Academia de Ingenieros del Ejército, donde ejerció de profesor de Redes Radio y de Sistemas de Información. En julio de 2006 asciende a Comandante y es destinado a la Sección de Ingeniería de la Jefatura de Telecomunicaciones y de los Sistemas de Información del Ejército de Tierra.

Está en posesión de diferentes condecoraciones militares, ha realizado varias misiones internacionales y tiene diversos cursos civiles y militares, nacionales y de OTAN, relacionados con las TIC y la Protección Civil entre los que destacan:

- Curso de Transmisiones para Oficiales del Ejército de Tierra.
- Curso de Seguridad de las Tecnologías de la Información.
- Curso de Guerra Electrónica en la Escuela de Transmisiones de Alemania.
- Curso "Sécurité Informatique pour Informaticiens" en la Dirección Central de la Seguridad de los Sistemas de Información de la Secretaria General de la Defensa Nacional Francesa. París-Francia.
- CIS ORIENTATION COURSE en Latina –Italia.
- Curso INFOSEC de la OTAN en Latina –Italia.
- Curso COMPUSEC de la OTAN en Latina –Italia.
- Curso de Técnicas de Planificación de Protección Civil (Planes Territoriales y Planes Especiales-Nivel III). Escuela Nacional de Protección Civil-Ministerio del Interior.
- Curso de Sistemas de Información y Telecomunicaciones en Emergencias (Nivel III). Escuela Nacional de Protección Civil-Ministerio del Interior.
- Cursos de Experto del Mecanismo de Protección Civil de la Unión Europea.
    - ¤ The Community Mechanism Introduction Course (CMI).
    - ¤ The Operational Management Course (OPM).
    - ¤ The Security and Media Course (SEMC).
    - ¤ The International Coordination Course (ICC).
    - ¤ Operational Management Refresher Course (OPM-R).

Es profesor eventual en la Escuela Nacional de Protección Civil y ha sido profesor de diferentes Máster impartidos por la Universidad Europea de Madrid, la Politécnica y por la Camilo José Cela. Es autor de varios artículos publicados en revistas especializadas de Telecomunicaciones y ha presentado múltiples conferencias en diversos foros civiles y militares, dentro y fuera de España.

PREFACIO:
¿POR QUÉ ESTE LIBRO ESTÁ DIRIGIDO A USTED?

La expresión ***Telecomunicaciones en Emergencias***, en según qué contexto, es tan amplia como inexacta. Es habitual encontrarla utilizada para hablar de cualquier tipo de sistema que se utiliza para la transmisión o gestión de información en el período de tiempo en el que se desarrolla una emergencia. Es decir, desde el mismo momento en el que las autoridades competentes detectan un riesgo o amenaza potencial para la sociedad, pasando por los periodos inmediatamente seguidos al incidente, llegando incluso a abarcar los momentos de rehabilitación y vuelta a la calma que se pueden extender por semanas, sino meses.

Es constante y reiterada la mezcla de conceptos, sin diferenciar entre las acciones de transporte de la información (realizada por las telecomunicaciones) y el procesamiento de la misma (llevada a cabo por los sistemas de información).

Son muchos los documentos escritos, blogs o foros que utilizan esta expresión **Telecomunicaciones o Comunicaciones en Emergencias** para hablar de temas totalmente dispares. Lo mismo la podemos encontrar para nombrar un capítulo de un libro en el que se instruye a hablar por radio a un futuro conductor de ambulancias; que para denominar grupos de trabajo en los que prestigiosas organizaciones relacionadas con las Tecnologías de la Información y Telecomunicaciones (TIC) sientan a expertos a hablar de los aspectos más relevantes de este tipo de comunicaciones.

Especial precaución nos producen los portales web que de manera reiterada e inconexa se dedican a "colgar" innumerables temas de debate o artículos "de supuesto interés" sin ningún tipo de orden ni concierto. Los visitantes de dichas páginas deben bucear durante demasiado tiempo para encontrar un mínimo de provecho. Sin dejar de reconocer la buena intención del propietario del sitio web, en estos portales todo vale. Desde un manual de una simple radio analógica hasta la versión más completa de los tipos de modulación digital implementados en los más recientes sistemas.

Este desconcierto viene provocado por la relevancia adquirida por las TIC en el día a día. Hasta el menos amante de las nuevas tecnologías acaba utilizándolas u opinando al respecto. Sin embargo también podemos achacar esta confusión relativa al **mundo TIC en las emergencias** a otras razones que en este texto trataremos de exponer.

Lo cierto es que hasta ahora **no existía una publicación** que tratara de una manera completa este asunto. Aunque existen multitud de cursos, incluso de post-grado, que incluyen las TIC entre sus asignaturas, no hay normalmente un libro en el que basarse, limitándose a apuntes o fotocopias de "asuntos variados" que no permiten abordar el asunto de una manera seria y global.

Por ejemplo. Normalmente detectamos un importante **desconocimiento de las características**

inherentes a este tipo de telecomunicaciones por parte de los usuarios potenciales, que en buena medida van a condicionar su funcionamiento. Tampoco se suele relacionar el uso de determinado medio o sistema con el periodo de tiempo o **fase en la que se encuentra la emergencia.**

Un aspecto determinante es la documentación utilizada. Los libros que tratan las TIC tienden a **sobresaturar al lector** dándole una infinidad de definiciones y datos técnicos, muchos de los cuales a la postre serán irrelevantes. Muy relacionado con este aspecto destaca el **exceso de detalles tecnológicos** que aparecen en los textos, en detrimento de la exposición de las capacidades de los medios o sistemas.

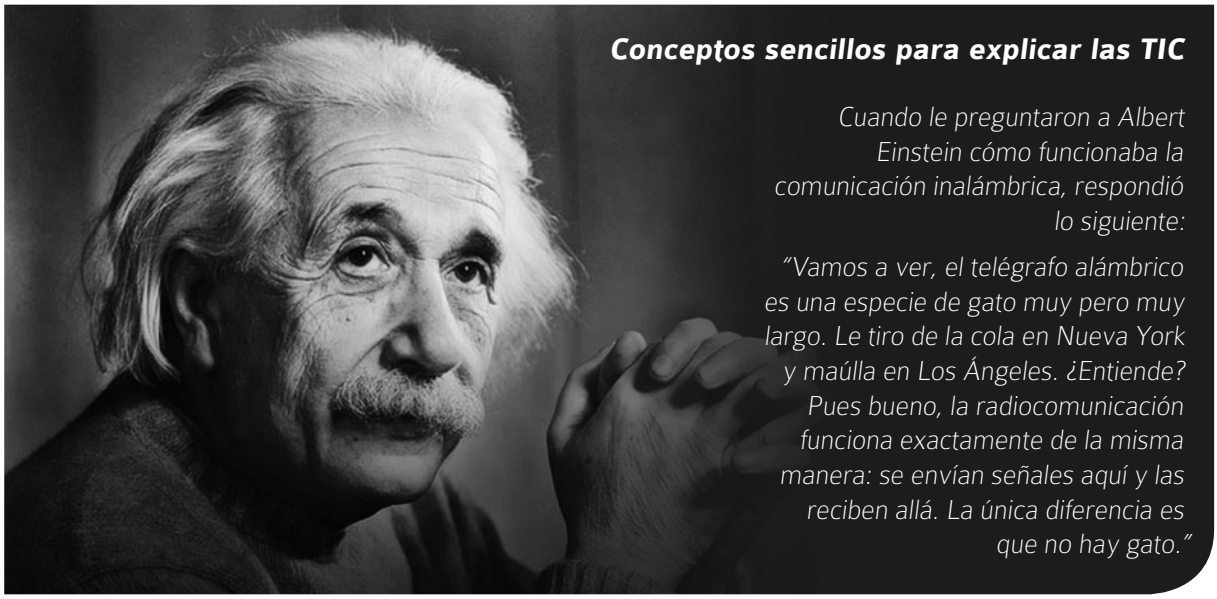
Otro aspecto relevante es la **no definición de la "audiencia objetivo"** a quien va dirigido el documento. Continuamente se elaboran manuales cuyos posibles destinatarios abarcan una amplia panoplia de puestos de trabajo; desde políticos, pasando por directores técnicos de emergencias, ingenieros de telecomunicaciones u operadores básicos de medios de transmisiones.

Por último, no debemos dejar la oportunidad de reconocer el mayor error de los que nos dedicamos al mundo de las telecomunicaciones: el uso de un **"lenguaje oscuro y encriptado".** Unos por incultura manifiesta, al no saber cambiar de registro idiomático y adaptarlo al del lector con menos conocimientos técnicos; y otros por arrogancia, intentando mostrar lo mucho que dominan la tecnología, lo cierto es que los que nos dedicamos a este "negocio" **nos empeñamos en hablar para que no nos entiendan**.

Por todo lo anteriormente expuesto, **este libro está dirigido** a aquellas personas que quieren tener una primera aproximación sencilla, no tecnológica y simplista a este mundo del enlace en las emergencias.

Puede que el término "enlace" sea un término desconocido y poco empleado para aquellas personas con relación previa con las TIC. Sin embargo nos inclinaremos por usar este término porque en el texto que ahora comienzan a leer hablaremos de los sistemas de telecomunicaciones y de información, pero también otros medios de enlace como los mensajeros o las señales acústicas; el diseño de las redes y sistemas o las funciones de mando y dirección de una emergencia. La pretensión es hacerlo de una manera llana, simple y comprensible, sin tratar de demostrar lo mucho o poco que sabemos; cediendo el protagonismo al lector que esté interesado en encontrar un mínimo de utilidad entre sus páginas.

El contenido del libro expone algunos temas que son completamente innovadores en este campo de las emergencias y recordaremos otros tantos que quizás el lector ya conozca, pero que interesa abordarlos desde una nueva perspectiva más sencilla, orientada a dar respuesta a los retos a los que se enfrentan los sistemas de enlace utilizados por los servicios de emergencia.



Conceptos sencillos para explicar las TIC

Cuando le preguntaron a Albert Einstein cómo funcionaba la comunicación inalámbrica, respondió lo siguiente:

"Vamos a ver, el telégrafo alámbrico es una especie de gato muy pero muy largo. Le tiro de la cola en Nueva York y maúlla en Los Ángeles. ¿Entiende? Pues bueno, la radiocomunicación funciona exactamente de la misma manera: se envían señales aquí y las reciben allá. La única diferencia es que no hay gato."

Los temas que abarcaremos son:

- Los mayores condicionantes del enlace, teniendo en cuenta las distintas fases por las que transcurre una emergencia o una catástrofe[2].
- Elección y diseño de los medios y sistemas más propicios a cada momento.
- La extraordinaria demanda de las Tecnologías de la Información y Comunicaciones (TIC) en las situaciones de emergencia hace replantearse nuevos procedimientos para sacar el mayor beneficio posible a la capacidad residual que queda tras una gran catástrofe.
- Las misiones que desempeñan los **responsables del enlace**, conocidos como "**Responsables TIC**", y su relación con los usuarios a los que sirven.
- La complejidad de los Centros de Gestión de Emergencias y los Sistemas de Información que los sustentan.
- Los gestores de la respuesta a los desastres, necesitan de herramientas que les puedan ayudar en la clasificación, evaluación, filtrado e integración de la enorme cantidad de información que reciben procedente de distintas fuentes. En definitiva Gestión de la Información en grandes catástrofes.
- La pobre interoperabilidad entre los organismos de socorro es un problema constante, pese a los esfuerzos realizados, que se pone de manifiesto una y otra vez en los momentos más críticos.
- Cómo hacer llegar de manera masiva y en un tiempo muy reducido la información indispensable a la población afectada o susceptible de serlo por una calamidad.
- Se establece de manera clara la relación de las Tecnologías de la Información y Comunicaciones o el enlace, con las funciones de Mando y Dirección que se desempeñan en una emergencia.
- La ascendiente de otros aspectos ajenos al enlace que influyen de manera decisiva en el éxito o fracaso de las TIC.
- La regulación normativa de las telecomunicaciones y el conocimiento de ciertos enlaces especiales que es necesario conocer para hallar la mejor de las respuestas a las crisis que se nos planteen.
- Por último, entendemos que este asunto es tan serio y de tanta trascendencia que al igual que han hecho otros países, cualquier Gobierno serio debe prepararse para el peor de los casos. En el caso concreto de España, proponemos que en la Secretaria de Estado de Telecomunicaciones del Ministerio de Industria se cree un organismo que dirija y coordine a nivel Estado todos los asuntos relacionados con las TIC en emergencias.

Nuestro objetivo de explicar qué es el enlace, cuáles son sus componentes y cómo se deben afrontar los retos inherentes al mismo, estará conseguido si el mensaje llega al lector con la suficiente potencia y claridad, es decir lo que en procedimiento radio se identifica con la expresión "**fuerte y claro**".

Pasemos por tanto a entrar en detalle en el asunto, para lo cual comenzaremos por presentar una serie de conceptos que sirvan al lector para comprender correctamente los mensajes planteados.

2. EMERGENCIA VS CATÁSTROFE

- Emergencia: suceso capaz de afectar el funcionamiento cotidiano de una comunidad pudiendo ocasionar víctimas o daños materiales, afectando la estructura social y económica de la comunidad involucrada y que pueden ser atendidos eficazmente con los recursos propios de los organismos de atención primaria o de emergencia existentes y concebidos a tal efecto.
- Catástrofe o Desastre: es todo evento violento, repentino y no deseado, capaz de alterar la estructura social y económica de la comunidad produciendo grandes daños materiales y numerosas pérdidas de vidas humanas, sobrepasando la capacidad de respuesta de los organismos de atención primaria o de emergencia para atender eficazmente sus consecuencias.

  Desde el punto de vista de las TIC, o del enlace como aclararemos más adelante, las implicaciones serán similares aunque no cabe duda de que en la catástrofe el esfuerzo de éstas sería mucho mayor. En este texto no entraremos a marcar las diferencias entre emergencia y catástrofe o desastre, aunque sin duda las hay. Hablaremos de la emergencia en general suponiendo que ésta alcanza las más altas cotas de intensidad, acercándose a las característica propias de la catástrofe.


15

CAPÍTULO 1

EL "ENLACE"

Los Sistemas de Telecomunicaciones e Información juegan un papel crítico en la gestión y operación de las plantas nucleares, de las presas, de las estaciones que conforman la red eléctrica, de la atención médica, en la enseñanza, en los mercados financieros o en las redes de transporte. Todas las empresas grandes y pequeñas confían en los ordenadores para la gestión de nóminas, control del inventario y de las ventas. Las últimas tendencias son la incorporación de capacidad de computación en todo tipo de dispositivos y entornos, así como la conexión en red de cada vez mayor número de sistemas. En cualquier país del primer mundo el apuntalamiento tecnológico es brutal y abarca desde el bucle de abonado de cada una de nuestras casas hasta los ordenadores que sustentan los procesos más vitales de una nación.

El acceso a los servicios de telecomunicación se ha convertido en los últimos años en algo básico, fundamentalmente para la población más joven, acostumbrada a la correspondencia electrónica o a "retransmitir sus vidas" a través de las redes sociales prácticamente en tiempo real.

Lejos quedan los tiempos de nuestros padres y abuelos en los que la carta postal era anhelada durante meses, sino años. Hoy día, la falta de contacto con nuestros seres queridos por un tiempo prolongado se ha convertido en la pérdida de un bien básico entrando de lleno en los niveles más bajos de la pirámide de Maslow. Existen opiniones encontradas sobre el

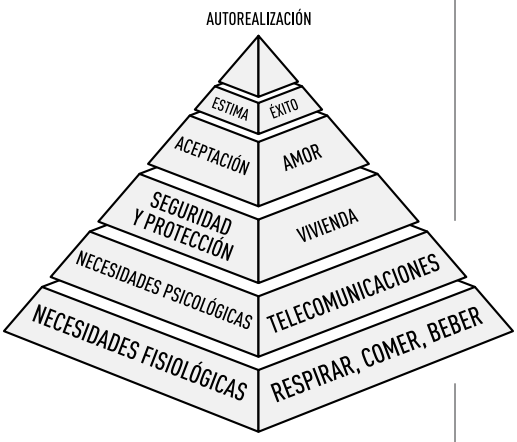
papel a desempeñar de las telecomunicaciones en una situación de emergencia. En un extremo se encuentran los llamados **tecnófilos**, apasionados de las nuevas tecnologías que las consideran imprescindibles, o los que sencillamente las consideran secundarias en comparación con otras necesidades más urgentes a cubrir como son el albergue, la alimentación o la atención sanitaria inmediata.

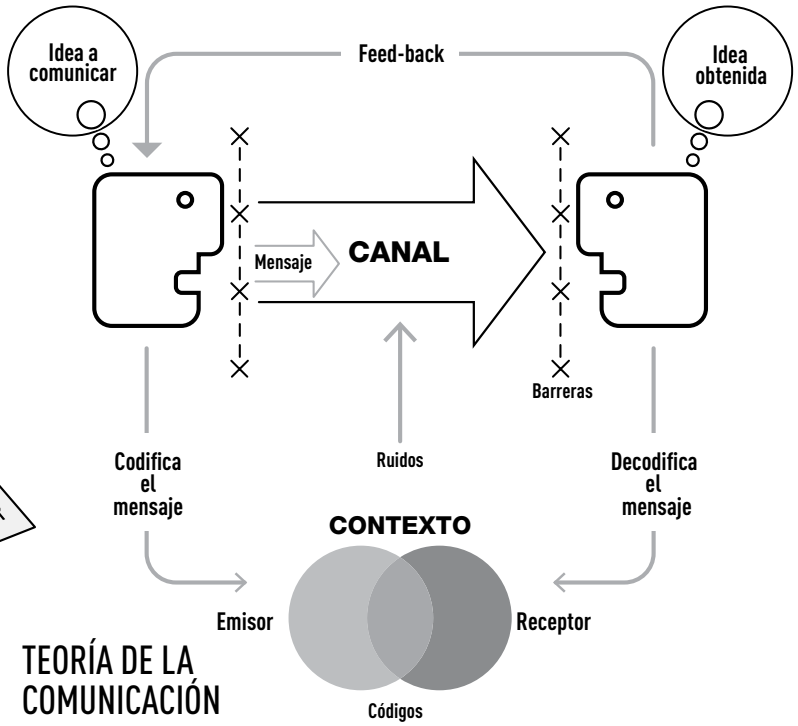
Por encima del papel que cumplen como instrumentos en mano de los especialistas en tareas de socorro, las telecomunicaciones **constituyen una necesidad real de la población azotada por una emergencia,** y por tanto no sólo son básicas para los profesionales que las utilizan para restablecer la situación previa a la catástrofe, sino que también es una necesidad más a suministrar a la población a un nivel equiparable al aporte de víveres o alojamiento. De hecho nos atreveríamos a afirmar que en una gran emergencia, tras asegurar las comunicaciones de los intervinientes de las organizaciones de socorro, **la segunda prioridad pasaría a ser el facilitar el contacto de los damnificados con sus familiares y amigos**.

EL ENLACE EN LAS EMERGENCIAS

Telecomunicación significa etimológicamente "**comunicación a distancia**". La Unión Internacional de Telecomunicaciones (ITU/UIT) para este mismo término dice que se trata de "**toda emisión, transmisión y recepción[3] de signos, señales, escritos e imágenes, sonidos e informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otro sistema radioeléctrico".** Incluso a veces, para simplificar, nos podemos encontrar el término **"comunicación"**, sin el prefijo "tele", aunque se trate del transporte de información entre dos lugares distantes.

PIRÁMIDE TIC DE MASLOW





TEORÍA DE LA COMUNICACIÓN

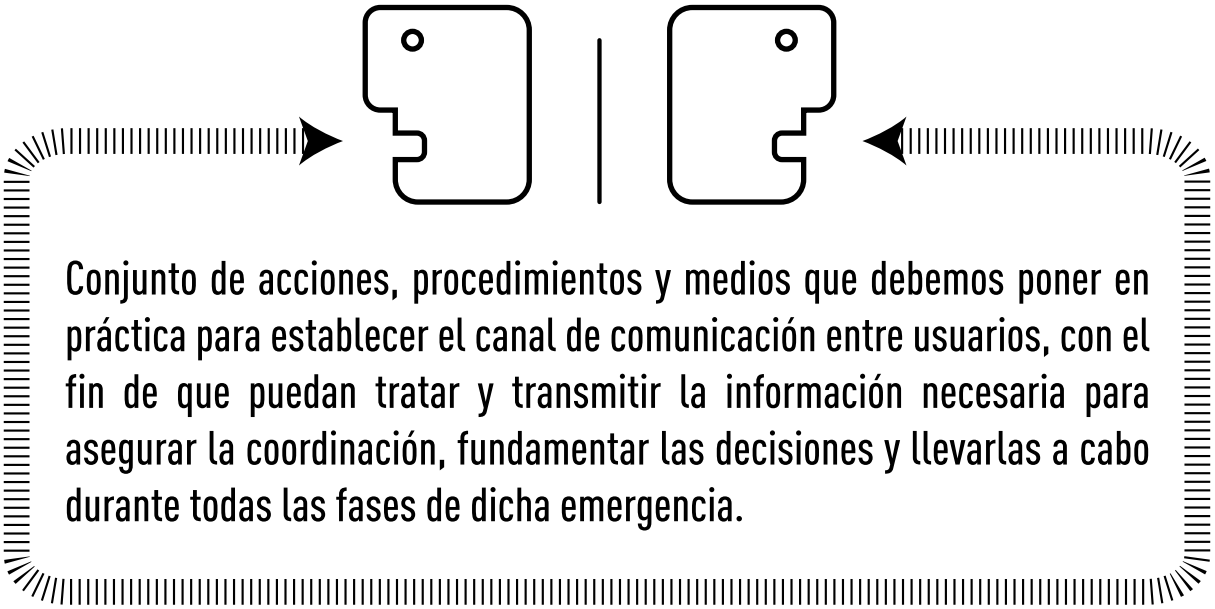
Nosotros pensamos que **esta definición se queda corta** al centrarse en exceso en el hecho físico del transporte de información entre localizaciones, sin tener en cuenta otros aspectos externos que influyen de lleno en éxito o fracaso de la telecomunicación. Aunque las TIC a priori se refieren en el mayor número de casos a las nuevas tecnologías, no podemos obviar que **son parte de una construcción mayor** que involucra a las **personas**

3. En ocasiones se refieren al proceso de envío de información como "emisión", y al de su recogida en lugar de destino como "recepción". También se recurre a veces al término "transmisión" para indicar el proceso que engloba la emisión y la recepción, de principio a fin.

y organizaciones. La pantalla en un sistema informático ofrece información a una persona que tiene sus propios atributos psicológicos y emocionales y que es parte de una organización con su propia cultura y procedimientos. También podíamos mencionar los **condicionantes o presiones provenientes de la sociedad o la política** como factores a considerar. Por lo tanto, para entender cómo las TIC alcanzan su objetivo o fracasan en el intento, siempre es necesario considerar la entidad más grande en la que están inmersas.

Es por ello que en este trabajo vamos a adaptar la **definición tradicional del término militar "el enlace"** que sí tiene en cuenta otros factores. Serán numerosas las referencias que hagamos a las Fuerzas Armadas pues, como se expondrá más adelante, las telecomunicaciones militares y las de emergencias tienen numerosos puntos de encuentro.

DEFINICIÓN DE ENLACE:



Conjunto de acciones, procedimientos y medios que debemos poner en práctica para establecer el canal de comunicación entre usuarios, con el fin de que puedan tratar y transmitir la información necesaria para asegurar la coordinación, fundamentar las decisiones y llevarlas a cabo durante todas las fases de dicha emergencia.

Queremos llamar la atención sobre estas "acciones, procedimientos y medios" a las que se refiere la definición del enlace. En ocasiones, tendrán poco o nada que ver con nuestras **misiones tipo de Responsable TIC**[4] de una organización. Es decir estamos hablando de llevar a cabo cometidos, que sin estar dentro específicamente de nuestras competencias, faciliten nuestro objetivo de enlazar.

Una de las acepciones de "**enlazar**" es la de unir unas cosas con otras. En nuestro caso nuestra misión será materializar la comunicación entre un emisor y un receptor de información, **haciendo uso de los medios materiales o inmateriales** que tengamos a nuestra disposición. Es más...como Responsables TIC habrá veces que nos conformaremos con alcanzar la eficacia, dejando si es necesario en segundo término la eficiencia.

Si además, tenemos la suerte de que tanto el emisor como el receptor cuentan con unos **procedimientos compatibles**, el éxito es alcanzable.

¿Cómo hacerlo? Muy fácil... **¡Como sea!** Nos explicaremos.

LA NORMA BÁSICA PARA ESTABLECER EL ENLACE EN LAS EMERGENCIAS ES QUE SE PUEDE Y SE DEBE HACER USO DE CUALQUIER ACCIÓN, PROCEDIMIENTO Y MEDIO DISPONIBLE.

4. Tal y como dijimos en el prefacio del libro, cada vez que nos refiramos al responsable en una organización de garantizar el enlace, lo haremos como Responsable TIC, independientemente de que haga uso de otros modos para establecer el enlace de modo diferente a las TIC. Aunque pueda resultar en alguna ocasión inexacto, es el nombre más extendido y por el que comúnmente se les denomina.

MODOS DE ESTABLECER EL ENLACE

Las TIC son una herramienta que puede contribuir a mejorar la eficacia de las respuestas a las situaciones de emergencia. Por sí solas no bastan, pero ayudan a realizar mejor y más rápido diversas tareas como la localización de las víctimas o la comunicación entre los diferentes usuarios. El mundo tecnológico ha invadido nuestro día a día. Internet, los aparatos electrónicos ya son una prolongación de nosotros. Esto hace que al pensar en métodos para materializar el enlace, inevitablemente se nos vaya la mente a "**algo con botones" que consume electricidad**. Sin embargo los modos a utilizar para materializar el enlace son muchos y variados.

Veamos los más comunes que tenemos a nuestro alcance.

- **El contacto directo entre responsables de la gestión de las emergencias** es algo obvio. Algo tan sencillo e indiscutible como fijar un lugar de encuentro para tratar algún tema concreto entre los distintos elementos que participan en una emergencia.
- En unión con el anterior está la **yuxtaposición de centros de mando o de coordinación**. Son, sin duda, los dos métodos más eficaces.
- **El intercambio de trabajadores entre organizaciones**[5] o dentro de la propia institución es, o debería ser, algo habitual.
- Y por supuesto los **sistemas de telecomunicaciones e información,** que por sorprendente que parezca para los no versados, pueden ser de diferentes tipos:

5. Comúnmente se les conoce como OFEN: Oficial de Enlace.

- **Medios que emplean procedimientos electrónicos o electromagnéticos, los más comunes y conocidos.** El Telégrafo Eléctrico, inventado por Samuel Morse en el año 1837, el primer teléfono patentado por Graham Bell en 1876, o la primera transmisión del italiano Marconi de señales inalámbricas en 1894, son los antecedentes más reseñables. Por supuesto aquí encontramos todas las comunicaciones basadas en radio, telefónicas, telegráficas, de datos y video. Los servicios de emergencia han sido los usuarios pioneros de sistemas de comunicación electromagnéticos, y en especial de comunicaciones móviles. Nos podemos remontar al siglo pasado, a los años 30 para encontrar equipos de radio en unos 5.000 vehículos de policía y bomberos en Estados Unidos, en lo que podría verse como el precursor de las radiocomunicaciones móviles privadas o profesionales (PMR en sus siglas en inglés).
- **Medios y procedimientos acústicos.** Los Tercios Viejos Españoles combatieron en toda Europa entre los siglos XV y XVII, siguiendo exclusivamente las órdenes transmitidas por tambores. Hoy día se mantiene la comunicación con cornetas, bocinas y silbatos.
- **Medios y procedimientos ópticos y visuales.** Los griegos desarrollaron la Heliografía, reflejando la luz del sol en superficies brillantes y los romanos utilizaron antorchas como sistema óptico telegráfico, puestas en grupos apartados a distancias variantes, en la cima de las montañas para comunicarse. En la marina mercante y en las Armadas se siguen usando persianas, banderolas y paineles.
- **Mensajeros**. Ya los egipcios 3000 a.c. representaban las ideas mediante símbolos (hieroglyphics), y la información era transportada por mensajeros a grandes distancias al ser transcritas en papiros. Estos individuos hoy día, con medios de transporte adecuados a la distancia y misión, siguen uniendo transmisores y receptores de información.
- **Animales adiestrados.** La primera referencia histórica de la **paloma mensajera** es una pintura de los hipogeos de Medinet-Abú, que representa una suelta de palomas para anunciar el advenimiento de Ramsés III. Los romanos y diferentes sultanatos las usaron de modo asiduo y jugaron un papel importante en el sitio de Cádiz durante la Guerra de la Independencia. En la Segunda Guerra Mundial, la resistencia las usaba para estar enlazados con Inglaterra. Las aves les eran devueltas en cestas lanzadas con paracaídas desde los aviones aliados. Junto a los **perros** son los animales tradicionalmente utilizados con las limitaciones propias de volumen de información transmitida y distancia máxima a alcanzar.

ANIMALES ADIESTRADOS

ENLACE USANDO ANIMALES

Soldado alemán de la 2ª Guerra Mundial portando a la espalda una jaula de palomas mensajeras; y perro mensajero, utilizado durante la 1ª Guerra Mundial para llevar información entre unidades del frente.

El objeto esencial del establecimiento del enlace no es otro que el de proporcionar al usuario final una herramienta adecuada para posibilitarle su trabajo durante la fase de la emergencia en la que le corresponda desempeñar su tarea. Por lo tanto deberemos aplicar el método más efectivo, y si hay opción también el más eficaz.

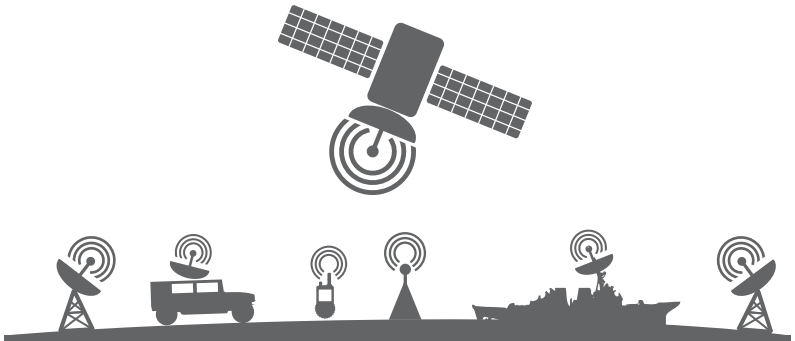
Sin entrar a valorar otras aportaciones de las telecomunicaciones como pudiera ser el **espaldarazo psicológico** para la población damnificada en una catástrofe que le supone el poder hablar con familiares y amigos para conocer su estado, lo cierto es que los distintos sistemas de enlace contribuyen a **facilitar la coordinación y cooperación entre participantes.**

ELECCIÓN DEL MODO Y DEL MEDIO

Nuestra misión como Responsable TIC pasará por facilitar el medio más adecuado a cada circunstancia mediante un cuidadoso estudio de las posibilidades y necesidades. Para ello deberemos tener en cuenta:

- **Las características de cada medio** en cuanto **a fiabilidad** (garantía de que funcione en todo momento, o al menos cuando haga falta).
- **Facilidad de manejo y puesta en marcha** (teniendo en cuenta carga logística aneja).
- **Portabilidad** (posibilidad de cambiar de ubicación).
- **Alcance** (incluyendo distancias máximas y/o zonas de cobertura)
- Y por último la **capacidad** del medio de aceptar el **tráfico** requerido y de proporcionar determinados **servicios** (voz, correo, videoconferencia, etc.).

CLASIFICACIÓN DE LOS SISTEMAS DE TELECOMUNICACIONES



SISTEMAS ANALÓGICOS

La información se convierte en una señal eléctrica. Esta forma de transmisión se llama transmisión analógica, porque el contenido de información mantiene su forma original (ondas de sonido en el aire) incluso cuando se transporta por otro medio (corriente eléctrica por cables). Son los sistemas más tradicionales, cuya gran ventaja es la sencillez, robustez y el bajo coste.

SISTEMAS DIGITALES

La información se digitaliza, se convierte el contenido de la información (letras, números, etc.) en señales que consisten en una secuencia de impulsos, y el enlace distingue solamente entre "corriente o no corriente". Expresado en términos matemáticos: los números uno y cero representan toda la información. Son los sistemas más modernos y ofrece también importantes ventajas, como la mayor calidad.

En ocasiones nos encontraremos con que **ningún medio de comunicación a distancia cumple a la perfección todas las características requeridas** para enlazar en una emergencia y que, por tanto, no responda con exactitud a los requerimientos de los usuarios. En este caso deberemos recurrir a una combinación de ellos con el fin de compensar sus ventajas e inconvenientes.

La **disponibilidad y aplicabilidad de los medios** de telecomunicaciones más idóneos en situaciones de emergencia son el resultado de una estrecha cooperación entre los fabricantes de los equipos, los organismos de emergencias usuarios de los mismos, y los proveedores de servicio que gestionan las distintas redes. Esta relación permitirá evaluar con objetividad qué pueden o no aportar estas tecnologías en diversas situaciones.

Una vez decididos los medios a entregar a los responsables de la gestión, sean autoridades o simples operarios, **sólo falta convencerles de que los usen, y si es posible que los usen correctamente**. Unas veces por "pánico escénico", otras por voluntad predeterminada, chocaremos con la realidad encontrando que nuestros esfuerzos han sido baldíos y que el enlace no se establece por causas que se escapan de nuestras responsabilidades técnicas. Es decir, adaptando el sabio refranero podríamos decir que "**dos no enlazan si uno de los dos no quiere...**".

El canal podrá estar establecido y los elementos necesarios para el establecimiento del enlace estarán en marcha. Sin embargo deberemos mover otros hilos para que a ambos lados del canal de comunicación "se descuelgue el teléfono", **¡Ah! Y para vosotros, los responsables de que todo funcione... mucha paciencia.**

CAPÍTULO 2

CARACTERÍSTICAS DEL ENLACE EN LAS EMERGENCIAS

El que de una u otra manera esté relacionado con alguna organización relacionada con la protección civil o las emergencias, o se dedique a este asunto del enlace (o las TIC, CIS, Telecomunicaciones, Transmisiones...etc.) debe ser consciente de **algunas singularidades que marcan y condicionan** este mundo**,** independientemente del lugar que ocupe en la jerarquía. Si además es el responsable dentro de su agencia o le corresponde la ingente misión de concienciar e instruir a los usuarios, que quede entre nosotros, pero que sepan que no nos dan ninguna envidia.

Vamos por tanto a exponer estas características, que van a condicionar nuestra tarea como **Responsables TIC** y por supuesto también a los **usuarios** de cualquier tipo de medio de enlace.

INDISPONIBILIDAD DE LAS REDES.

Las fuerzas de la naturaleza (o la mano del hombre) tienen un poder descomunal que golpea con diversa intensidad a las estructuras de telecomunicaciones preestablecidas en las sociedades. En los países del "primer mundo"se toman una serie de precauciones que obligan a implementar las TIC con determinadas medidas de seguridad para soportar unos niveles de estrés. En muchas ocasiones estas precauciones no son suficientes y se ven afectadas quedando muchas de ellas inoperativas. En los países menos desarrollados como se puede suponer los efectos suelen ser mucho mayores ya que en ningún momento se llegan a aplicar tales normas.

Las causas de tal **indisponibilidad de redes** pueden ser entre otras las siguientes:

- **Recursos de telecomunicaciones dañados**

  Aunque entre las prioridades definidas en la **Conferencia Mundial sobre Reducción de Desastres** celebrada en Japón en enero de 2005, se estableció la necesidad de proteger y fortalecer las infraestructuras de comunicaciones al considerarse críticas, lo cierto es que los recursos de telecomunicaciones ligados a infraestructuras terrestres se ven afectados en un alto grado cuando ocurre una gran emergencia.

  Los tendidos de **cableado** de cobre y, en mayor grado, los de fibra óptica sufren **roturas** en caso de seísmos, o se quedan las conducciones **cubiertas por el agua** en las inundaciones. Las estaciones base de telefonía móvil quedan inoperativas por destrucción física o por la pérdida del enlace con el resto de la red. Son normales la caída de los radioenlaces o las roturas de cableado que las une entre sí.

  El 12 de enero de 2010 tuvo lugar un gran terremoto en Haití. El sismo afectó al único cable submarino de fibra óptica que conectaba a Haití con el exterior. Afortunadamente se dio la circunstancia de que la mayoría de los proveedores de acceso a Internet tenían salida internacional a través de satélite, por lo que a los pocos días, una vez reapuntadas las antenas y restituido el suministro eléctrico, se pudo restablecer la conexión con el resto del mundo.

- **Pérdida de suministro eléctrico**

  Tal y como acabamos de ver en el ejemplo anterior, **las fuentes de alimentación eléctrica son vulnerables** a las repercusiones físicas que puede originar una catástrofe. Los sistemas de telecomunicación quedan fuera de servicio, a menos que tengan acceso a otras fuentes de energía alternativa basadas en Sistemas de Alimentación Ininterrumpida (SAI), generadores auxiliares (grupos electrógenos), placas o mantas solares o una combinación de varias de estas posibilidades. Sirva como ejemplo que en la Región del Bío Bío, en Chile, tras el terremoto de 8,8° Richter que asoló varias zonas del país andino el 27 de febrero de 2010, seis días después, sólo el 18 % de las estaciones-base de telefonía móvil se encontraban operando debido a la carencia de energía eléctrica. La combinación de cortes de corriente, rotura de conducciones de cableado y caída de los postes que formaban parte de la infraestructura de acceso a los domicilios[6], hicieron que sólo el 20% de la capacidad de la red de telefonía fija estuviera operativa una semana después.

- **Saturación de los medios disponibles**

  Si pese a todo alguno de los sistemas ha quedado operativo, entonces deberemos tener previsto que con toda probabilidad **se acabarán saturando.**

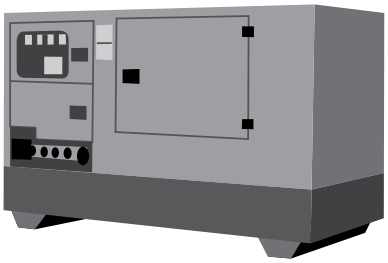
  Encontraremos **tres causas**. Primera, los **pocos recursos** que queden deberán asumir con su capacidad residual el tráfico

11-S

Las antenas principales de los sistemas de radiocomunicaciones del Departamento de Bomberos de Nueva York, la policía de Nueva York, y del Sistema de Emergencias Médicas de la Gran Manzana estaban situadas en la azotea de la Torre 1 del World Trade Center, la primera que se derrumbó tras los ataques. Debido a este hecho las operaciones se vieron gravemente influenciadas.

6. Informe presentado por la Subsecretaría de Telecomunicaciones del Gobierno Chileno el día 3 de marzo de 2010.

ALTERNATIVAS DE SUMINISTRO ELÉCTRICO



que no pueden cursar las redes caídas. Segunda, la propia gestión de la crisis lleva implícita un **aumento del volumen de llamadas** a cursar. Y tercera y última, **la propia naturaleza humana.** Es inevitable que se produzca un aumento de llamadas entre familiares y amigos para informar del estado de las personas afectadas.

Tras el impacto del primer avión en los atentados de las Torres Gemelas de Nueva York, los informes posteriores indicaron que momentos después del choque se registró la saturación de la telefonía fija y móvil de Manhattan. El 29 de agosto de 2005, se produjo la llegada a Nueva Orleans del huracán Katrina. Las pocas comunicaciones telefónicas y accesos a Internet que resistieron el impacto acabaron colapsando por sobresaturación. Las áreas afectadas quedaron incomunicadas con el resto del país. Una vez más la labor recayó en los radioaficionados quienes cursaron todo el tráfico con las autoridades y unidades de salvamento.

- **Sistemas no fiables**

  Los sistemas supervivientes se vuelven inconsistentes, comenzando a fluctuar los enlaces. Hasta que las compañías eléctricas y de telecomunicaciones responsables no sean capaces de restablecer las redes; y hasta que los ciudadanos no pasen

CORTES EN EL SUMINISTRO ELECTRICO

Ante los cortes de suministro eléctrico los sistemas de telecomunicación quedarán afectados a menos que tengan acceso a otras fuentes de energía.

- Las baterías son la alternativa más evidente, pero su capacidad y el tiempo durante el cual pueden suministrar corriente son limitados.
- Los grupos electrógenos o generadores alimentados por motores a explosión, pueden atender demandas mayores durante periodos más largos. Existen de diferentes tamaños y potencias.
- Mantas solares, para recarga de baterías.
- Instalación de paneles solares o generadores eólicos. Estos requieren conocimientos y personal especializados.
- Generadores manuales o "molinillos". De aspecto similar a los molinillos de café de nuestras abuelas, que sirven para recargar baterías.
- Células energéticas, que producen energía eléctrica mediante la combustión del hidrógeno y el oxígeno.

FUNCIONAMIENTO DE LAS TIC EN EL 11-S

INFORME DEL NIST

El derrumbe del World Trade Center (WTC) en Nueva York tras los atentados terroristas del 11 de Septiembre de 2001 provocó la muerte de 2800 personas de las cuales 350 pertenecían a los servicios de emergencia y rescate. El Instituto Nacional de Estándares y Tecnología (NIST) estudió el comportamiento de los sistemas de radiocomunicaciones empleados por los servicios de emergencia durante la catástrofe.

Los informes del NIST revelaron que todos los organismos de emergencias implicados tuvieron problemas de distinta índole con sus sistemas de radiocomunicaciones, causados por dos motivos principales: por un lado, la elevada atenuación que las señales de radio sufren en edificios de hormigón armado y acero. Y por otro lado, el incremento espectacular en el tráfico de comunicaciones radio.

Tras el primer impacto, el tráfico de radiocomunicaciones se multiplicó por 5 aproximadamente y posteriormente por 3, respecto a una situación de normalidad. La primera consecuencia de este incremento fue la dificultad en la gestión de los mensajes. Del análisis de las grabaciones se desprendió que entre ⅓ y ½ del total de los mensajes de radio no pudieron completarse o eran ininteligibles, bien por problemas de cobertura, bien por la incapacidad de gestionar tan elevado volumen de mensajes en los centros de control.

el shock inicial, debemos prever cortes en los servicios, que en el mejor de los casos serán puntuales, mientras que en otras ocasiones serán definitivos.

- **Problemas de Interoperabilidad**

  Pese a que en los últimos años es una **obsesión** (al menos en la teoría), lo cierto es que muchos de los organismos que tendrían que trabajar juntos en estos momentos de emergencia, **utilizan sistemas de transmisiones incompatibles**. El Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos concluyó tras la tragedia del 11-S de 2001, que uno de los principales problemas fue la falta de interoperabilidad entre las agencias intervinientes.

  Lo ideal, por supuesto, sería una interoperabilidad total entre organizaciones. Como hoy por hoy, esto es ciencia ficción, no queda otra que recurrir a las llamadas "**interfaces**". Se llaman así a los puntos o puentes de conexión entre diferentes redes para intercambiar la información necesaria entre usuarios de distintas organizaciones que usan sistemas incompatibles desde el punto de vista técnico u operativo.

  Cada medio de transmisiones en uso marcará los factores que condicionaran la interoperabilidad. Esto no es nada nuevo, se trata de encontrar un lenguaje común o pasarela para hacer efectiva la comunicación, algo que técnicamente a veces es imposible, y otras económicamente inviable.

  En el capítulo 8 profundizaremos sobre este aspecto fundamental para el enlace.

- **Diversidad y multitud de usuarios**

  Como veremos en apartados siguientes dependiendo del momento dentro de la emergencia encontraremos distintos tipos de usuarios. Las telecomunicaciones son una herramienta imprescindible en cualquier organización, y dentro de ésta en todos los niveles de la jerarquía independientemente que se dediquen a la dirección o a la ejecución táctica.

  Desde políticos tratando de recibir información en los primeros momentos de la catástrofe, pasando por elementos de búsqueda y rescate, cuerpos policiales, o voluntarios de protección civil. Todos tienen en común la necesidad de dar y recibir instrucciones de lo que está aconteciendo. Gracias a los equipos de comunicaciones portátiles toda persona se convierte en un posible usuario. Esto va a ocasionar sin dudas problemas en las redes, ya que muchos de ellos desconocerán los procedimientos o no tendrán ninguna formación (o ésta será muy básica) sobre los equipos a utilizar. Esto se traducirá en retardos, ocupación innecesaria de canales y saturación de los mismos.

- **Urgencia de la información a tramitar.**

  Los primeros momentos de una emergencia están marcados por el caos y el descontrol. La necesidad de salvar vidas e informar a las autoridades de lo acontecido, hace inevitable que todo el mundo intente **hablar de manera urgente con sus corresponsales**. Dado que la capacidad de los sistemas de telecomunicaciones es finita, los responsables, a todos los niveles, deben cuantificar y asignar la debida prioridad a las comunicaciones y asegurar que se ejerce una adecuada disciplina en el flujo de información.

- **Se manifiesta el mal diseño de algunas redes**

  En este apartado trataremos dos aspectos diferentes.

  - **Zonas remotas o rurales**

    Uno de los beneficios de la manida Globalización es, sin duda, que **las nuevas tecnologías son accesibles prácticamente desde cualquier zona urbana del mundo.** En mayor o menor grado las redes urbanitas están dotadas con unas capacidades y unas redundancias lejos de ser alcanzadas en zonas rurales. Cuando las desgracias acontecen en ciudades suele quedar siempre un soporte de telecomunicaciones residual, que con pequeñas reparaciones, pueden revivir los sistemas en modo degradado.

    Por el contrario **en las zonas rurales son evidentes las deficiencias.** Falta de infraestructuras, poca cobertura de redes radio o incluso la escasa capacidad de la telefonía móvil. Las antenas que atienden a los pueblos se suelen caracterizar por proporcionar un número reducido de canales simultáneos, en ocasiones limitados a tráfico de voz o con una mínima capacidad de transmisión de datos (tecnologías 3G o 4G).

    Cuando las calamidades tienen lugar en este tipo zonas remotas, la situación resulta extremadamente complicada desde el punto de vista del enlace. No se rompe nada...porque no había nada que romperse. El esfuerzo a realizar por la dirección de la emergencia en estos lugares es titánico para garantizar un mínimo de flujo de información, puesto que **hay que construir una infraestructura TIC partiendo prácticamente de cero.**

¤ **Zonas urbanas**

Ya hemos visto que en los países más avanzados las redes públicas deberían estar diseñadas con ciertas garantías para resistir cierto nivel de estrés. **Los operadores suelen contar con medios de reserva y centros de respaldo para soportar caídas de servicios.** Incluso existen tendidos de fibra óptica completos de respaldo y son habituales los vehículos móviles denominados "**restauradores de red**" que permiten reforzar o reemplazar nodos de telecomunicaciones caídos.

Las últimas tendencias apuntan a que los gobiernos se obligan a sí mismos a prever el uso de las telecomunicaciones en situaciones extremas de crisis o emergencia. Es el caso de los países firmantes del **Convenio de Tampere** del cual hablaremos mas profusamente en el capítulo 16. Los Gobiernos obligan por ley, o **acuerdan con los operadores de telecomunicaciones públicos, poder priorizar las comunicaciones de los equipos de rescate y emergencia.** Cuando la catástrofe se desencadena y la red no tenía prevista esta priorización, normalmente se acaban produciendo los efectos característicos del enlace en emergencias.

A veces se amortigua este hecho con la **existencia de determinadas redes privadas** para equipos de socorro o policiales, pero que obviamente tienen una **capacidad mucho más reducida que las redes públicas.** Sin embargo estas redes particulares suelen estar ya implementadas con requisitos exigentes para trabajar en condiciones degradadas. La mayoría de las veces cuentan con sistemas de alimentación ininterrumpida y generadores auxiliares para el caso de caída de la red eléctrica, que como hemos visto es uno de los principales problemas al que nos enfrentaremos.

- **Insuficiencia de medios**

En situaciones extremas existen grandes probabilidades de que los medios de comunicación habituales no funcionen correctamente. En tales circunstancias **habrá que acudir a materiales alternativos** que normalmente **no van a existir en las cantidades necesarias** para poder sustituir por ejemplo a la telefonía móvil. Nos estamos refiriendo fundamentalmente a equipos portátiles, bien de radio, bien de telefonía satélite, que por su facilidad de despliegue se deberán poner a disposición de los elementos de intervención o de la dirección de la emergencia más importantes.

- **Indisciplina e Intrusismo en las redes**

Habrá momentos en los que la "**ley de la jungla**" sea la que impere en el aspecto del enlace. **La disciplina en la red** será prácticamente inexistente en los primeros minutos. Los usuarios no respetarán las conversaciones de otros corresponsales. Se producirá un constante atropello en las conversaciones radio, o la población hará caso omiso a la no utilización de los teléfonos en beneficio de los intervinientes.

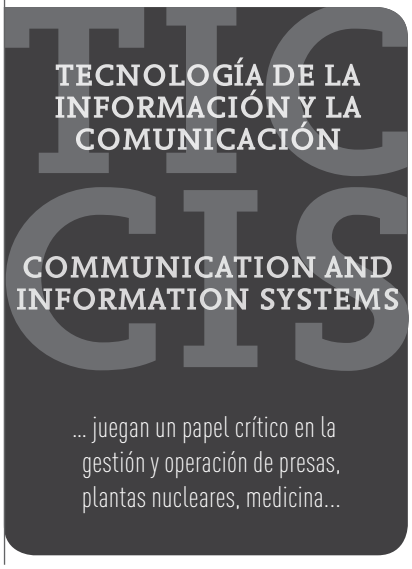
También podrán aparecer **usuarios** de los medios de transmisiones **que no estén autorizados**, y que mediante diferentes procedimientos, intentan acceder a la información sensible de la gestión del incidente en busca de alguna noticia impactante.

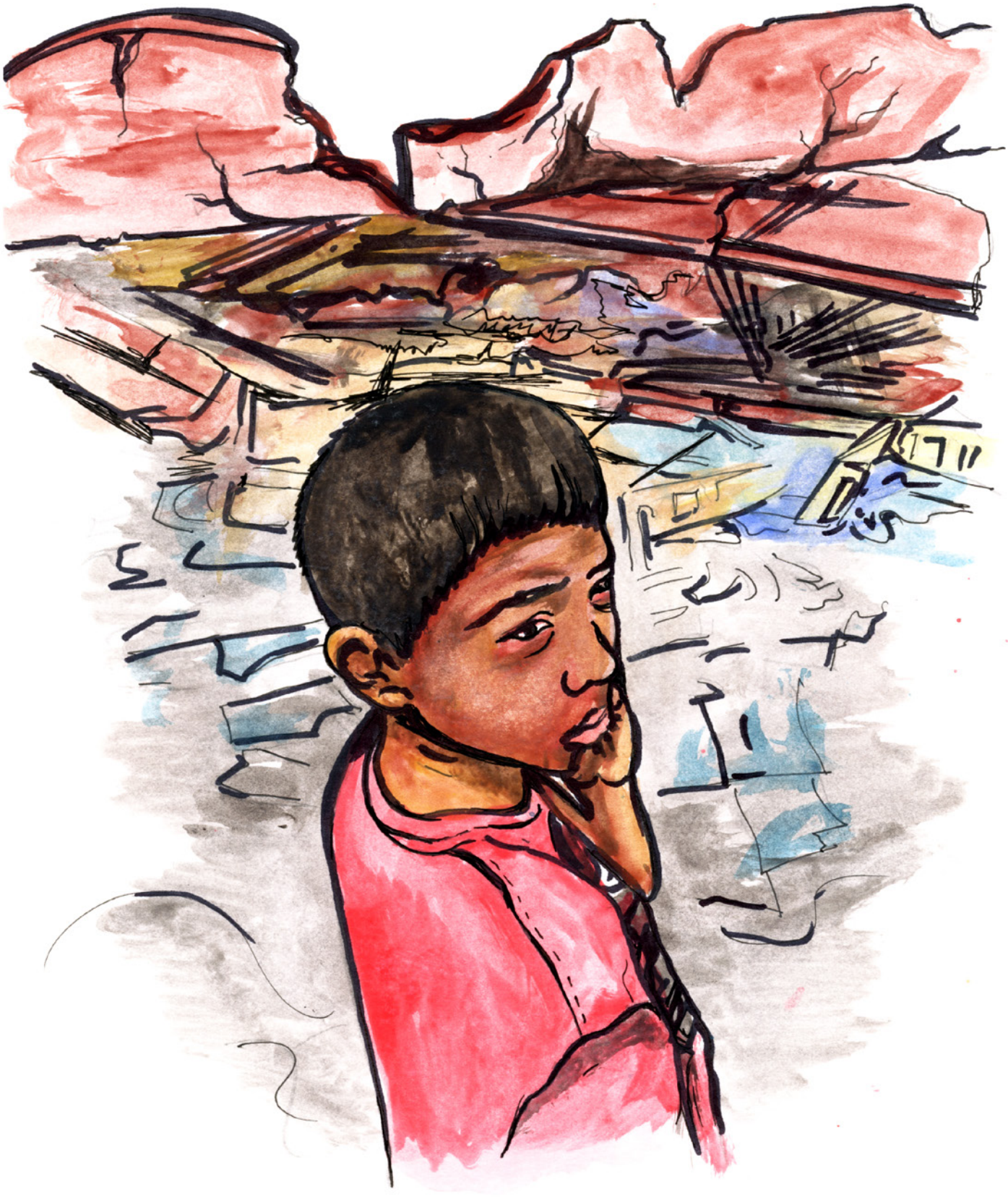
- **Incumplimiento de normativa legal existente en las redes**

Tampoco es de descartar que en estos momentos de *totum revolutum* el **tráfico cursado por las distintas redes no se ajuste a la normativa legal,** sobre todo en lo referente a la protección de datos personales y a la seguridad informática.

- **Pueden aparecer condicionantes políticos y personales**

Aunque pudiera parecer que en un tema tan técnico como el que nos ocupa, la influencia de determinados estamentos no sería perceptible, lo cierto es que aunque nos pese, en algún momento nos puede afectar de lleno. Nos referimos a l**os "otros" condicionantes** del enlace. No sería la primera vez que determinada autoridad ordena que se deje de utilizar un sistema para, por ejemplo, dejar de recibir órdenes de determinado organismo. O sencillamente que traten de justificar una decisión errónea amparándose en un supuesto fallo de los equipos de telecomunicaciones.





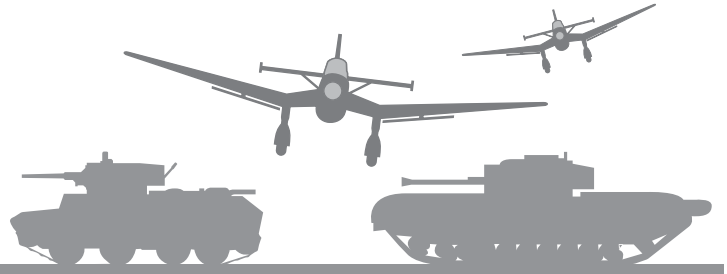
CAPÍTULO 3

SOLUCIONES A MEDIDA: DISEÑO APROPIADO

Un alto porcentaje de las características del enlace en las emergencias que se han señalado en el capítulo anterior eran ya conocidas en un contexto diferente desde hacía tiempo. En su día se detectaron, se estudiaron, y a lo largo de los últimos decenios se han venido ofreciendo soluciones diversas a un problema similar. Nos estamos refiriendo al enlace o **transmisiones en los conflictos armados.**

Las Fuerzas Armadas de todos los países del mundo tuvieron que encontrar soluciones de telecomunicaciones válidas para dirigir a las tropas en el combate. Desde muy pronto se enfrentaron a escenarios en los que las **redes de transmisiones de la época eran destruidas** porque el enemigo rápidamente fue consciente de la superioridad que adquiría si le impedía hacer uso de sus medios de comunicaciones. En el siglo XIX bastaba con cortar el cable del poste de telégrafos para aislar una ciudad del resto del mundo. El primer blanco atacado durante la Guerra del Golfo Pérsico en el año 1991 fue la red de telecomunicaciones iraquí. Una vez dicha red fue destruida, los iraquíes nunca volvieron a recuperar su capacidad operativa.

La conducción de las operaciones en el campo de batalla nunca fue un problema. Desde tiempos inmemoriales los generales movían sus elementos de maniobra a base de mensajeros, banderolas, toque de corneta o redoble de tambor. Eso sí... no sin cierto retardo. La orden dada por el emisor tenía un desfase entre el momento de ser generada y el inicio de la ejecución de la misma por parte de la unidad receptora. Este retraso venía marcado por el procedimiento de transmisiones empleado y la distancia que separaba al transmisor del receptor.



ANTECEDENTES DE LAS COMUNICACIONES MÓVILES

La irrupción de la radio en la Primera Guerra Mundial constituyó un hito en la infraestructura de telecomunicaciones en el campo de batalla, produciéndose una gran aceleración de las operaciones motivada por la inmediatez de la recepción de órdenes entre los diferentes elementos que se movían en la zona de contienda. A lo largo de la historia los **Ingenieros militares** (o Ingenieros del Rey en España), hoy día representados por la especialidad o cuerpo de **Transmisiones** en todos los ejércitos del mundo, tuvieron que desarrollar sistemas para **sustituir recursos de telecomunicación dañados, falta de suministro eléctrico**, e incluso tuvieron que inventar "**la disciplina radio[7]**", para evitar la **saturación de las redes.** Huelga decir que la **falta de equipos** era una constante. Nunca había suficientes.

Los intensos bombardeos de la Segunda Guerra Mundial convertían a las incipientes redes telefónicas públicas, en **poco fiables,** en el mejor de los casos, cuando no eran completamente borradas del mapa. La innovadora ***Blitzkrieg[8]***, o guerra relámpago introducida por los alemanes en la Segunda Gran Guerra introdujo la filosofía de atacar entre otros objetivos los centros de transmisiones y puestos de mando del enemigo. Mientras que los aliados habían preparado unas comunicaciones basadas fundamentalmente en tendidos de cable anclados al terreno que unían sus centros de mando, el *Generaloberst* de la *Werhmacht*, Heinz Wilhelm Guderian, artífice de las fuerzas acorazadas alemanas, solicitó que **cada carro de combate estuviera equipado con radio**. Al comienzo esta solicitud le pareció al mando alemán una exageración, pero el General Guderian se las arregló para convencerlos que tenía razones suficientes para pensar que era posible hacer un nuevo tipo de guerra. Además decidieron que las divisiones Pánzer alemanas tuvieran sus equipos de comunicaciones montados en vehículos del mismo tipo que las fuerzas que acompañaban, constituyendo el **Batallón de Señales Pánzer** de la división, ingeniando de este modo los **puestos de mando móviles de la era moderna**.

Con las primeras operaciones militares conjuntas[9] y combinadas[10], apareció el problema de la **falta de interoperabilidad,** al que ya hemos

COMUNICACIONES EN LA *BLITZKRIEG*

Las telecomunicaciones, durante las campañas de Polonia y Francia fueron claves para el éxito de las tropas alemanas, pues las fuerzas acorazadas no podrían haber realizado los veloces avances que hicieron, de estar incomunicados o de haber empleado las técnicas de telecomunicaciones de la Primera Guerra Mundial.

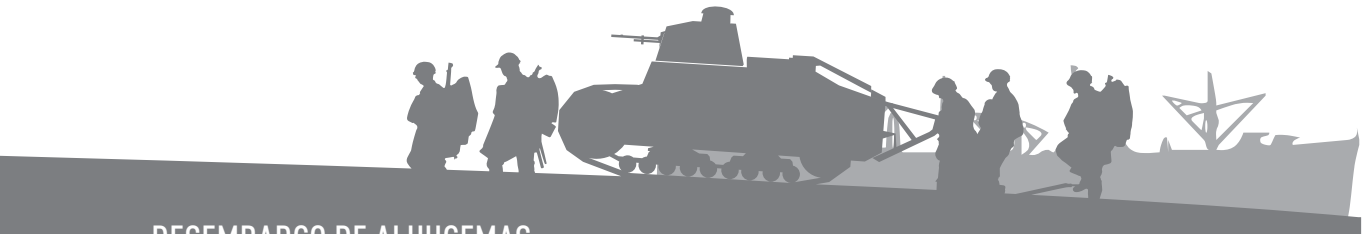
Fueron notables también las comunicaciones entre las fuerzas terrestres y la aviación de apoyo. Los Stukas eran el arma aérea de apoyo a las divisiones Panzer y su trabajo se sincronizaba por radio con las tropas terrestres.

A la vez que desarrollaron las comunicaciones radiales, crearon el cable telefónico de campaña de doble alcance, que por medio de equipos especialmente diseñados amplificaban las señales de voz, telegrafía y teletipo que se utilizaban simultáneamente en el campo de batalla. Los cables se tendían a razón de 150 km diarios.

7. Se entiende por "disciplina radio" las medidas que impone una de las emisoras de la red que es reconocida por el resto como "directora", y que es la que marca los momentos en que cada uno de los corresponsales puede entrar en malla.
8. Nombre popular alemán por el que se conoció a la doctrina bélica basada en un bombardeo inicial masivo, seguido de un ataque de fuerzas terrestres acompañadas de apoyo aéreo cercano que se desplegaban a la mayor velocidad posible, para golpear con contundencia y sorpresa en la retaguardia del enemigo, impidiendo que pudiera organizar una defensa coherente.
9. Son aquellas operaciones en las que participan los ejércitos de tierra, mar y aire de una misma nación a la vez en el mismo combate. Hasta esa época se hacían guerras separadas, la terrestre, la aérea y la naval.
10. Son aquellas operaciones en las que participan ejércitos de diferentes naciones formando parte de un mismo bando y enfrentándose a un mismo oponente.

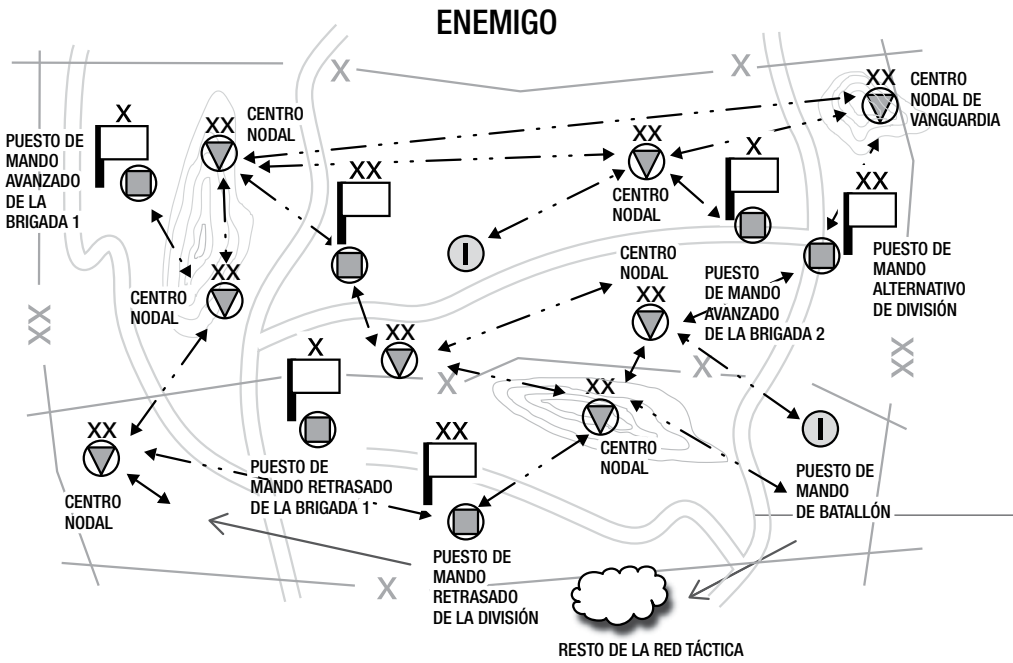
TELECOMUNICACIONES EN ALHUCEMAS

Desde el acorazado Alfonso XIII, el Capitán Enrique Gallego, coordinó al Centro Electrotécnico y de Comunicaciones, las compañías de redes telegráficas, radiotelegráficas, de telegrafía óptica, telefónica y radiotelefónica para contribuir al éxito de la operación.



DESEMBARCO DE ALHUCEMAS

RED MALLADA



hecho mención. El 8 de Septiembre de 1925, en **Alhucemas**[11], los soldados del entonces **Regimiento de Telégrafos,** antecedente del actual Regimiento de Transmisiones Tácticas 21 del Ejército de Tierra español, tuvieron que organizar las comunicaciones[12] del primer desembarco anfibio realizado con éxito en la historia del mundo, y que el mismo Eisenhower estudió al detalle para su ataque a las costas Normandas. Y es que nadie había previsto la necesidad de contar con equipos de comunicaciones compatibles con los de otros ejércitos de su propio país, y mucho menos con los de los aliados.

Hasta este punto podríamos decir que hemos acumulado razones para pensar que **existe una similitud más que notable entre las singularidades del enlace en una emergencia y las que se producen en una zona de combate.**

CENTROS DE TRANSMISIONES NODALES

Hasta finales de los ochenta, las redes de transmisiones tácticas militares se concebían como una **estructura de nodos** unidos entre sí. Se partía de una infraestructura de telecomunicaciones terrestre, normalmente basada en potentes Cuarteles Generales con unos Centros de Comunicaciones proporcionales; y a través de los denominados **Centros de Transmisiones Nodales** se iba alargando y ensanchando la red hasta llegar a la vanguardia donde tenían lugar los combates.

La red se materializaba estableciendo una **retícula o malla**[13] de tal manera que cada centro nodal estuviera como mínimo enlazado a otros dos. El objeto buscado con esta regla era evidente. Si alguno

RED NODAL MILITAR DE LOS AÑOS 90

Cada Centro Nodal o Puesto de Mando debe estar enlazado como mínimo con el resto de la red por dos vías diferentes, de esta manera si alguno de los centros es destruido siempre habrá una vía de enlace alternativa. A más número de vías alternativas, mayor robustez de la red ante un posible ataque del enemigo a los centros de transmisiones o puestos de mando.

11. Mediante una acción combinada de las fuerzas de tierra, mar y aire del ejército español y en menor medida del francés, desembarcaron 13.000 soldados españoles en un territorio hostil controlado por los rifeños a las órdenes de Abd el-Krim.
12. Como consecuencia se realizaron ejercicios en los que intervienen las secciones de enlace de toda la brigada de Melilla y las unidades de «ingenieros de transmisiones», estudiándose y perfeccionando los enlaces internos de esta gran unidad, los externos con la división y los que permitían los apoyos navales y aéreos.
13. Se utiliza el verbo "mallar" para indicar que se cubre la zona de acción con una red de nodos.

de los centros con los que un nodo estaba unido era destruido, la información se reencaminaría por el que quedara, garantizando así la **supervivencia de la red**.

Cualquier unidad que se moviera en el área cubierta por la retícula conformada por los centros nodales podía unirse a la red ("engancharse" en argot TIC) a través de estos nodos. Por entonces **el uso de terminales satélite era escaso** y el rol protagonista lo ejercían **los radioenlaces[14] de visión directa.** Las unidades de primera línea cumplimentaban su misión frente al enemigo gracias a las radios, pero mantenían radioenlaces desde sus Puestos de Mando con los centros nodales más a vanguardia para asegurar su integración en la cadena de mando.

Hoy día, **muchas organizaciones de emergencias, sanitarias y de protección civil, siguen manteniendo esta "filosofía nodal" en las redes privadas que montan,** aunque adaptadas a sus características. Veamos como lo hacen.

El campo de batalla se sustituye por la **zona de actuación** o ámbito de competencia de la organización, los centros nodales militares se sustituyen por **estaciones-base[15]**, bien de telefonía móvil, bien de redes radio trunking (dependiendo del sistema que utilicen), y los puestos de mando de brigadas y divisiones son reemplazados por **comisarias, parques de bomberos, o Puestos de Mando Avanzados (PMA)** de los organismos civiles.

Desde el punto de vista de un **Responsable TIC,** si nos referimos a una organización civil, o a la de un **Oficial CIS** en terminología militar, las **circunstancias** de dotar de comunicaciones una zona de emergencia distante y fuera de cobertura de las redes habituales de uso, y el garantizar las transmisiones en una zona remota dónde se va a producir un combate, son prácticamente **idénticas**.

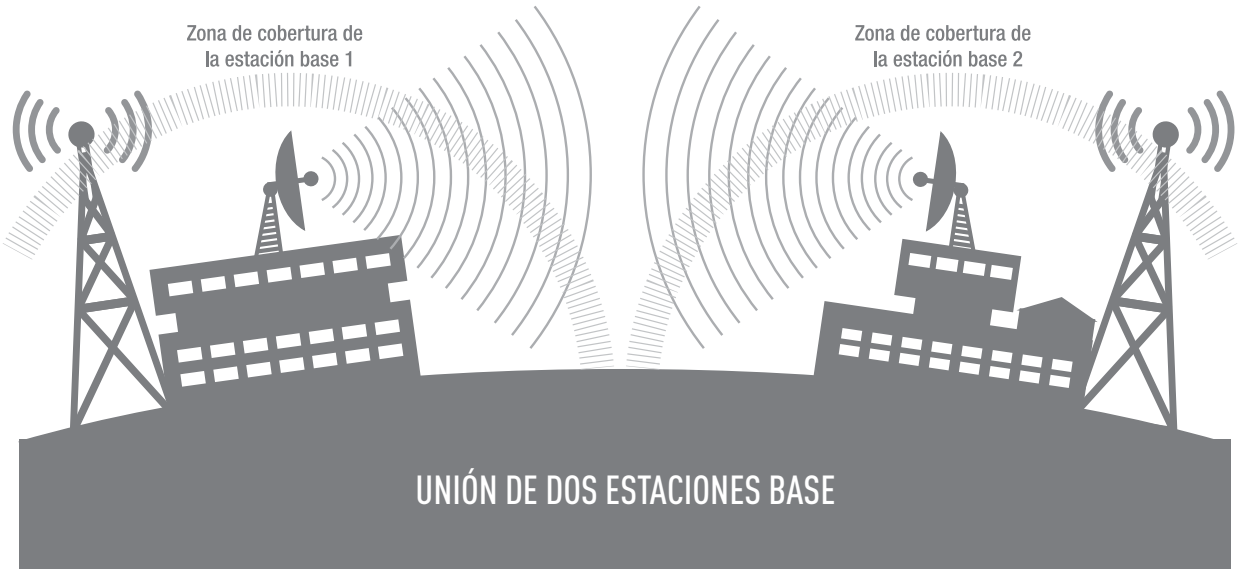
En ambos dos casos se trata de **asegurar el enlace y materializar la cadena de mando mediante el uso de las telecomunicaciones**,

14. En el capítulo 5 se explica en detalle qué es un radioenlace.

15. Estación-base: equipamiento, que proporciona cobertura de telefonía móvil o red radio trunking a una zona próxima formando la denominada célula de cobertura. La superposición de estaciones base proporciona la cobertura de un área mayor, permitiendo que los usuarios se "enganchen" a la estación base que proporcione mejor calidad o que se encuentre libre en cada momento.

ESTACIONES BASE DE REDES RADIO TRUNKING O DE TELEFONIA MÓVIL

La forma habitual es mediante radioenlace o cable, bien fibra óptica, bien cable de cobre multipar.



UNIÓN DE DOS ESTACIONES BASE

uniendo a los intervinientes (fuerzas y cuerpos de seguridad del estado, bomberos, sanitarios, etc.) con los centros de decisión (Puestos de Mando, PMA, Centros de Coordinación o agencias 112).

A modo resumen diremos que estos organismos vienen a implantar tantas estaciones-base o nodos como sea necesario para cubrir sus zonas de actuación, creando zonas de cobertura alrededor de las antenas de estas estaciones-base. Estas **zonas de cobertura** deben estar solapadas para que un usuario que se mueve de una a otra no pierda el enlace. Cuando no se consigue dan lugar a las zonas sin enlace conocidas por **zonas de sombra**.

Podemos encontrar sin embargo algunas **diferencias** entre el diseño de redes militares y el de organismos de gestión de emergencias.

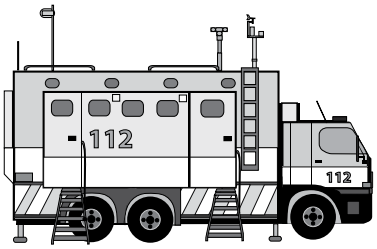
- En el caso militar los nodos son dispositivos móviles no anclados al terreno, mientras que en el caso de las organizaciones civiles relacionadas con las emergencias sí que suelen ser fijas porque se apoyan en infraestructuras de telecomunicaciones permanentes.
- La segunda versa sobre el modo de unión entre nodos. Los centros nodales militares se unían entre sí principalmente por radioenlaces, mientras que hoy día las estaciones base de telefonía móvil y redes trunking usadas por los servicios de emergencia suelen hacerlo mediante fibra óptica.
- En el campo militar, el soldado no accede normalmente a la red directamente con su equipo de telecomunicaciones de dotación. Tenían que hacerlo a través de los Puestos de Mando desplegados. Que cualquier policía, sanitario o bombero pueda acceder a la red cuando lo necesite es una ventaja incontestable.

Muchos de los llamados PMA (Puestos de Mando Avanzados) que se utilizan en las organizaciones de protección civil, precisan tener acceso a su red privada para materializar el enlace con intervinientes y sus instalaciones fijas.

El gran contratiempo se produce cuando la emergencia se declara en una zona en la que no hay cobertura de las redes privadas de *trunking* o no se puede utilizar la telefonía móvil. En este momento **tanto los intervinientes como el propio PMA se ven avocados al aislamiento** al no poder establecer los enlaces necesarios para la gestión de la emergencia.

NODOS CIS/TIC DESPLEGABLES

Una vez más **un problema similar** apareció con anterioridad **en el contexto militar** a finales del siglo XX. Los conflictos empezaron a cambiar su fisionomía, apareció la llamada asimetría, donde las partes confrontadas dejaban de ser ejércitos regulares y las fuerzas insurgentes con técnicas terroristas ganaban terreno. Surgió un nuevo concepto, "**el campo de batalla vacío**", el cual entre otras consecuencias supone la imposibilidad de mallar las enormes zonas de terreno que pasaban a constituir potenciales zonas de operaciones. El terreno era demasiado extenso para ser ocupado en permanencia por tropas, o sencillamente se podía tratar de zonas discontinuas separadas unas de otras por miles de kilómetros. Ante la imposibilidad de seguir usando centros nodales se adoptó una nueva idea. La del **Nodo CIS Desplegable**[16].



CAMIÓN PMA

PUESTO DE MANDO AVANZADO DE CCAA

La Fundación La Caixa hizo una donación a todas las comunidades y ciudades autónomas de un camión para poder dirigir las operaciones de emergencia de nivel 2 e inferior desde las cercanías donde ha ocurrido el evento.

16. Nodo CIS Desplegable: Nodo de Telecomunicaciones y de Sistemas de Información Desplegable de una unidad militar.

NODOS CIS DESPLEGABLES

SISTEMA CIS DE LA GUARDIA NACIONAL AMERICANA BASADO EN NODOS CIS DESPLEGABLES

Los Nodos CIS Desplegables de la Guardia Nacional Norteamericana conforman el JCCSE y constan de tres partes.

- El primer componente es el Módulo Conjunto de Capacidades de Comunicaciones del Incidente (JISCC), que son elementos de comunicaciones que puedan desplegarse en vehículos CIS o rápidamente en cajas dentro de una tienda o en un pabellón deportivo. Consta de elementos de información, equipos radio y satélite, y un módulo para interconectar e integrar sistemas civiles (ACU). En los últimos tres años, la Guardia Nacional ha instalado módulos JISCC en los 50 estados de EE.UU.
- El segundo componente del JCCSE es el Centro de Control de Comunicaciones (JCCC), que surgió como una lección aprendida del huracán Katrina (2005). Después de la tormenta, aunque la Guardia Nacional había desplegado todas sus capacidades CIS en la región devastada, pronto se echó en falta un elemento que las coordinara y gestionara todos los enlaces.
- La tercera pieza del JCCSE es el Módulo de Intercambio de Información (JIEE). El JIEE es una Web basada en herramientas colaborativas que da a la Guardia Nacional la capacidad de conocer la situación real en los estados.

Esta nueva filosofía de enlace consiste en llevar el nodo hasta las inmediaciones de la zona de operaciones, constituyéndose en un concentrador (HUB) de comunicaciones. Allí se ofrece al resto de unidades que van a trabajar en esa zona del territorio y permitirles que se puedan unir a sus cadenas de mando. Estos nodos integran sensores de diferente índole, sistemas de armas capaces de cubrir las zonas de acción y sistema de seguimiento y localización de vehículos y fuerzas propias.

Por otro lado la mayor movilidad en el campo de batalla, exige proporcionar la capacidad de ejercer la dirección de las operaciones en movimiento, llegando cada vez a escalones más bajos. Es decir, además de usar elementos desplegables, se exige que enlacen en movimiento.

La "*raison d´être*" de estos nuevos nodos desplegables es el satélite. Este elemento es el que permite una total independencia de las redes de telecomunicaciones terrenas, existan, no existan o hayan sido destruidas.

En ocasiones los Puestos de Mando Avanzados (PMA) de las organizaciones de socorro sin sistemas satelitales se ven obligados a desplegar a kilómetros de distancia de la emergencia cuando ésta se produce fuera de núcleos urbanos, o cuando ocurre en zonas de orografía complicada, debiendo buscar zonas donde puedan recibir la señal de sus redes de telecomunicaciones privadas (TETRA, TETRAPOL, etc.), o al menos de telefonía móvil. Por suerte en nuestro país ya existen muchas organizaciones que se han unido a la filosofía del Nodo TIC Desplegable[17], incorporando sistemas basados en satélite a sus PMA.

17. Nodo TIC Desplegable: Nodo de las Tecnologías de la Información y Telecomunicaciones Desplegable de una organización civil de emergencias.

Uno de los grandes aciertos a la hora de constituir la **Unidad Militar de Emergencias** en España, fue apostar por aplicar las nuevas ideas procedentes del concepto de campo de batalla vacío y hacer realidad unos Nodos CIS Desplegables, que en combinación con otros Nodos CIS fijos, constituyen el sistema nervioso del Mando y Control de la unidad.

A nivel internacional puede servirnos como referente la **Guardia Nacional de Estados Unidos.** Esta fuerza es la primera encargada de auxiliar a los estados en caso de grandes catástrofes y posee igualmente capacidades CIS desplegables.

La experiencia adquirida en dos grandes desgracias como fueron los atentados del 11-S y el paso del huracán Katryna, el Jefe de la Guardia Nacional propuso crear un sistema de comunicaciones en todo el territorio continental norteamericano sobre el que sustentar el mando y control en las grandes emergencias. El sistema se pasa a denominar **JCCSE** (Joint Connus Communications Support Environment Concept for Joint C4) y se diseñó para integrar redes diferentes: redes de telecomunicaciones fijas del Departamento de Defensa, redes de organismos civiles de socorro; y redes desplegables, fundamentalmente las suministradas por los Nodos CIS Desplegables de las unidades de transmisiones de la Guardia Nacional.

SOLUCIONES GENÉRICAS

La dirección de las emergencias se realiza en un entorno complejo en el que es necesario disponer, en tiempo y lugar oportunos, de la información adecuada para poder tomar decisiones. Las **soluciones** que estas organizaciones han venido dando a "**su problema de enlace**" se suelen repetir en los sistemas de forma sistemática. Analicémoslas.

- **La diversidad de medios** para alcanzar la complementariedad. Se obtiene usando equipos de distinta naturaleza para combinar las ventajas de cada uno de ellos y reducir sus inconvenientes. A modo de ejemplo puede servir que en los Centros de Coordinación, existen tanto líneas telefónicas fijas, como troncales de telefonía móvil, o líneas ADSL y RDSI para efectuar videoconferencias.
- **La redundancia de vías y circuitos** entre usuarios potenciales. Se obtiene diseñando un sistema que permita unir transmisor y receptor por múltiples y diferentes caminos. Por ejemplo el enlace entre un Centro de Coordinación de Operaciones Integrado (CECOPI), y un Puesto de Mando Avanzado (PMA) se suele materializar por un enlace satélite, otro de telefonía móvil y además una red radio trunking, de tal manera que será más difícil que todo falle a la vez.
- **La particularización de medios** a la especificidad de la misión. La encontraremos en el tipo de equipamiento con el que se tendrán que dotar determinadas organizaciones para llevar a cabo la misión. Los equipos radio de un grupo de buceadores se diferenciarán sustancialmente de uno de rescate en montaña.
- **La reducción de la dependencia de la infraestructura de telecomunicaciones terrestre** se alcanzará haciendo uso de **satélites portátiles**, cuando la economía lo permita, o simplemente mediante el uso de **radios**.

A pocos debería sorprender cuando digamos que precisamente **esas mismas soluciones** son las que desde hace más de un siglo se han ido incorporando en los sistemas de transmisiones utilizados por las Fuerzas Armadas de todo el mundo, llegando a ser el **signo distintivo de los Sistemas Militares de Telecomunicaciones e Información (CIS)**.

La transferencia de tecnologías y procedimientos entre la milicia y el mundo civil ha sido bidireccional a lo largo de la historia. En las **épocas de paz** es la industria civil la que en mayor medida impulsa este intercambio de conocimiento. Los **tiempos de conflicto,** incluyendo periodos previos y posteriores a su desenlace, siempre fueron momentos en los que el mundo militar marcó su preponderancia. A la Primera Guerra Mundial se la conoció como la "guerra de los ingenieros", mientras que a la Segunda Guerra Mundial se la describió la "guerra de los científicos".

Hoy día sigue activo este canal de transferencia de conocimientos entre la sociedad civil y la militar. Los terrenos que pisan unos y otros no tienen propiedad exclusiva, aunque a tenor de lo expuesto estamos convencidos de la **importancia del papel desempeñado por los ingenieros militares** en la aportación de soluciones al mundo civil en su conjunto, y en particular al de las telecomunicaciones en las emergencias.

DISEÑO DE UN SISTEMA

Vistas las soluciones que tanto militares como civiles ofrecen a los gestores de las emergencias, ahora quedaría explicar cómo diseñar un sistema completo. Como la pretensión de este libro queda muy lejos de impartir doctrina, y mucho menos en la rama de ingeniería de sistemas, únicamente **nos vamos a permitir**

unos consejos para aquel lector que le pudiera haber tocado en suerte tener que afrontar el diseño de un sistema completo, sin por supuesto abordar las etapas y tareas propias de un "diseño formal".

ARQUITECTURAS

En la Organización del Tratado del Atlántico Norte (OTAN), su agencia NCI (NATO Communications and Information Agency) es la responsable del diseño de sistemas que se ponen al servicio de la Alianza. Desde hace muchos años comenzó a aplicar en sus desarrollos el llamado diseño por arquitecturas[18].

El diseño de cualquier sistema arranca con la redacción de una **Arquitectura de Referencia Global** que describe las especificaciones y soluciones técnicas de cada componente o subsistema. A continuación se acometen las **Arquitecturas Objetivo** específicas de cada sistema componente. Estas Arquitecturas recogerán la composición y características de los sistemas con el suficiente **detalle técnico, logístico y operativo** como para que se puedan redactar los **Pliegos de Prescripciones Técnicas** que se utilizarán para realizar los procesos de contratación correspondientes.

Siendo muy simplista, y tratando de no caer en lo obvio, podemos decir que estas arquitecturas son una herramienta muy útil para establecer **planes directores** que permitan acometer la vida de un sistema desde su diseño, pasando por su puesta en funcionamiento y actualización, hasta acabar con su retirada del mercado, **sin caer en "olvidos imperdonables"** que pudieran hacer fracasar o mal funcionar el sistema.

Las arquitecturas se componen de varios subapartados[19], de los cuales solo vamos a destacar los tres más importantes a nuestro entender:

- La **Vista Operativa** es una descripción de un sistema específico en función de las necesidades operativas que marquen los usuarios finales. Es aquí donde el que va a dirigir las operaciones tiene que decirnos como quiere hacerlo. Es un documento en el cual los responsables de una organización (ya sea una empresa, una institución o una Organización No Gubernamental) establecen los objetivos que desean cumplir y estipulan los pasos a seguir. Es lo que se conoce como **Concepto Operativo.**
- La **Vista de Sistema** consiste en desglosar el sistema en componentes o que facilitarán unos servicios para cumplir lo que ha pedido el usuario mediante los requisitos especificados en la vista operativa o Concepto Operativo.
- La **Vista Técnica,** finalmente es una descripción del sistema global en función de los estándares, tecnologías y protocolos existentes en el mercado para cada uno de los componentes identificados en la Vista de Sistema, de tal manera que satisfagan los requisitos operativos y proporcionen los servicios descritos en la Vista de Sistema. Es en este punto donde tendremos que tener en cuenta las "**soluciones**" que hemos visto se dan para los sistemas de enlace en emergencias

En definitiva se trata de hacer un trabajo sistemático, arduo o puede que incluso pesado, pero que permite obtener soluciones completas sin lagunas en el diseño, con periodo de vigencia de al menos diez años.

CONCEPTO OPERATIVO

Aunque no es una garantía absoluta, desde nuestro punto de vista lo

18. NATO C3 System Architecture Framework (NAF).

19. Partes de una Arquitectura

- Introducción
- Vista Operativa
- Vista de Sistema
- Vista Técnica
- Modelo de Datos
- Concepto de Seguridad
- Vista Funcional de Gestión de las Capacidades CIS

primordial para acercarnos al éxito es contar con un buen **Concepto Operativo.** Debe quedarnos claro que éste no nos corresponde a nosotros los Responsables TIC. Es más, debemos negarnos a realizarlo porque es al "**operativo" al que corresponde decidir cómo quiere dirigir la emergencia.**

El concepto operativo recogerá el escenario en el que va a trabajar el sistema que estemos diseñando. Nada tendrá que ver un sistema para una aldea de 30 personas en los Picos de Europa, que el sistema que se use en una línea de metro de Barcelona. Son los llamados **condicionantes o requisitos operativos:** extensión de terreno, orografía, climatología, número de usuarios, etc.

En más ocasiones de las que a priori pudiéramos pensar, nos encontraremos que el jefe **"no sabe lo que quiere..."**. En ese caso nos veremos obligados a echarles una mano e "iluminarles". Tendremos que dirigirles. Es **importante que definan la cadena de mando** o jerárquica de la organización, dependencias organizativas y funcionales. ¿Cuáles son sus posibles **colaterales**? ¿Quiénes son sus **elementos o peones de maniobra?**

En cualquier caso reiteramos que **el concepto operativo** de uso de un sistema que va a servir para ejercer el mando, la dirección o la coordinación (hablaremos de esta disyuntiva en el capítulo 12) **no debe ser redactado ni por el personal TIC/CIS de la organización ni mucho menos por personal de empresas tecnológicas.** Los primeros porque, aunque tienen buenas intenciones, tratan de buscar en la técnica soluciones a requisitos operativos, que en muchas ocasiones complican en exceso los sistemas. Los segundos porque tienen intereses económicos y van a tratar de justificar, a martillazos si fuera necesario, el uso de un producto de su catálogo que rara vez se ajusta a lo requerido en el concepto operativo.

Tampoco debemos olvidar en nuestro diseño que **la tecnología se utiliza siempre en un contexto social y organizacional,** y el comportamiento humano es capital en el éxito o fracaso del sistema. Es decir la tecnología no puede examinarse en forma aislada a cómo se despliega.

Será muy extraño que en los tiempos que corren se nos presente la oportunidad de iniciar el diseño de un sistema partiendo de cero. Esto sería lo ideal, porque podríamos ser ortodoxos y aplicar la teoría (la de arquitecturas o cualquier otra) de una forma sistemática para obtener un buen resultado. Por desgracia **lo normal será recibir un sistema previamente establecido al que nos pedirán introducir mejoras.**

En este caso partimos de una situación de desventaja, porque lo primero que deberemos comprobar es **si permanece vigente el concepto operativo** con el que fue concebido el **sistema heredado**.

Vamos a intentar conceptos con un pequeño ejemplo.

EJEMPLO

Nos acabamos de convertir en el responsable TIC de una Policía Local, la cual utiliza un viejo sistema de radios analógicas unidas con la comisaria situada en el ayuntamiento. Imaginemos que el concepto operativo (vista operativa) que dio el alcalde, Don Manuel, hace 20 años fue el siguiente:

"La policía local durante sus patrullas por las calles del pueblo estará en condiciones de informarme de cualquier altercado o incidente de manera inmediata para que el consistorio pueda tomar medidas".

El pueblo tenía 3.000 habitantes y un término municipal de 40.000 metros cuadrados **(condicionantes operativos).**

En su día alguien decidió que la mejor forma de conseguir hacer lo que exigía el alcalde, con los condicionantes operativos existentes, era comprar un grupo de radios **(vista de sistema)** *para poder hablar con los policías (servicio de voz).*

Finalmente el concejal de fomento y tesorero decidió comprar 4 walkies y una estación base radio analógica **(vista técnica),** *que salía muy bien de precio y que se instaló en el ayuntamiento.*

Ahora estamos en el siglo XXI. El pueblo ha multiplicado por diez sus habitantes y por cuatro su área urbana, es decir han cambiado sustancialmente los requisitos operativos. El alcalde que acaba de llegar tras las últimas elecciones es un "friki" de las nuevas tecnologías. Lejos queda el concepto operativo de Don Manuel. "El Mechas", que así se hace llamar, ha decidido que quiere ver desde su despacho consistorial y en tiempo real, lo que acontece en cada una de las calles del pueblo. ***Éste es su concepto operativo...***

Como Responsables TIC del "Mechas", podemos imaginar que poco podremos hacer con el sistema heredado de radios analógicas para hacer frente a la nueva misión encomendada.

Es evidente que lo expuesto es una exageración, pero el trasfondo es real. Lo normal será que tengamos que hacer actualizaciones, mejoras o integrar nuevos servicios. **Nos encontraremos con otros problemas** como podrá ser el de encontrar tecnologías compatibles, problemas de interoperabilidad y por supuesto la resistencia al cambio de la organización y de las personas cuando les digamos que tienen que hacer el esfuerzo de aprenderse un nuevo equipo.

Principalmente si vamos a diseñar un sistema *ex novo* tendremos que tener también en cuenta en la fase de diseño cómo vamos a llevar a cabo **el desarrollo del sistema y la implantación del mismo.** Las prisas no suelen ser buenas en este tipo de tarea. En los últimos años se están poniendo de moda los **desarrollos y entregas de productos en "espiral".** Esto consiste en la entrega versiones operativas de menor a mayor capacidad. Cada nueva versión integra nuevas funcionalidades y servicios adicionales, permitiendo corregir defectos de las versiones primeras. Las empresas no suelen ser muy favorables a este tipo de desarrollos porque les obliga a un mayor esfuerzo que el que harían si los entregables fueran aislados y sin relación entre ellos.

El **condicionante económico** está siempre presente. Nunca tendremos dinero suficiente para hacer lo que queremos, que recordamos debería ser lo que quiere la persona que definió el concepto operativo. Los costes no se limitan sólo a la **adquisición** del sistema. Se les debe sumar los de **instalación** y **formación** de usuarios (suelen estar incluidos en la adquisición), **mantenimiento** preventivo y correctivo y **actualizaciones** de componentes durante el ciclo de vida.

Nos resistimos a terminar este apartado sin un poco de **autocritica** hacia los Responsables TIC. Nos gusta la innovación y a veces nos obstinamos en implementar servicios y herramientas tecnológicas "curiosas" que queremos hacer pasar por útiles. Nos obstinamos tanto que acabamos tratando de imponer su uso al operativo. Si el operativo dice que quiere una radio para hablar... no debemos intentar convencerle de que es mejor un sistema de video full motion, con sistemas de seguimiento biométricos y localizador GPS de los intervinientes. Podemos hacer propuestas de mejoras dentro del presupuesto económico, que se adapten a lo que quiere el jefe en su concepto operativo, pero no debemos tratar de darle la vuelta como a un calcetín.

En más de una ocasión hemos visto un "maravilloso" sistema de telecomunicaciones ya construido y entregado sobre el que se ha escrito un **concepto operativo *a posteriori*.**

Por último con el nuevo sistema entregado o actualizado por la empresa, y con el concepto operativo, procederemos a redactar el **procedimiento de uso y mantenimiento del sistem**a para que el usuario y los técnicos de mantenimiento saquen el máximo partido.

CARACTERÍSTICAS PRINCIPALES DE NUESTRO SISTEMA

Una vez vistas las soluciones genéricas que los profesionales del mundo de las emergencias han dado a sus sistemas de enlace, y las pautas a seguir para lograr un diseño correcto, nos resta añadir las características que deben cumplir las infraestructuras que soporten nuestro sistema de enlace.

El **nivel de exigencia** que nos autoimpondremos vendrá marcado tanto por el **concepto operativo** como por el **presupuesto disponible**. Por lo tanto nuestro objetivo estará focalizado en el desarrollo de un sistema avanzado, que debiera estar **basado en la última tecnología contrastada**[20] que sea más adecuada a nuestros propósitos, y que permita una implantación adaptada a las necesidades de los usuarios de nuestra organización. Se debe huir del "esnobismo tecnológico".

Por tanto, un **sistema de enlace** para apoyar la gestión de las emergencias debería contar con las siguientes características:

- **Resistente**
  Debe ser lo más robusto posible y capaz de resistir el impacto de las catástrofes.

- **Telecomunicaciones "transparentes"**
  El medio de transporte de la información requerida por los usuarios del sistema, bien basada en voz, bien en datos, debe ser transparente para los éstos. Lo ideal como hemos visto es la duplicidad de medios y de

20. Notar que hemos dicho que nuestro sistema se debe basar en la última tecnología contrastada, en lugar de la tecnología más moderna. Las inversiones económicas en las TIC, sobre todo cuando son cuantiosas, deben hacerse sobre seguro.

vías de comunicación entre localizaciones, por lo tanto lo más recomendable seria que usara automáticamente el medio que esté disponible, sin intervención de las personas.

- **Redundante**

  Deberá ser capaz de ofrecer enlaces redundantes y proveer trayectos alternativos para el encaminamiento del tráfico de la red durante los periodos de congestión o bien en caso de fallo de alguna de las rutas.

- **Autonomía energética**

  Los equipos que integran el sistema deben estar preparados para funcionar con equipos de energía auxiliares o con baterías en caso de fallo de la fuente de alimentación principal.

- **Fiabilidad/disponibilidad**

  Nuestro sistema debe estar disponible en todo momento, 24 horas al día, 365 días al año. Para que nuestro sistema sea útil debe ser fiable y los servicios que por él discurran deben establecerse de manera sólida.

- **Tolerancia a fallos**

  Debe ser capaz de funcionar incluso a pesar de que puedan fallar algunos de sus componentes. Para ello será necesario disponer de redundancia en los componentes críticos.

- **Priorizable**

  Se debe contar con mecanismos para establecer prioridades entre usuarios cuando la capacidad de nuestro sistema esté completa. De esta manera se podría dar preferencias a ciertas comunicaciones que por sus características puedan imponerse a otras de menor importancia.

- **Escalabilidad**

  Nuestro sistema debe poder ser utilizado de manera progresiva, y poder crecer o decrecer de acuerdo a las necesidades.

- **Simplicidad de uso**

  Los equipos sencillos tienen la ventaja de ser más fáciles de instalar, mantener y usar.

- **Independencia máxima de las infraestructuras fijas**

  Sin ánimo de generalizar, es importante que nuestro sistema sea lo menos dependiente posible de la infraestructura terrena. Habrá sistemas que no lo puedan ser por propio diseño. En este caso habrá que fortalecerlos para minimizar el riesgo de que quede fuera de servicio mediante la duplicación de vías y circuitos, o la instalación de equipamientos duplicados.

- **Interoperabilidad**

  Debe ser capaz de trabajar con las organizaciones habituales con las que tenemos que llevar a cabo nuestra misión, por lo que se buscarán estándares o tecnologías conocidas que permitan su fácil integración con aplicaciones de otros organismos de protección civil, sanitarios, etc.

- **Movilidad adaptada a las necesidades**

  El concepto operativo debe habernos indicado los escenarios de actuación más probables. Para que un equipo resulte manejable, debe ser ante todo de fácil transporte hasta la zona dónde se ha producido la catástrofe. Otra de las particularidades requeridas es que los equipos de comunicaciones funcionen sin cables y ofrezcan libertad de movilidad a las personas.

- **Seguridad**

  El tipo de información sensible que circulará por nuestro sistema hace recomendable dotarlo de algún nivel de seguridad. Aunque lo más sensato es que tanto los datos como las comunicaciones tengan la máxima confidencialidad, lo cierto es que nos adaptaremos una vez más al concepto operativo y al recurso económico.

- **Ergonomía**

  Será interesante prestar atención a los equipos de usuario, su diseño y ergonomía, que permitan una operación eficaz, cómoda y sin riesgos para los usuarios.

CAPÍTULO 4

DISTINTOS MEDIOS DE ENLACE PARA CADA FASE DE LA EMERGENCIA

La ciencia y la tecnología, incluidas las de la Información y las Comunicaciones (TIC), aportan un número cada vez mayor de medios para **determinar la presencia de peligros** y facilitar la administración de los mismos. **La necesidad de comunicarse es inherente a una situación de emergencia:** por parte de los afectados con los servicios de emergencia; entre los servicios de emergencia para dar una respuesta coordinada; entre los propios damnificados; y, en situaciones que van más allá de la emergencia personal, donde las comunicaciones son un factor clave para restaurar cuanto antes la deseada normalidad.

En caso de emergencias y catástrofes **el enlace cumple un rol preponderante**. La robustez de los sistemas de telecomunicaciones e información públicos en un país dependerá, quedando aparte factores de desarrollo económico y social, del grado de colaboración de todos los participantes. Es decir, autoridades, operadores públicos, aportación académica y empresas tecnológicas. Otros sistemas como los de los cuerpos policiales, de protección civil, sanitarios, fuerzas armadas deberían ser ya **resistentes a las calamidades públicas desde la misma concepción de los mismos.**

Durante los momentos previos, en la predicción, en la prevención y en la alerta temprana **las TIC** son fundamentales para salvar vidas humanas, sobre todo en desastres naturales. Las nuevas tecnologías también están presentes en los

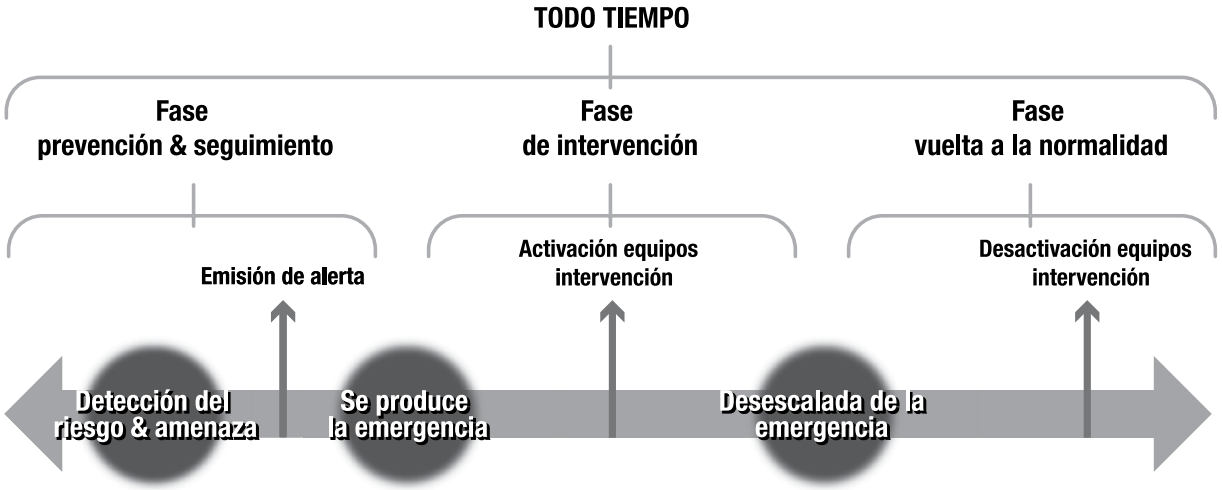
instantes durante los que se desencadena la emergencia y en los posteriores, en los que los afectados sienten la necesidad imperiosa de contactar con sus allegados. Por último, Internet, las Redes Sociales y los SMS intervienen cada día con más fuerza en las donaciones económicas que los ciudadanos de a pie realizan para ayudar a la recuperación de las zonas afectadas.

FASES DE LA EMERGENCIA DESDE EL PUNTO DE VISTA DEL ENLACE

Son multitud los sistemas de telecomunicaciones que se utilizan continuamente, cada día, y otros tantos los que se usan únicamente en momentos concretos de una etapa de la emergencia. **La flecha** de la figura a la derecha representa el tiempo. Al período comprendido entre los extremos de la flecha le denominaremos período **"todo tiempo". La leyenda** sobre la flecha representa **tres hechos,** que a nuestro entender, marcan la transición entre las distintas fases en las que se puede dividir una emergencia desde el punto de vista del enlace.

- La primera fase la vamos a denominar **prevención y seguimiento.** El inicio de la fase no está determinado claramente, ya que el riesgo o amenaza existía con antelación aunque no se fuera consciente del mismo. Para nosotros el hecho de **detectar el riesgo** es el que va a marcar la entrada en consideración de los medios de telecomunicaciones, que como veremos llevará pareja la implementación de una serie de redes que nos permitirán, en el mejor de los casos, **emitir una alerta** previa a que se produzca la catástrofe. En ocasiones esta separación temporal no existe y la alerta se producirá instantes después de que la desgracia se haya producido.
- **La fase de intervención** está marcada por la aparición sobre el terreno de los equipos de intervención de las diferentes organizaciones encargadas de mitigar los daños producidos. En este punto destacaremos tanto el proceso de la activación hasta los locales donde están esperando las organizaciones, como los sistemas que utilizan dentro de la zona de la emergencia.
- Por último trataremos la **fase de vuelta a la normalidad,** en la que poco a poco las agencias de

MEDIOS DE ENLACE PARA CADA FASE DE LA EMERGENCIA



emergencias irán dejando paso a los órganos encargados de la reconstrucción, y que vendrá marcada por la desescalada del nivel de la emergencia.

Como veremos a continuación, el enlace es decisivo en todas las fases de la gestión de una catástrofe. En este apartado trataremos de poner el acento en **aquellos sistemas que son más preponderantes y que diferencian una etapa de otra.**

SISTEMAS USADOS "TODO TIEMPO"

No queremos ser pesados repitiendo cada dos páginas que las TIC están en todas partes, pero está claro que en el primer mundo hay muchos sistemas que son usados de manera cotidiana y que podrían prestar su servicio en una emergencia siempre y cuando no hubieran colapsado. Somos de la opinión que aunque no se pueden calificar de "sistemas puros de enlace en emergencias", tendrán un papel a desarrollar en determinados momentos. Hablaremos entonces de las redes de telecomunicaciones públicas, privadas, medios de comunicación pública y otros sistemas que participan.

REDES PÚBLICAS

Nos estamos refiriendo por ejemplo a las **redes públicas de telefonía fija y móvil,** u otras infraestructuras de comunicaciones alámbricas como redes de cable coaxial o de fibra óptica usadas como soporte físico de la televisión por cable o de las líneas de internet que estamos acostumbrados a usar en nuestros hogares. La Unión Internacional de Telecomunicaciones (ITU/UIT) hace una serie de **recomendaciones**[21] de medidas a adoptar en las redes públicas para garantizar su funcionamiento en caso de catástrofe.

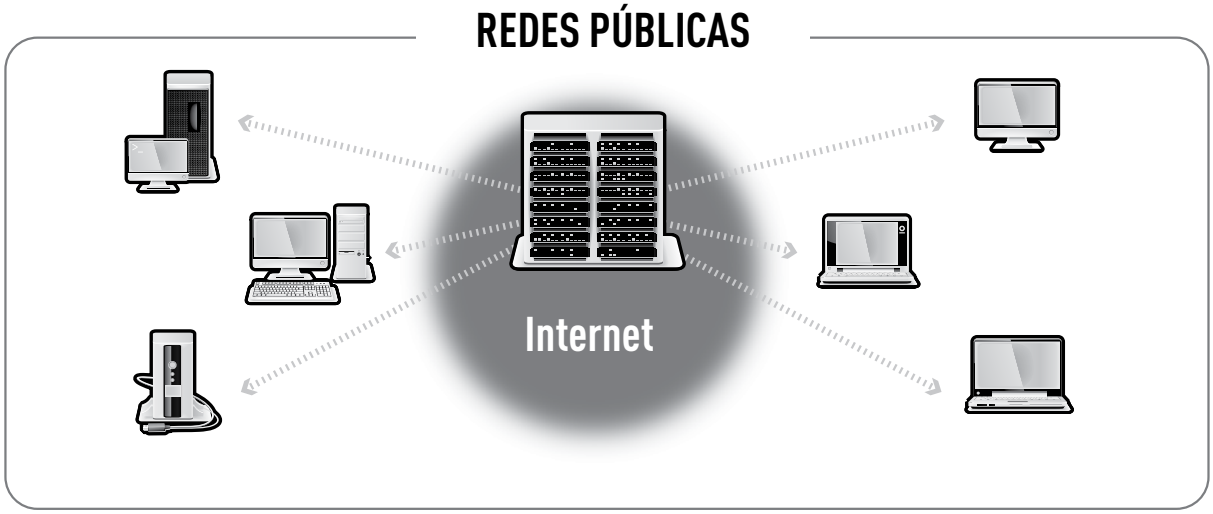
En nuestro país rápidamente se nos viene a la mente la red de **Telefónica S.A.** Pero por suerte no es la única. Vodafone, Orange... **JAZZTEL** instaló a lo largo de 2005 la primera red de nueva generación (Next Generation Network o NGN) de estas características en nuestro país. Este grupo empresarial apostó por crear su propia

21. Las dos más relevantes son:
    - RECOMENDACIÓN UIT-T E.106 – Plan internacional de preferencias en situaciones de emergencia para actuaciones frente a desastres
    - RECOMENDACIÓN UIT-T E.107 – Servicio de Telecomunicaciones en caso de Emergencia (STE) y marco de interconexión para la implantación nacional de STE

REDES PÚBLICAS

Una red pública es la red a la que tienen acceso los ciudadanos, aunque puede estar operada por empresas públicas o privadas. Cuando no está afectada por ningún incidente o avería permite realizar y recibir simultáneamente llamadas de entre el 5 y 10% de los abonados. Cuando la red telefónica Pública Conmutada (rtPC) sufre una avería, las pérdidas de comunicación son mayores que las del servicio telefónico ya que el mismo sistema soporta muchos otros servicios a parte de la telefonía. Suele tener mucha importancia para el usuario en una emergencia el llamado "bucle local", o último kilómetro que une el teléfono de nuestras casas con la central telefónica más próxima. Algunos operadores ofrecen acceso a sus centrales por medio de soluciones de "bucle local inalámbrico" (WLL, wireless local loop).

El cometido de los operadores de servicios de telecomunicaciones ya sean públicos o privados en situaciones de emergencia es controvertido. Aunque estas empresas buscan ganar dinero, cumplen también una responsabilidad social y deben procurar que sus redes presten apoyo a las organizaciones que tratan de que se atenúen sus consecuencias.



red de fibra óptica metropolitana y provincial en las principales ciudades, uniéndolas mediante una red troncal nacional (Backbone). Dicha red nacional está soportada sobre más de 20.000 kilómetros de fibra.

Sobre estas redes de operadores públicos es donde la UIT aboga por implementar el llamado **Servicio de Telecomunicaciones de Emergencia (ETS).** La implementación de un ETS es, por definición, una cuestión de competencia nacional, y no es obligatorio. Proporciona **telecomunicaciones prioritarias** a los usuarios autorizados en situaciones de catástrofe y emergencia. Esta prioridad versa en el acceso privilegiado a los recursos de las redes, aumentando por tanto la probabilidad de establecer enlaces de extremo a extremo. Por ejemplo el Gobierno Peruano decidió instalarlo quince días después del terremoto del 15 agosto de 2007, en el que tras el sismo hubo un corte global de comunicaciones en todo el país.

Podríamos seguir nombrando redes a nivel nacional como la **Red SARA** de la administración pública, o la **RedIRIS** que une las universidades y centros de investigación de todo el país, para acabar de constatar la existencia de un enorme número de redes dotadas de unas capacidades desorbitantes.

REDES PRIVADAS

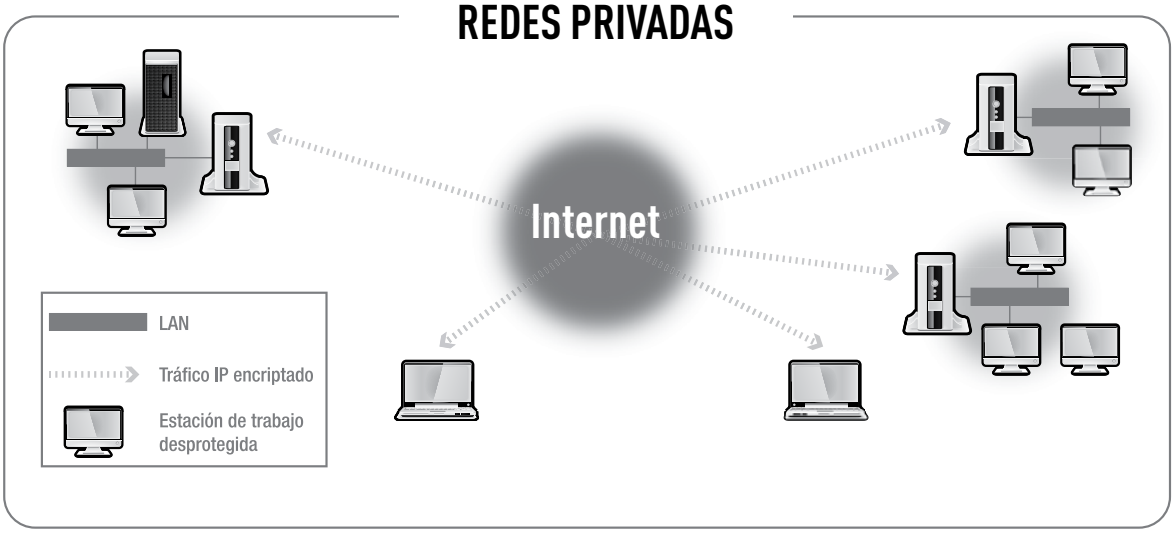
Ya hemos mencionado que determinadas organizaciones apuestan por crear sus propias redes para llevar sus cometidos en el día a día. Son las denominadas **redes privadas**. Éstas pueden ser de diferentes tipos: radio, telefonía, satélite, etc., y dan servicio a colectivos como cuerpos de policía, transportistas, sanitarios, taxistas, etc.

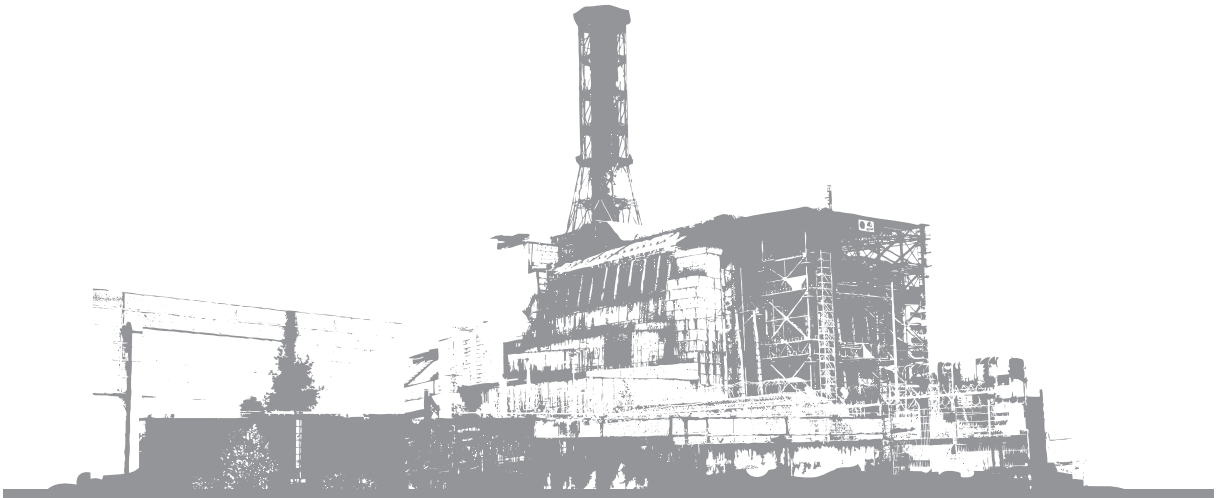
Pongamos como ejemplo de este tipo de redes la red RESCAT de tecnología trunking digital TETRA de la Generalitat de Catalunya o la red de comunicación TETRA de la Ertzaintza.

Las organizaciones no gubernamentales (ONG,s), nacionales e internacionales desempeñan una función clave en la prestación de ayuda en las operaciones. La Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna (IFRC), mantienen **sus**

REDES PRIVADAS

Estas redes se refieren a las infraestructuras de telecomunicaciones que han financiado y utilizan las organizaciones especializadas, como sanitarias, bomberos, policías, ambulancias, servicios públicos, protección civil, transporte, autoridades estatales, ministerios y Fuerzas Armadas. las empresas y el sector de las industria pueden también emplear estas redes. Por lo general, la red pertenece a los usuarios privados, quienes tarde o temprano pueden compartirla si se les requiere. es habitual que los usuarios gestionen su propia red privada y, en algunos casos, lo hacen los operadores públicos como un servicio a sus clientes.





ACCIDENTE NUCLEAR DE CHERNÓBIL

propias redes privadas de telecomunicaciones y apoyan a sus homólogos nacionales cuando los enlaces de telecomunicación normales sufren daños debido a una catástrofe. Un grupo nuevo e importante entre las ONG son las empresas comerciales, como Ericsson, que ponen a disposición los expertos de su sede y sus oficinas de muchos países para que colaboren en las operaciones de socorro tras una catástrofe.

A nivel internacional entre otras, podríamos hacer mención del **Comité Internacional de la Cruz Roja (CICR)**, dedicada a la aplicación de los convenios de Ginebra, que rigen el derecho humanitario en caso de conflicto, cuyas delegaciones están conectadas mediante su propia red privada de telecomunicaciones.

Las Fuerzas Armadas disponen de sus propias redes. Unas que utilizan recursos de operadores civiles y otra, la más importante, totalmente independiente de la infraestructura civil por motivos de seguridad. En España nos referimos al **Sistema de Telecomunicaciones Militares (STM),** que a su vez es un Subsistema de otro de mayor entidad llamado Sistema de Mando y Control Militar (SMCM)[22], y que constituye el nexo de unión e integración del resto de los subsistemas componentes (puestos de mando, información sensores), permitiendo la interconexión de otros sistemas de telecomunicaciones de OTAN y de países aliados.

MEDIOS DE COMUNICACIÓN PÚBLICA

Dentro de estos sistemas todo tiempo no podemos olvidar tampoco los **medios de comunicación pública, televisión y radio**[23] fundamentalmente, que aunque no sean sistemas de enlace pueden resultar una poderosa herramienta para transmitir mensajes o la llamada "propaganda blanda". Es decir las campañas de concienciación o de comunicación que por ejemplo realizan periódicamente el Ministerio del Interior a través de la Dirección General de Protección Civil o la Dirección General de Tráfico.

USO DE LOS MEDIOS DE COMUNICACIÓN PÚBLICA

El accidente de Chernóbil, acontecido en dicha ciudad de Ucrania el 26 de abril de 1986, fue el accidente nuclear más grave de la historia. Alcanzó el nivel 7 (el más alto) en la escala INES. De las lecciones que se extrajeron en aquella catástrofe se vio la necesidad de que la población cercana a las centrales nucleares pudiera ser avisada en caso de accidente grave. Independientemente de los condicionantes políticos imperantes en la época, si se hubieran empleados medios de información pública como radio o televisión para advertir de los peligros existentes, las consecuencias de aquel acontecimiento habrían sido sensiblemente menores. Hasta 2006 habían muerto entre 50.000 y 100.000 de los liquidadores que participaron en las tareas de minimizar las consecuencias del desastre, mientras que entre 540.000 y 900.000 quedaron inválidos.

22. El Sistema de Mando y Control Militar (SMCM) se compone del Subsistema de Telecomunicaciones Militares (STM) y del Subsistema de Información Militar (SIM).

23. Aunque son cosas diferentes, lo cierto es que la "revolución digital" en la radio y teledifusión han hecho converger ambos mundos, el de los Medios de Comunicación Pública (MEDIA) y el de las TIC.

OTROS SISTEMAS TODO TIEMPO

Los 112 de las diferentes Comunidades Autónomas a través de sus **portales web** están habituando a los ciudadanos a acceder a información sobre las emergencias y riesgos relevantes de su región. Es una forma de preparar a la ciudadanía a utilizar las nuevas tecnologías para estar informado ante la proximidad de una emergencia e influye positivamente en su respuesta durante y después del suceso.

Igualmente existen **sistemas de información** como los **meteorológicos**, o los de **navegación** de vehículos terrestres (los extendidos GPS de los automóviles) que usan como base los **sistemas de información geográfica (GIS)**.

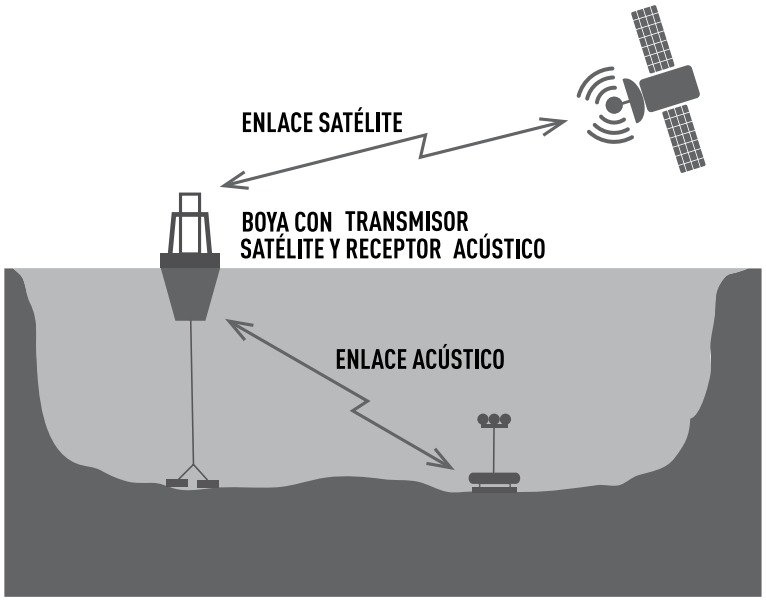
Sin duda estos sistemas ofrecen una serie de **capacidades no específicas del mundo de las emergencias** pero a las que recurriremos, ¡SEGURO!, en algún momento.

24. En algunos textos se las denomina redes de alerta temprana, pero nosotros no utilizaremos esta nomenclatura para no confundirlas con las redes generadoras de alerta que veremos a continuación.

RED DE SENSORES DE TSUNAMIS

A raíz de los últimos incidentes relacionados con tsunamis (Chile y Japón) la instalación de redes detectoras de posibles sismos ocurridos en el fondo de los océanos se han convertido en una prioridad para los gobiernos de los países en riesgo.

REDES DE ALERTA Y VIGILANCIA



SISTEMAS USADOS EN LA FASE DE PREVENCIÓN Y SEGUIMIENTO

Si partiéramos de una situación "ideal" ya en esta fase deberían existir una serie de medidas referidas a las TIC que tendrían que estar presentes. Un correcto diseño e implantación de redes públicas y privadas, una normativa legal precisa y exigente, unos planes de emergencias que contemplen el enlace en todas sus formas, y por qué no, una ciudadanía formada y educada en estas materias. El lector entiende perfectamente que este punto de partida no se va a dar prácticamente nunca, por lo que no vamos a fijar en una situación menos favorable para nuestros intereses.

La fase de prevención y seguimiento es vital para asegurar que las organizaciones y la sociedad civil estén preparadas para sobrellevar las emergencias. Las lecciones aprendidas de otras catástrofes demuestran que **la planificación es la clave para sobrevivir a los peores desastres.**

Si nos volvemos a fijar en la figura que representa las fases de la emergencia, podemos darnos cuenta que en algún momento, "alguien" detecta un riesgo o amenaza. Como es lógico y comprensible, este alguien decide prepararse y apuesta por hacer un seguimiento de la evolución de los peligros que acechan. Las TIC posibilitan la obtención de información relevante para la detección y prevención de emergencias. En este instante echa a andar esta fase.

Las catástrofes, al generarse de forma repentina, hacen que el factor tiempo sea fundamental. Tener un buen sistema de alerta y vigilancia para estos casos es el primer paso para dar una óptima respuesta evitando muchos de

los daños personales y materiales posteriores. Vamos a señalar tres aspectos importantes en los que los sistemas de telecomunicaciones e información intervienen. Las redes de vigilancia, las de alerta y el papel de algunas redes privadas que a su vez asumen tareas de vigilancia y alerta.

REDES DE VIGILANCIA: SENSORES

En primer lugar las tecnologías de la información y telecomunicaciones son sumamente útiles para observar y detectar a distancia fenómenos que tienen lugar en un punto potencialmente vulnerable o peligroso a través de las **redes de vigilancia**[24]. El principal elemento de estas redes son los llamados **sensores**. Antes de que ocurra la catástrofe, las TIC pueden transmitir información sobre la inminencia de la amenaza y están reconocidas mundialmente como elementos esenciales en la reducción efectiva de riesgos.

Una vez se obtiene la información los sensores se enlazan con los **centros de observación y control** dónde se produce el **análisis y evaluación de los datos.**

Las redes de vigilancia son casi infinitas... Desde una simple persona física, que mediante sus cinco sentidos detecta alguna anomalía en su entorno, pasando por redes detectoras de escapes radiológicos, y acabando por ejemplo con las redes de sensores de alerta de tsunamis. Como ya habrá pensado el lector **cada una de estas redes estará soportada por sus respectivas telecomunicaciones** que se dedicarán a transportar la información recogida por los sensores hasta el lugar de procesamiento de la información al centro de observación y control.

ALGUNOS EJEMPLOS ILUSTRATIVOS

El más básico puede ser el caso de una persona, por ejemplo un agente de la autoridad, que ve como se produce un robo, a través de sus sensores, en este caso su vista. Éste, valiéndose de su red de telecomunicaciones, su radio portátil, se lo comunicará a su centro de observación y control, es decir a su central de policía.

El caso más conocido puede que sea en nuestros días las catástrofes naturales en las que los **centros meteorológicos** nacionales e internacionales juegan un papel de alerta imprescindible. Los servicios meteorológicos y los de observación de la tierra permiten tener con el debido adelanto las previsiones meteorológicas y climáticas.

Compliquemos el patrón o modelo. Ahora son unos sensores de presión en una estación de bombeo que detectan una bajada del nivel de crudo en un oleoducto. El sistema transmite vía satélite dicha información al centro de observación y control (en este caso se llama centro de operaciones), dónde a través de la pantalla de un ordenador, y de modo automático, se informa a los operadores de servicio.

La complejidad del ejemplo la podemos aumentar tanto como queramos, pero al final los componentes son prácticamente los mismos expresados al principio de este apartado.

REDES GENERADORAS DE ALERTAS

La segunda etapa es la **emisión de las alertas** una vez se ha recibido una llamada o aviso proveniente de la red de vigilancia de sensores. Ahora **lo urgente es informar a las autoridades competentes del problema y llegado el caso a la población** de una forma rápida y clara que permita preparar las siguientes acciones.

Los radioaficionados suelen ser partícipes como veremos más adelante en el libro de la recepción y distribución de mensajes de alerta. Otro procedimiento de divulgar las alertas es a través de la radio o teledifusión.

El aviso también lo podría generar el propio centro de observación y control de la red de sensores explicada en el apartado anterior, aunque en un porcentaje cercano a cien, se ven implicadas las "**Agencias o Centros de Emergencias 112**" en Europa[25], o los centros 911 ó los 061 en los países anglosajones y latinoamericanos respectivamente.

112

25. En el caso de Europa, el teléfono único de emergencias emana de la normativa de la Unión Europea que promovió la implantación en todos los Estados Miembros de un único número para todas las emergencias, el 1-1-2, tomando como referente las experiencias de gestión integrada en los países nórdicos y en los Estados Unidos.

CENTROS 112

Los centros 112 europeos se han convertido en un "seguro de vida" para los ciudadanos del viejo continente, así como un elemento fundamental de interoperabilidad e integración de servicios de emergencias.

En Europa el modo más habitual de comunicar una situación de emergencia es mediante una llamada telefónica al 112, número unificado en la Unión Europea para el acceso a servicios de emergencia según directiva de 1991. Estos centros receptores de llamadas, a través de los enlaces habilitados, procederán a **avisar** a la población, organizaciones del mundo de las emergencias, de protección civil y asistencia sanitaria, cuerpos policiales, y responsables de la gestión de catástrofes en general.

Las llamadas al 112 se pueden hacer desde terminales fijos, móviles, o teléfonos públicos. Desde un terminal de telefonía móvil se puede llamar al 112 para conectarse al servicio de emergencias de forma gratuita incluso desde móviles bloqueados o sin tarjeta SIM, o incluso introduciendo 112 como PIN en un móvil que encendemos. Las redes de telecomunicaciones nacionales tienen el **deber de tratar la llamada con prioridad**, incluso en situaciones de congestión; y, en el caso de redes móviles, obligación de atender móviles en su área de cobertura aunque no sean clientes de la empresa propietaria de la estación-base.

Los 112 se suelen valer de centros localizados en edificaciones diseñadas ex profeso. Estas instalaciones cuentan con unas importantísimas infraestructuras de telecomunicaciones y plantas de energía auxiliares para garantizar su correcto funcionamiento todos los días del año. Están dotados de sistemas de información muy específicos que permiten la distribución de los avisos entre los medios de intervención disponibles. Es el denominado **despacho** o "***dispaching***" de los recursos, del cual hablaremos más extensamente en próximos capítulos.

La detección a tiempo de la proximidad de un desastre es poco eficaz si no va a acompañado de una rápida comunicación de la situación a la población afectada por lo que los 112 están equipados con **sistemas de aviso telefónico masivo a la población.** Emergencias 112 de la Comunidad de Madrid fue activado con motivo del incendio del edificio Windsor. En un momento dado, se necesitó avisar a la población en un radio de 500 metros, para que cerraran ventanas y bajaran persianas y así evitar la inhalación de gases tóxicos. El mensaje fue enviado a unos 10.000 abonados en menos de 2 horas.

Estas agencias 112, de valor incalculable por el servicio prestado a la sociedad, en muchas de las catástrofes **no sólo se limitan a recibir avisos y alertar a los cuerpos competentes,** sino que en muchos casos **incluso realizan la gestión del incidente** propiamente dicho.

Además suelen jugar un papel muy relevante en los Planes de Emergencia, sean interiores, exteriores, Territoriales, Específicos o Estatales.

Otros organismos expertos en campos muy concretos, como el **nuclear, las instalaciones ferroviarias, las portuarias, el de hidrocarburos, o el de la energía eléctrica** tienen sus **propios centros de recepción de alertas y de gestión de incidencias,** que aparte de la conexión con su centro 112 regional, lógicamente también estarán enlazadas con la autoridad competente de su sector o incluso del Gobierno de la nación, por la trascendencia de las incidencias en sus dominios de actuación.

PLANES DE EMERGENCIAS

Dentro del Sistema Nacional de Protección Civil, la Norma Básica de Protección Civil define los tipos de emergencias que, dadas sus características, son susceptibles de desarrollar un Plan especial de Protección Civil, entre los que se encuentran los siguientes:

- Plan especial de riesgo nuclear.
- Riesgo químico, incendios forestales.
- Inundaciones, sismos y transporte de mercancías peligrosas.

El resto de los riesgos están cubiertos, bien por los Planes territoriales de Comunidades Autónomas, o bien los Planes estatales de Protección Civil.

REDES PRIVADAS

Todas las organizaciones y agencias dedican una gran proporción de sus presupuestos a dotarse de los sistemas de comunicación necesarios. Estas redes privadas ya las hemos mencionado como medios TIC "todo tiempo". Sin embargo las volvemos a señalar en esta fase de la emergencia para que el lector, aparte de constatar su uso, advierta que **algunas de ellas forman parte de las redes de vigilancia o de alerta de su organización**.

SISTEMAS USADOS EN LA FASE DE INTERVENCIÓN

Para disminuir los efectos de las catástrofes es fundamental el transvase de información para adelantarse a la propia emergencia a través de las redes de vigilancia y alerta, pero igual de vital es el correcto empleo de los medios que permiten el enlace una vez que los daños ya se han producido. Organizaciones internacionales como la ITU han impulsado la redacción y promoción de acuerdos, como el ya mencionado Convenio de Tampere, que facilitan el uso de las TIC disminuyendo las barreras burocráticas que obstaculizaban la utilización de las telecomunicaciones. Las organizaciones de socorro **tratan de dotarse con los mejores sistemas** de enlace dentro de sus posibilidades **para atender a la fase de intervención.**

Una vez la emergencia se declara, numerosos servicios acudirán a la **llamada de los 112** o equivalentes. En caso de que estos **112 hayan dejado de funcionar** será una de las principales misiones a acometer: **su restablecimiento**. Aunque veremos en posteriores capítulos que están bien estudiados y dimensionados para resistir grandes impactos, no debemos olvidar la fuerza inusitada de la naturaleza. En este caso deberemos acudir a los **operadores de telecomunicaciones nacionales o a las Fuerzas Armadas** que suelen contar con potentes equipos que podrían restablecer los servicios en un tiempo reducido.

Dependiendo del nivel de la misma serán organizaciones locales o regionales, pudiendo llegar incluso a haber contribución de medios nacionales y de la comunidad internacional. Ahora es el momento de coordinar las actuaciones, lo que es una **tarea esencial pero nada fácil de materializa**r.

Los servicios de emergencia locales, regionales y nacionales, o los equipos de ayuda internacional suelen tener la posibilidad de utilizar sus propios sistemas de enlace en el desplazamiento hasta la zona de la emergencia. Otras veces únicamente lo podrán hacer cuando lleguen al lugar del siniestro y hayan completado la instalación de los equipos necesarios.

El problema al que nos enfrentaremos como Responsable TIC, es el de **identificar los canales de comunicación necesarios a establecer.** Si recordamos la definición del enlace expuesta en el

CENTRO NACIONAL DE COORDINACIÓN DE ALERTAS Y EMERGENCIAS DE SANIDAD Y CONSUMO

En 2004, se inauguró el Centro de Alertas y emergencias Sanitarias español, que permite un uso remoto y una conectividad completa tanto con las Comunidades Autónomas, con las redes de vigilancia ya existentes de organismos nacionales (Centro Nacional de Epidemiología, Agencia Española de Seguridad Alimentaria, etc.) así como con organismos internacionales de una forma prácticamente instantánea. Dispone de un potente sistema de información geográfica que facilita la gestión de alertas y recursos y permite la elaboración de mapas de riesgo con gran rapidez.

RED DE ALERTA

GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD Y CONSUMO

capítulo primero, es evidente que nuestra misión será la de enlazar distintos usuarios de nuestra organización, garantizando la materialización y uso de esas vías de telecomunicación imprescindibles.

En estos momentos la sensación inicial es que todos quieren estar enlazados con todos. Pero en un análisis más pausado podemos identificar diferentes **líneas de comunicación o canales**:

- Línea de Comunicación 1: entre centros generadores de alertas y elementos de guardia del servicio correspondiente.
- Línea de Comunicación 2: elementos intervinientes y sus sedes de procedencia.
- Línea de Comunicación 3: entre los intervinientes de la misma organización en la zona de la emergencia.
- Línea de Comunicación 4: entre intervinientes de distintas organizaciones en la zona de la emergencia.
- Línea de Comunicación 5: solicitud de asistencia internacional.
- Línea de Comunicación 6: entre las autoridades responsables de la gestión de la emergencia y la población.
- Línea de Comunicación 7: entre servicios de emergencia y la población.
- Línea de Comunicación 8: entre servicios de asistencia internacional y sus bases de procedencia

Veámoslas en detalle.

LÍNEA DE COMUNICACIÓN 1: Centros generadores de alertas ↔ Elementos de guardia del servicio correspondiente.

Los elementos operativos acuden al lugar de la catástrofe porque les llega el aviso o alerta a sus sedes[26] a través de las redes de alerta o vigilancia correspondiente. Es decir, los 112 o asimilados jugarán un papel protagonista en esta función.

La **comunicación de la orden de intervención al elemento operativo** llega normalmente a través de **canales preestablecidos**, vía voz o vía datos. Estos servicios al tener normalmente un ámbito local de actuación van a condicionar el tipo de sistema de telecomunicación que se vaya a utilizar.

En el caso de la **comunicación de la alerta vía fonía** (voz) suelen utilizarse líneas telefónicas públicas o privadas, o si la distancia lo permite, emisoras de radio.

El ejemplo más claro es la comunicación radio a una ambulancia de un servicio sanitario que acuda a un atropello en vía pública. Podemos adornarlo y complicar tecnológicamente tanto como queramos (recepción de datos vía PDA, videollamadas, etc.). En capítulos posteriores valoraremos el impacto de la tecnología en los procedimientos operativos, pero de momento nos conformaremos con señalar los aspectos más básicos y aclaratorios.

Los avances tecnológicos apuntan una nueva tendencia. Ahora los **centros generadores de alertas y los parques donde se concentran el personal interviniente** a la espera de ser activados durante sus guardias, se unen **mediante terminales de datos (ordenadores)** que se sitúan en sendos emplazamientos.

En todas las regiones, el enlace entre los 112 y los servicios de intervención suelen estar garantizado por el uso simultáneo de diferentes sistemas aparte del enlace a través de sistemas informáticos; por ejemplo con radio o teléfono.

LÍNEA DE COMUNICACIÓN 2: Elementos intervinientes ↔ sedes de procedencia.

El **flujo de información** entre estos componentes será muy intenso, tanto en el transcurso del **recorrido hasta llegar al lugar de la emergencia, como en la misma zona del siniestro.**

Tengamos en cuenta que la **velocidad de respuesta prima sobre la cantidad de información inicial sobre el siniestro.** Por lo tanto, serán las sedes de procedencia las que irán retransmitiendo datos adicionales sobre el evento a los equipos intervinientes por "el camino", con el fin de que cuando lleguen a la zona, lo hagan con el mayor conocimiento de la situación, y así facilitar su actuación.

Amén de otros condicionantes (económicos culturales, etc.), la **orografía** y la **distancia** entre el centro de procedencia del servicio y el lugar del incidente marcarán el medio de telecomunicaciones a utilizar. Ilustremos este apartado con varios ejemplos.

Si pensamos en un **servicio municipal** (ambulancias, bomberos...), que acude a un incidente de su comunidad, la comunicación más común será **vía radio**[27], aunque ya existen algunas policías, como por ejemplo la del municipio madrileño de Alcobendas, que basan su red en **telefonía móvil.** El condicionante de la orografía estará siempre presente. Lo normal será contar con una cobertura radio o de telefonía móvil preestablecida y conocida por los servicios de emergencia.

26. Dependiendo del tipo de organismo, estas sedes, que denominaremos "**sedes de procedencia**", reciben un nombre u otro. Algunos ejemplos pueden ser: parques, puestos de mando, centros de coordinación, base de operaciones, cuarteles, comisarias, etc.

Ya hemos mencionado estas redes en el apartado "Medios Todo Tiempo" y en la fase de "Prevención y Seguimiento".

Los avances tecnológicos han llevado, por un lado, a la universalización de las comunicaciones portátiles en forma de redes telefónicas públicas y, por otro, a la sofisticación de las soluciones radio para profesionales.

Podían parecer innecesarias **redes privadas dedicadas a las emergencias** en un contexto en el que las redes de comunicaciones móviles de acceso público cubren amplias zonas del territorio con garantías de seguridad y disponibilidad.

Sin embargo sabemos cómo en una situación de emergencia que afecta a las redes de telecomunicación públicas y por lo tanto los beneficios de **disponer de una red alternativa de alta disponibilidad y seguridad,** empiezan a hacerse evidentes.

Un correcto diseño e instalación de una red privada lleva implícito el **estudio detallado de cobertura** por parte de las empresas instaladoras, por lo que las zonas de sombra (sin cobertura) remanentes serán mínimas, y perfectamente conocidas por los usuarios del servicio.

Esto se conseguirá instalando cuantos **repetidores**[28] radio se necesiten para cubrir el área de actuación o pidiendo a los operadores de telefonía que instalen un número suficiente de **estaciones-base**[29] de telefonía. Por supuesto que se deberá tener muy presente el número de usuarios a los que dar servicio. Nótese que estamos hablando de medios en gran parte soportados por **infraestructura terrestre,** y que por tanto son vulnerables a una caída de servicios en determinadas circunstancias.

Sigamos con los ejemplos. Ahora el **equipo de intervención se desplaza a cientos o miles de kilómetros** de su sede de procedencia. Estaríamos hablando de una intervención de ámbito regional, nacional o incluso internacional.

Imaginemos que por ejemplo los Bomberos del Ayuntamiento de Murcia deciden acudir a una emergencia que ocurre en China. En este caso es de suponer que los sistemas radio habituales utilizados en este ayuntamiento no estarán preparados para cubrir una emergencia de estas características.

Veamos entonces que otras opciones tendríamos para **enlazar elementos intervinientes con sedes de procedencia muy lejanas**[30].

- Por supuesto que el **enlace telefónico** lo tendremos siempre presente. Algunas organizaciones buscan la sencillez y se decantan por el uso de la telefonía civil fija y móvil para coordinar actuaciones de intervinientes y sedes.

  Desde nuestro punto de vista es un planteamiento discutible por las razones ligadas a la vulnerabilidad de las infraestructuras terrenas. Sin embargo, para organizaciones con pocos recursos, podría ser una solución aceptable transitoriamente, hasta la llegada del momento que permita la compra de medios más profesionalizados.
- Hasta finales de los años ochenta la respuesta hubiera sido inmediata. Enlace Radio, y siendo más concreto hubiéramos dicho **enlace radio HF.** En el capitulo siguiente veremos alguna nociones de los soportes radioeléctricos y de los terminales estaciones radio y radioteléfonos.

  Vamos a ver unas **breves nociones de radio.** En primer

27. A grandes rasgos en Europa existen los siguientes tipos de redes radio:
    - Redes radio analógicas: suelen precisar repetidores por su limitada cobertura.
    - Redes radio trunking analógicas: usadas en grandes poblaciones, donde la misma red es utilizada por muchos usuarios. Consta también de repetidores y decenas de canales.
    - Redes radio trunking digitales: dos son las tecnologías preponderantes TETRA y TETRAPOL. Son similares a las anteriores pero con las ventajas propias de los sistemas digitales mucho más modernos y con más servicios.
28. Repetidor: dispositivo que recibe una señal y la retransmite a una potencia superior con respecto al nivel de la recepción, de tal modo que se puedan cubrir distancias más amplias.
29. Estación-base: equipamiento de filosofía similar de funcionamiento a un repetidor de radio, que proporciona cobertura de telefonía móvil a una zona próxima formando la denominada célula de cobertura.
30. En el capítulo 14 se explica un ejemplo de misión internacional y los enlaces que lleva aparejada.

lugar podremos usar diferentes bandas de trabajo. Los **enlaces HF** permiten hablar entre distancias que van de cientos de metros a miles de kilómetros. El único "problema" que tiene este procedimiento de enlace es que el operador del equipo debe saber de **propagación** y tener nociones de **antenas** para sacarle un rendimiento mínimo.

Los **enlaces HF no pasan su mejor época** debido a dos causas principales. La primera es la complejidad de uso en relación a la baja calidad del enlace proporcionado; y la segunda es el abaratamiento de los sistemas portátiles satélite que permiten unos enlaces de calidad similar a la proporcionada por la telefonía, y que sobre todo no necesitan ningún tipo de especialización para su uso.

La principal ventaja con respecto a sus competidores, lo terminales satélites tipo IRIDIUM, Inmarsat, GlobalStar o Thuraya, es que **el "HF" es gratis.** Sólo se paga el terminal, siendo su **uso discrecional.**

- Se podría plantear el uso de **redes radio de trunking** pues es el sistema más empleado entre las organizaciones de emergencia. Sin embargo su aplicación como ya hemos dicho se suele restringir a las zonas normales de responsabilidad que están previamente "malladas" y cubiertas con las estaciones bases necesarias.

En cualquier caso en estos sistemas apenas existen redes transnacionales, por lo que en una intervención internacional, no suelen ser utilizados en **modo red**[31], aunque como veremos en el siguiente apartado su uso es posible en otros modos.

- Y por supuesto no podemos olvidarnos de los **terminales satélites portátiles**. Como hemos mencionado con anterioridad han alcanzado una **posición de liderazgo** en los medios de enlace utilizados en las emergencias internacionales.

  Su principal ventaja es una garantía muy alta de obtener el enlace independientemente del estado de la infraestructura terrena y del estado de la red eléctrica.

- Acabamos este apartado mencionando la opción de acudir a la **transmisión de video**, sea en formato **videoconferencia**[32], o en formato **transmisión de imágenes de la catástrofe en tiempo real** entre centro de control y unidades intervinientes.

  Son soluciones posibles y utilizadas cada vez con mayor asiduidad, pero que suponen un gran esfuerzo para el personal TIC, y sobre todo muy demandantes para las capacidades de los sistemas empleados para su materialización.

LÍNEA DE COMUNICACIÓN 3: Entre intervinientes de la misma organización en la zona de la emergencia.

Una vez las dotaciones de los diferentes organismos relacionados con las emergencias llegan a la zona de la emergencia, deben **coordinar su intervención *in situ***.

El contacto personal y las órdenes transmitidas **a la voz** deberán ser complementados con otros medios de telecomunicaciones que permitan una correcta sincronización para reducir o mitigar los daños, y recuperar y salvaguardar cuántas vidas sea posible.

Toda organización contará normalmente con los medios adecuados y adaptados a los escenarios más probables de trabajo.

Los cuerpos policiales, de protección civil o sanitarios suelen estar dotados de **equipos radio portátiles y vehiculares** que permiten por un lado estar conectado con sus sedes origen a través del modo red tal y como hemos visto en el apartado anterior. Es básico subrayar el hecho de que este mismo equipo les va a permitir enlazar con los propios intervinientes, bien entrado en la red, o bien en **modo directo.**

El **enlace a través de telefonía móvil** suele ser muy complicado en los primeros momentos, ya que como hemos explicado aunque las instalaciones de telefonía hubieran sobrevivido a la catástrofe, la gran acumulación de personas en la zona tratando de acceder a los servicios acaba provocando la caída del sistema por saturación del mismo.

Tanto para redes radio trunking, como para telefonía móvil existe la posibilidad de instalar repetidores móviles o estaciones-base auxiliares para **restaurar la cobertura** en zonas donde se ha perdido. Estas no suelen estar accesibles inmediatamente ya que normalmente están operadas por operadores civiles cuya participación se debe solicitar *ex profeso*.

En muchas ocasiones, cuando las cosas pintan mal, son los mismos operadores públicos de telefonía los que despliegan medios sin que medie solicitud. Por ejemplo en los terribles incendios que asolaron la provincia

31. **Modo red** se refiere a enlazar dos terminales pasando la comunicación por al menos una estación base o repetidor terrestre. Si no pasa por infraestructura terrestre y enlazan directamente entre sí los terminales portátiles se llama entonces **modo directo.**

32. La videoconferencia es a menudo conocida por las siglas "VTC", siglas resultado de la expresión inglesa que la representa, ***Video Teleconferencing.***

de Valencia en el mes de julio de 2012, Telefónica instaló una estación desplegable de telefonía móvil en Cortes de Pallás para facilitar las operaciones del Centro de Coordinación de Operaciones Integrado (CECOPI) que se encontraba constituido en esa zona.

Sin embargo existen organizaciones, como ocurre en España con el caso de la **Unidad Militar de Emergencias,** que con las primeras unidades de intervención envían un vehículo de transmisiones dotado de la capacidad de crear un **"burbuja" de cobertura diferente a la proporcionada por las estaciones-base de la red SIRDEE** (red en la que habitualmente trabajan), para asegurar la operatividad y la seguridad de su personal en caso de trabajar en lugar sin cobertura o si se produce un fallo de la infraestructura terrestre.

En determinadas ocasiones los equipos de rescate más especializados deberán contar con equipos **muy específicos** de comunicaciones para poder ejecutar sus misiones.

Nos estamos refiriendo por ejemplo a equipos de rescate urbano (USAR-Urban Search and Rescue), **equipos de subsuelo o de espeleosocorro,** que deberán recurrir a equipos que permitan el enlace a través de los escombros, túneles o cuevas respectivamente, y que aseguren la comunicación con la superficie. O a **equipos de buceadores** que deberán contar con equipos específicos para enlazar con las embarcaciones. En un capítulo 15 ampliaremos este tema de enlaces especiales.

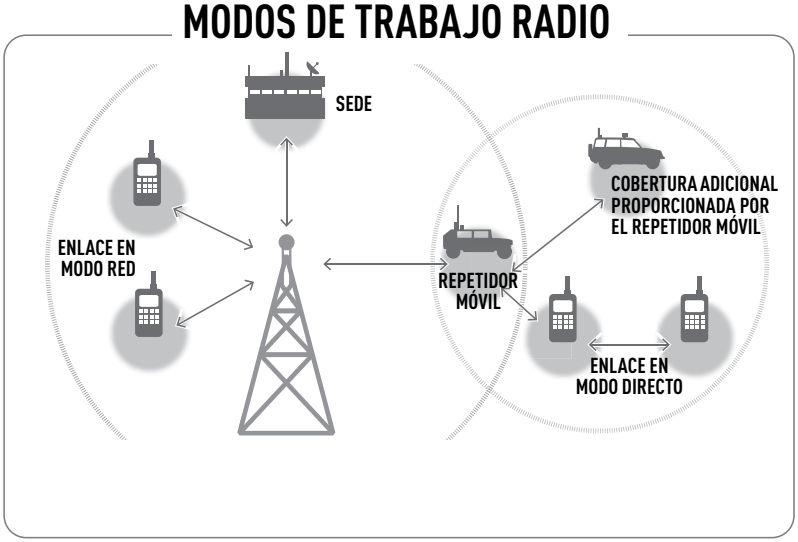
En esta fase de la emergencia predomina la **fonía**, quedando el uso de los sistemas de información minimizados, sino aparcados, hasta un momento más idóneo.

Finalmente, en este punto se debe introducir un matiz a tener en cuenta tanto por los directores de la emergencia como por el propio personal TIC. Nos referimos a los **voluntarios espontáneos** y a otros **llegados desde el exterior**[33] que pueden aparecer en ciertos momentos sin ningún medio de telecomunicaciones. En ocasiones convierten sus buenas intenciones en problemas de coordinación, al internarse en la zona de emergencia, poniendo en riesgo su vida y las de otros intervinientes.

LÍNEA DE COMUNICACIÓN 4: Entre Intervinientes de distintas organizaciones en la zona de la emergencia.

Ya hemos planteado que el problema de la **falta de interoperabilidad** será muy tangible en estos momentos. Aunque en los últimos años se ha trabajado duro para reducir este problema, lo cierto es que todavía queda un largo recorrido para solucionarlo.

Los ejercicios y simulacros entre **organizaciones que estén destinadas a trabajar juntas** en algún momento, permitirá atajar parte de



EMPLEO DE LA RADIO

La formación y la experiencia en el uso de los medios radio es fundamental. El uso de una emisora radio no es baladí, más si cabe cuando una buena coordinación será la base para asegurar el Mando y Control de la emergencia y puede evitar poner innecesariamente en peligro la vida de los intervinientes.

Todo operativo tendrá en mente cual es el modo más optimo, o incluso el "único", que tiene y puede usar en cada momento.

Los modos posibles son los que se señalan:

- Enlace Modo directo
- Enlace Modo Red
- Empleo de Repetidores

33. Este último caso suele darse en grandes catástrofes internacionales en las que aparecen profesionales de las emergencias "freelanders".

la problemática, ya que se habrán tomado las medidas oportunas para minimizar los problemas de compatibilidad entre equipos.

Sin embargo aquellas organizaciones que se vean en la tesitura de **trabajar por primera vez juntas** se verán castigadas por este condicionante. Incluso en el mejor de los casos, que es que de alguna manera tengan equipos de comunicaciones compatibles, se deberán tomar las medidas necesarias por parte de los Responsables TIC para coordinar canales, números de abonado y/o frecuencias de trabajo.

Por desgracia, en muchas otras ocasiones **esta incompatibilidad será insuperable** mediante un simple intercambio de información técnica, debiendo acudir a otras soluciones más complejas.

Aunque en el capítulo 8 abordaremos este problema de una manera más profunda y teórica, vamos a identificar **cuatro niveles posibles de intercambio de información** para de esta manera soslayar la falta de interoperabilidad en la misma zona de la intervención. Para ello nos ayudaremos de la figura adjunta en la que se reflejan dos organizaciones trabajando en la misma zona de emergencia. En la figura se representan tres niveles: nivel interviniente, nivel puesto de mando desplegado en las inmediaciones de la zona de operaciones y sede de procedencia de cada una de las organizaciones.

PROBLEMAS DE INTEROPERABILIDAD EN EL NIVEL INTERVINIENTE

Empecemos por la parte inferior. **A nivel intervinientes (bajo nivel).** En este momento el Responsable TIC, es decir usted, deberá acudir a la imaginación para arribar a buen puerto. En primer lugar vamos a buscar lo fácil y sencillo.

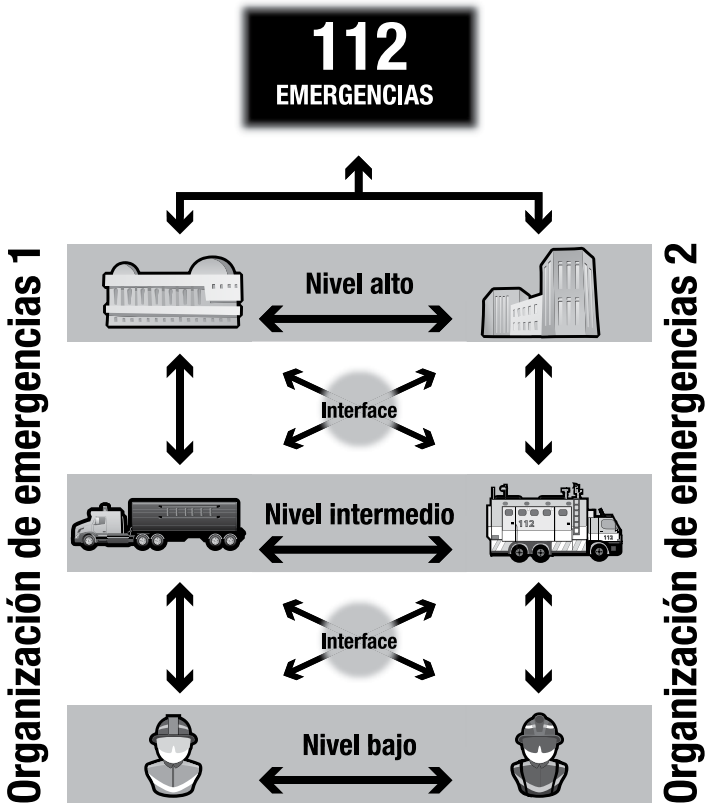
Pongamos un ejemplo aclaratorio. Imaginemos que queremos enlazar el personal de una BRIF (Brigada de Refuerzo de Incendios Forestales) del Ministerio de Agricultura con elementos de un Consorcio Provincial de Bomberos Forestales que trabajan en el mismo sector de un incendio.

Si los **equipos radio** de los intervinientes de cada una de las organizaciones **no son compatibles,** comprobaremos si funciona la **telefonía móvil.** Si la telefonía móvil no funciona o nos estamos moviendo en una zona sin cobertura..., evidentemente esta solución no nos servirá de nada. Pero si por una vez tenemos suerte, hoy día casi todo el mundo posee un teléfono celular. Si es así el intercambio de número de teléfonos es una solución básica.

Si no, buscaremos otra opción. **Existe la posibilidad de intercambiar radios.** Esta opción es buena si son sencillas de utilizar, aunque dificulta la operación de los intervinientes que se ven obligados a trabajar con medios que no son propios, que no conocen y que distraen su atención.

Si todavía no hemos logrado solucionar nuestro problema de enlace en el nivel del interviniente deberemos recurrir a subir de nivel. **Nos vamos al nivel intermedio** (según esquema adjunto).

NIVELES DE INTERCAMBIO DE INFORMACIÓN



En caso de optar por la solución de intercambio de equipos **es preferible hacerlo en el nivel intermedio.** No se complica al interviniente con equipación adicional, y además al subir un escalón se reducirá el número de radios necesarias a intercambiar.

PROBLEMAS DE INTEROPERABILIDAD EN EL NIVEL PUESTO DE MANDO O INTERMEDIO

Nos situamos ahora en el nivel intermedio para resolver el problema del enlace en este mismo nivel. Notar que en el apartado anterior nos fuimos al nivel intermedio sólo para solucionar un problema de enlace del nivel bajo.

Ahora debemos comprobar si a través de cada una de las cadenas de mando de las respectivas organizaciones se tiene enlace. Este nivel intermedio serán, por ejemplo, los **Puestos de Mando tácticos u operativos en la zona de la emergencia de cada organización** que normalmente estará en las inmediaciones del **Puesto de Mando del Director de la Emergencia.** En este punto deberemos volver a revisar las opciones:

- ¿Radios compatibles? Es difícil que si las organizaciones no tienen radios compatibles en el nivel interviniente, que las tengan en sus puestos de mando. No obstante lo inspeccionaremos ya que los vehículos que hacen las funciones de puesto de mando suelen incorporar más material.
- ¿Posibilidad de intercambio de números de teléfono móvil? Realmente puede que las condiciones de cobertura hayan cambiado, por lo que al menos lo comprobaremos.
- ¿Yuxtaposición de puestos de mando? Lo que queremos decir es que si estamos en la misma tienda o en el mismo camión, simplemente hablando entre responsables de sendos equipos de intervienes la coordinación se podrá realizar de un modo efectivo, y cada cual solo operará sus equipos para enlazar con sus respectivos intervinientes.
- ¿Intercambio de oficiales de enlace? En este caso cada organización conserva su puesto de mando en emplazamientos separados, pero en cambio cada cual destacará un trabajador de la propia en el puesto de mando del otro servicio. Esta simple operación permitirá el intercambio deseado de información.
- ¿Intercambio de terminales radio? Ya lo hemos comentado antes. El intercambio de radios a este nivel tiene ventajas a considerar por el responsable TIC.

Si de nuevo nos encontramos que no es posible enlazar los intervinientes, o que el enlace entre elementos del nivel intermedio no es factible, una vez más subiremos de nivel.

PROBLEMAS DE INTEROPERABILIDAD EN EL NIVEL ALTO O SEDE DE PROCEDENCIA

Estamos en el **nivel alto.** Este nivel corresponde a las **Sedes o Centros de Coordinación fijos de las organizaciones intervinientes.** El lector debe notar que realmente nos estamos alejando de la zona de la emergencia, por lo que existirán más posibilidades de que la infraestructura de telecomunicaciones esté menos afectada.

Una vez más revisaremos las opciones:

- ¿Radios compatibles? En estas instalaciones fijas no se suelen considerar, ya que incluso las distancias entre centros puede

***TÉLÉCOMS SANS FRONTIÉRES* (TSF)**

Un grupo de ingenieros de telecomunicaciones franceses crearon hace 12 años una organización especializada en levantar redes de telecomunicaciones en zonas afectadas por catástrofes. Su intervención fue decisiva tras el tsunami que afectó a las islas Salomón en 2007. TSF desplegó entonces una red de telecomunicaciones sobre el archipiélago desde su base en Bangkok, lo que permitió a los servicios de emergencia conocer el estado de los habitantes de las islas más alejadas y sus necesidades, así como que éstos se comunicaran con sus familiares en el extranjero.

TSF es la primera ONG declarada como socia por la Oficina de Naciones Unidas para la Coordinación de Asuntos Humanitarios, lo que supone su participación inmediatamente tras una catástrofe en la valoración de la situación junto con la OCHA para definir el plan de acción, en lo que se conoce como el *Emergency Telecom Cluster*.

TSF con 3 bases en el mundo (Pau, Managua y Bangkok) garantiza el despliegue de personal y equipos de telecomunicaciones entre 24 y 48 horas en cualquier parte del mundo donde se haya producido una gran catástrofe. Su actuación sobre el terreno tiene dos ámbitos: por un lado, el facilitar infraestructuras de comunicaciones (generalmente comunicación de voz y datos vía satélite) a Naciones Unidas y todas las ONG presentes y, por otro, facilitar a la población general víctima de la catástrofe la posibilidad de contactar con sus familiares (una llamada gratuita) iniciativa sencilla pero de gran impacto humano.

superar la distancia máxima de enlace de los equipos radio.

- ¿Posibilidad de intercambio de números de teléfono móvil? No sólo de móvil. Normalmente serán los teléfonos fijos y enlaces de datos los que permitirán la coordinación entre diferentes cuerpos y servicios.
- ¿Yuxtaposición de puestos de mando? No será viable ya que normalmente son centros fijos inamovibles.
- ¿Intercambio de oficiales de enlace? Más que recomendable, ya que permitirá un mejor desarrollo de los trabajos en común.
- ¿Intercambio de terminales radio? No ha lugar por las mismas razones esgrimidas con anterioridad.

Nos queda por último comentar dos aspectos. Los 112 y los posibles interfaces que pueden aparecer entre los niveles.

CENTRO 112

Normalmente están integrados por diferentes servicios (policía, guardia civil, sanitarios, bomberos...) localizados en una misma ubicación que garantizan su enlace por diferentes procedimientos con sus organizaciones origen.

Por lo tanto podemos decir que como última opción se podría plantear subir por cada una de las cadenas de mando de las organizaciones a enlazar, hasta llegar a estos centros para conseguir intercambiar la información en cualquiera de los tres niveles señalados. No olvidaremos tampoco que el subir de nivel implica una mayor complejidad.

INTERFACES

Por último comentaremos la posibilidad de que aparezcan los llamados interfaces en cada uno de los niveles. Estos **interfaces** se tratan de vehículos de telecomunicaciones con los que cuentan determinadas agencias. Tienen un gran número de equipos que a su vez se conectan en un **integrador**, permitiendo la conmutación, automática o manual de todos con todos.

Por ejemplo, estos sistemas suelen tener las siguientes capacidades:

- Realizar llamadas independientes a diferentes tipo de abonado: GSM, INMARSAT, THURAYA, V-SAT, Telefonía IP, Radios de Banda Ciudadana, Radios de Banda Forestal, Redes TETRAPOL, TETRA, etc.
- Poner en comunicación abonados de redes diferentes.
- Interconectar varios equipos diferentes formando una red *ad hoc*.

LÍNEA DE COMUNICACIÓN 5: Solicitud de asistencia internacional.

La cercanía de regiones limítrofes, o en caso de catástrofes de grandes dimensiones, que sobrepasen las capacidades de los servicios de emergencias propios, provocará la aparición de la llamada **asistencia**[34] **exterio**r, regional o internacional. Esta ayuda suele consistir en grupos de intervinientes que se desplazan hasta la misma zona de la emergencia para colaborar con los servicios locales.

La ayuda externa, incluyendo la internacional, suele movilizarse a través de **redes telefónicas públicas mundiales,** aunque no se debe descartar la participación de los **radioaficionados**.

Las nuevas tecnologías han ocasionado la aparición de **redes de datos y sistemas de información dedicados** a este tipo de ayuda. Podríamos mencionar la **red CECIS** (The Common Emergency Communication and Information System) de la Unión Europea por ejemplo, a través de la cual el Mecanismo de Protección Civil de la Unión Europea moviliza módulos y expertos. Estas redes son accesibles a través de internet, por lo que su uso es sencillo.

Por último debemos hacer mención en este apartado al papel que pudieran jugar los **medios de comunicación social** (radio y televisión principalmente) a través de los cuales podría realizarse radiodifusión o "broadcasting" para lanzar una **petición de ayuda masiva.**

LÍNEA DE COMUNICACIÓN 6: Entre las autoridades responsables de la gestión de la emergencia y la población.

Las autoridades gubernamentales encargados de adoptar decisiones necesitan llegar a la población afectada o en peligro de serlo. En una emergencia, los canales para proporcionar información al público son claramente necesarios. Radio, televisión, y a menudo Internet suelen proporcionarla, aunque en ocasiones suele ser muy genérica y puede que no ayude necesariamente a las personas en áreas específicas.

Existirán tres opciones. Primera, hacer uso de los **medios de comunicación social** para a través de ellos pasar cuanta información sea necesaria. La segunda opción, que se detalla en el siguiente apartado, es transferir la responsabilidad a los **propios servicios de emergencia.** Y por último una **combinación de ambas**.

34. ¡Cuidado! Aunque estemos hablando de "ayuda" en determinados contextos no es políticamente correcto y en cualquier idioma se favorece el uso de la palabra "asistencia".

El **uso de los medios de comunicación social** es una herramienta poderosa que sin embargo puede resultar complicada de controlar, al no poder discernir con la debida exactitud las áreas dónde se recibirá la señal. Se corre el riesgo de contribuir a aumentar el nerviosismo en determinadas zonas que no están afectadas, o incluso en las que sí lo están, se puede aumentar el nivel de estrés, por ejemplo de un potencial personal a evacuar. Hoy día existe tecnología en el mercado que permite introducir mensajes en la parte inferior de las pantallas de televisión sin llegar a alterar las programaciones habituales.

LÍNEA DE COMUNICACIÓN 7: Entre servicios de emergencia y la población

Tenemos que hacer una clara diferenciación entre la población que se encuentra en el propio lugar de la catástrofe y la que no lo está. Para los primeros, es evidente que el **modo más sencillo será establecer contacto directo** y comunicar por los mismos intervinientes las instrucciones a seguir.

Los que no están damnificados, pero que están en situación de peligro o al menos preocupados por su estatus deben ser también tenidos en cuenta. Pero claro, el contexto no nos va a ayudar. Por lo tanto, una vez más, deberemos acudir a cuantos medios tengamos a nuestro alcance.

En los momentos inmediatamente posteriores a una emergencia, se produce un importante crecimiento de llamadas telefónicas, sobre todo móviles. En la tarde-noche del 23 de agosto de 2005, el momento más crítico de unas intensas inundaciones ocurridas en el sur de Alemania, se registró un incremento de llamadas de móviles y de mensajes SMS de un 275% y 350%, respectivamente, en las dos estaciones base más congestionadas.

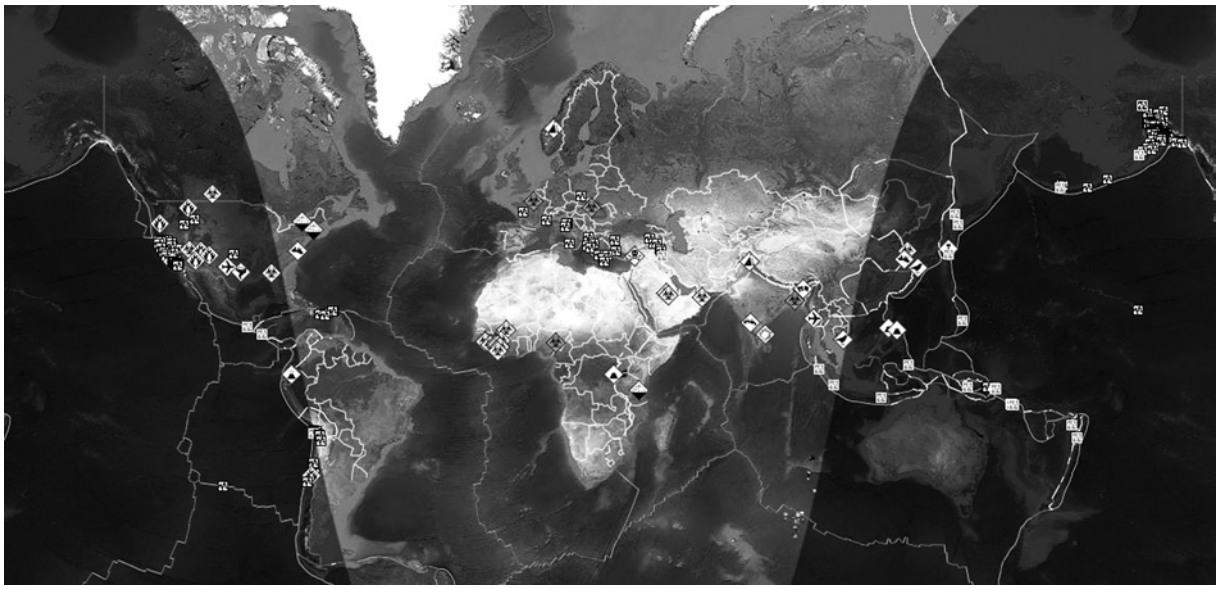
Una vez conocida la existencia de una emergencia, **Internet** es el medio que muchos ciudadanos utilizan para consultar información actualizada. Son numerosos los sitios en la red, nacionales e internacionales, o redes sociales utilizadas por los propios 112 que ofrecen información en tiempo real para mantener a la última a la población afectada. No debemos echar en saco roto que el suministro de información a la población proporciona un bienestar psicológico importante. Por ejemplo tras los atentados del 11S comenzaron a aflorar de forma espontánea "**tablones de anuncios**" en internet con el lema "**Estoy vivo**".

Para comunicarse con el resto de usuarios que no usen Internet, deberemos volver al capítulo 1 de este libro y recordar otros modos con los que contábamos para materializar el enlace.

PORTAL WEB DE CATÁSTROFES MUNDIALES

Alertmap es una web que, de forma gráfica y sobre un mapamundi, informa en tiempo real sobre las emergencias más significativas que ocurren en el mundo, mediante la utilización de datos procedentes de una amplia red de sismógrafos y detectores de desastres en todo el planeta. Se trata de una iniciativa húngara promovida por la ONG emergency and Disaster Information Services (eDiS).

ALERTMAP



En primer lugar hicimos mención a los medios y procedimientos electromagnéticos. Exceptuando Internet, ya comentado, los servicios de emergencia **deberán hacer uso de medios de transmisión compatibles** con los que pueda tener un ciudadano común. De nuevo el teléfono, la radio y la televisión. También hemos mencionado los sistemas de **transmisión de mensajes** masivos que al igual que se usan para informar que se acerca "un problema" o para dar instrucciones. Una vez que el interlocutor descuelga el teléfono recibe un **mensaje grabado** en el que recibe la información necesaria. Otra opción es mediante envío de **mensajes SMS** a los teléfonos móviles identificados en una zona.

Por último existe la opción de enviar **mensajes emergentes a través de internet** a los ordenadores que se detecten activos.

Sin embargo no debemos dar por supuesto que estos centros 112 van a estar operativos, y ni tan siquiera que existen en la zona donde se ha producido la emergencia. Es entonces cuando acudiremos al resto de procedimientos mencionados en el primer capítulo. Los **medios acústicos, y los ópticos y visuales.**

Un simple coche de policía con sus sirenas circulando por las calles, o un bombero con megáfono en mano ilustra una sencilla imagen de esta opción sonora.

En cuanto a la visual podríamos recurrir a luces estroboscópicas, paineles, o incluso pantallas gigantes de televisión en las calles para mandar los mensajes.

35. Cuando se realizan intervenciones internacionales, es común denominar "**Base de Operaciones**" al campamento que se establece en el lugar donde se despliega, y "**Base Retrasada**" o "**Home Base**", a la sede que se deja en el país origen. También se les conoce como enlace "Tango November"... por las siglas de **T**erritorio **N**acional.

LÍNEA DE COMUNICACIÓN 8: Entre servicios de asistencia internacional y sus bases de procedencia

Estos equipos acuden normalmente con medios de telecomunicaciones para cubrir tres tipos de enlace:

- **Enlaces con su base origen**[35], que consistirán en equipos que permitan comunicar con sus lugares de procedencia, y que por tanto serán acordes con las distancias a cubrir. Pueden variar desde un simple teléfono móvil, pasando por equipos radio, o como ya hemos mencionado, con equipos portátiles satélite.
- **Equipos de telecomunicaciones destinados a garantizar su operatividad y seguridad** en la intervención propiamente dicha. Sin duda los equipos radio son los más habituales.
- **Sistemas de telecomunicaciones instalados en la zona afectada con vocación de permanencia.** Es decir nos estamos refiriendo a sistemas que organismos como la Unión Internacional de Telecomunicaciones (UIT, ITU en inglés) instala en zonas golpeadas por catástrofes y que luego donan a las autoridades locales para favorecer la recuperación en etapas posteriores de la reconstrucción.

SISTEMAS USADOS EN LA FASE DE VUELTA A LA NORMALIDAD

Los servicios de emergencia irán disminuyendo su actividad dejando paso a los **servicios de reconstrucción.** Esta afirmación lleva consigo que lógicamente cada organización se volverá normalmente a sus Cuarteles Generales llevándose los medios de enlace que habían traído, mientras que los recién llegados aportarán lógicamente los suyos propios.

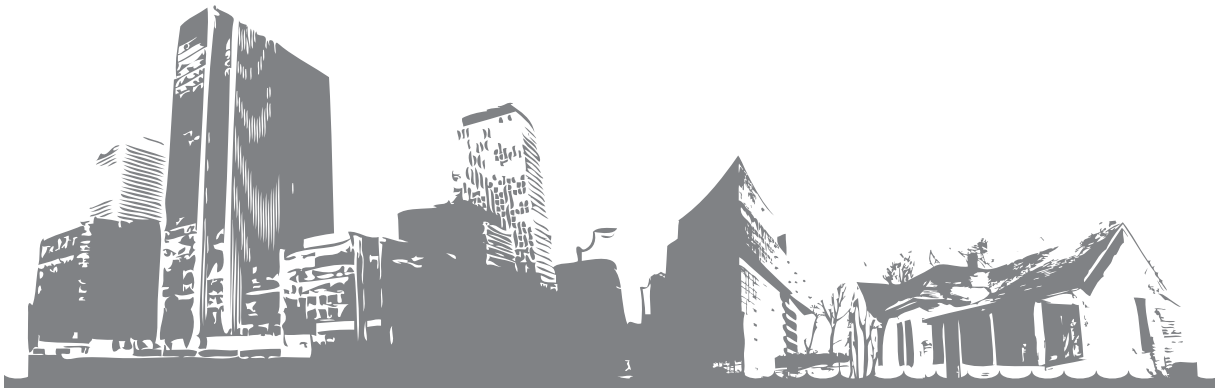
Diferentes misiones, implican normalmente diferente tipo de materiales. Si la fase de intervención se caracterizaba por recursos de telecomunicaciones dañados, saturados y poco fiables, es de suponer que en el periodo trascurrido hasta llegar a la fase de vuelta a la normalidad, **gran parte de la infraestructura terrestre se habrá recuperado.**

Si no fuera así, las autoridades responsables habrán montado un sistema sobre el que ejercer sus funciones de dirección y coordinación, y que deberá mantenerse operativo. Esto llevará implícito unas **tareas de relevo** de terminales y de adiestramiento en su uso del personal entrante.

Durante la fase de intervención urgente, hay que establecer las telecomunicaciones literalmente "a toda prisa", y sobre todo la infraestructura telefónica fija y móvil no será fiable. Como hemos visto en la anterior fase, eran los equipos radio portátiles y los teléfonos satélites los más usados

Una vez la situación se estabiliza, las organizaciones encargadas de la reconstrucción o estabilización de la zona dañada harán uso de sus propios equipos de transmisiones. Si se trata por ejemplo de una empresa constructora que llega a recuperar una ciudad devastada por un terremoto, tendrán sus propios sistemas para enlazar capataces con camiones u operadores de maquinaria pesada. El lector debe notar que **en este momento la urgencia es ya relativa,** y en muchos casos se limitarán a equipos radio vehiculares o teléfonos móviles.

Otro ejemplo. Tras un gran incendio forestal, las dotaciones de consorcios de bomberos se repliegan una vez éste se ha extinguido. Con posterioridad los



HURACÁN KATRINA (2005)

agentes forestales comenzarán sus tareas de rehabilitación y harán uso de los medios que tenían antes de que se produjera el incendio, estamos hablando ahora de **medios de telecomunicaciones de la fase de prevención y seguimiento o medios "todo tiempo".**

En el **caso de las ayudas externas** en forma de medios de telecomunicaciones, éstas deberían haber llegado en la fase anterior. Suele tratarse de sistemas duraderos, **basados en tecnologías que podrán quedar posteriormente en manos de colaboradores** locales para la fase de vuelta a la normalidad o estabilización. Las actuaciones de la UIT en este campo son muy conocidas[36].

En julio de 2010 la UIT instaló en Pakistán 100 terminales de satélite de banda ancha a raíz de inundaciones devastadoras que causaron el desplazamiento de 15 millones de habitantes e importantes daños a la infraestructura. Los equipos se utilizaron para servicios de comunicaciones básicas y de telemedicina. Ya en marzo de 2011, tras el devastador terremoto de Japón, la UIT envió 78 teléfonos satélite Thuraya, 13 teléfonos Iridium y 37 terminales Inmarsat para facilitar las actividades de búsqueda y salvamento.

Reiteramos de nuevo que algunos de los medios identificados como preponderantes en una fase de la emergencia, se utilizarán en otras fases sucesivas o previas, pero con menos peso específico. Valga como ejemplo que las Agencias 112, no finalizan su trabajo cuando comienza la fase de intervención; o que las redes radio de los cuerpos policiales que echan el resto en la fase de intervención, son utilizadas por supuesto en la fase prevención y en la de vuelta a la normalidad.

Vamos a finalizar este apartado mencionando que esta última fase de la emergencia han cogido un peso importantísimo las **TIC como medio para facilitar donaciones,** que sirvan a los damnificados para mejorar su situación. Como ejemplo podemos mencionar que tras el desastre del tsunami de Sumatra, Cruz Roja Española recaudó más de 8 millones de euros a través de los millones de SMS enviados a través de las tres operadoras móviles en la campaña 'Un puente solidario', iniciada por la cadena televisiva Antena 3.

En los últimos años se ha experimentado un fuerte incremento de las donaciones económicas realizadas por Internet, que permiten a los ciudadanos sensibilizados poder aportar su ayuda, fácil y rápidamente desde cualquier parte del mundo.

TIC FUERA DE SERVICIO

Con el paso del huracán Katrina, más de 3 millones de líneas de telefonía fija quedaron dañadas, así como algunas centrales. Más de 2.000 celdas de las redes locales móviles quedaron sin servicio. Un mes más tarde, 264.000 líneas de telefonía fija y 820 celdas de telefonía móvil permanecían todavía fuera de servicio.

Sin embargo, en las zonas más próximas al área afectada, había cobertura de telefonía móvil gracias a la utilización de estaciones base portátiles y generadores, que hacían posible el enrutamiento de llamadas.

36. El despliegue sobre el terreno de telecomunicaciones de emergencia que realiza la UIT forma parte de su Marco para la cooperación en situaciones de emergencia (más comúnmente conocido como IFCE). Además de ofrecer servicios de telecomunicaciones para la mitigación de la catástrofe en todas las fases de la gestión de la misma, IFCE también moviliza recursos para garantizar una respuesta inmediata, fiable y oportuna si una catástrofe afecta a algún Estado Miembro de la UIT en cualquier lugar del mundo.

CAPÍTULO 5

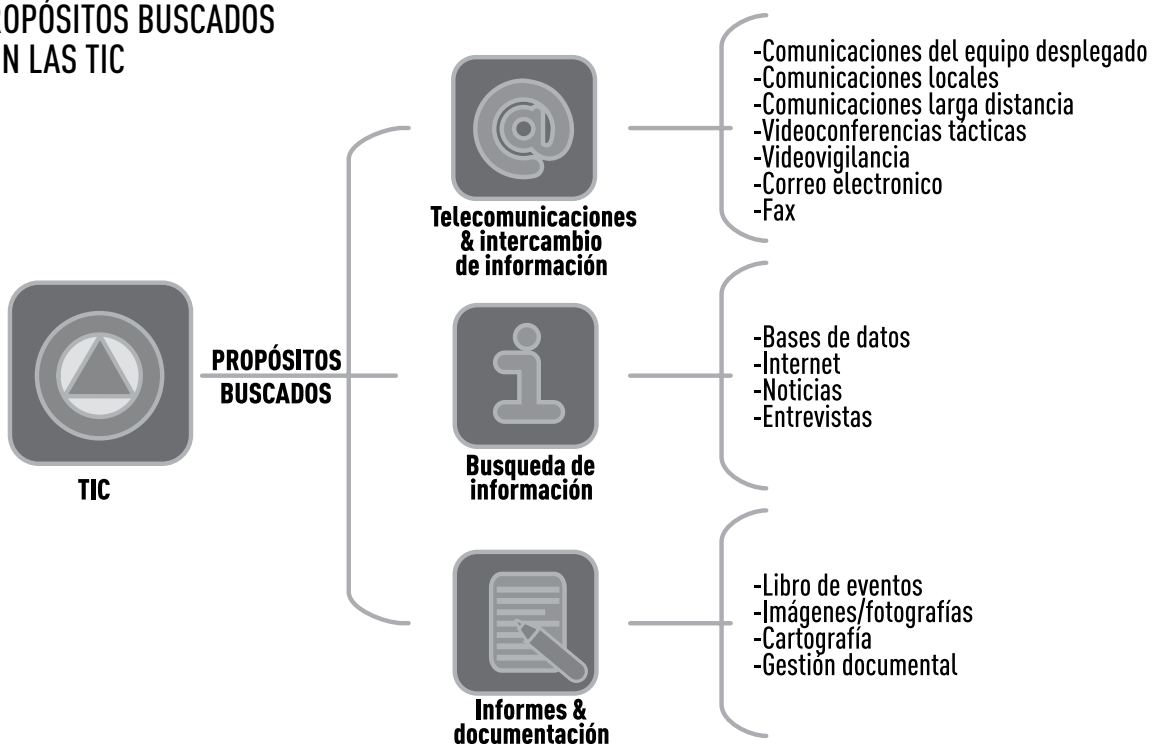
MEDIOS QUE MATERIALIZAN LAS TELECOMUNICACIONES

No queremos que nuestro lector se sienta traicionado. Habíamos dicho que una de las intenciones que pretendíamos alcanzar era usar un lenguaje claro sin entrar en la tecnología. No es que nuestra palabra, esté al nivel de la de ciertos políticos..., sino que para poder dar una visión completa del tema del enlace tenemos que hablar de manera sucinta de los distintos medios de telecomunicaciones que existen. De esta manera aquellos que tienen un primer contacto con este mundo, no se vean obligados a recurrir a bibliografía complementaria para entendernos, mientras que los que ya tienen nociones pueden saltárselo sin más, si no tienen esperanza de encontrar nada nuevo.

Pues lo dicho... Lo cierto es que **la voz** constituye el modo de comunicación más adecuado para la transmisión de mensajes breves en tiempo real, sin ninguna necesidad adicional en materia de equipos si lo hacemos en presencia del otro interlocutor (el lector recordará que a este sistema de enlace le llamamos "**contacto directo entre responsables**"). En situaciones delicadas y de urgencia sigue siendo el modo predilecto. El principal **inconveniente del tráfico vocal** es la ausencia de almacenamiento permanente, lo cual dificulta la transmisión y recepción de información compleja.

Si le añadimos equipos adicionales incluso mejoraremos la eficacia de las comunicaciones en fonía. Estamos hablando por ejemplo de sistemas de megafonía o de grabación.

PROPÓSITOS BUSCADOS CON LAS TIC



En este capítulo vamos a tratar los soportes y terminales de usuario utilizados en el **procedimiento de enlace más extendido que es el que utiliza señales electromagnéticas.** En el capítulo 15 haremos lo propio con el resto de modos de materializar el enlace (mensajeros, oficiales de enlace, procedimientos acústicos, visuales, etc.).

Una pregunta recurrente entre los que se están iniciando en los temas relacionados con él, es plantearse **qué tecnologías TIC son las más apropiadas para las emergencias.** En general, no existe ninguna tecnología que sea ideal. Normalmente, existe un compromiso entre la facilidad del uso de la tecnología, su coste y los servicios demandados por el usuario, que como ya sabemos vendrán reflejados en **el concepto operativo y en los escenarios** más probables de empleo.

TIPOS DE TELECOMUNICACIONES BASADAS EN PROCEDIMIENTOS ELECTROMAGNÉTICOS

Es frecuente encontrar clasificaciones de los distintos tipos de telecomunicaciones basadas en procedimientos electromagnéticos. Una básica, que no exacta, podría ser la siguiente:

TELEFÓNICAS

Se fundamentan en el intercambio oral de información, es decir mediante el habla. Éstas eran hasta hace unos años muy fáciles de reconocer porque llevaban asociadas un aparato, llamado "**teléfono**" que mediante un cable transportaba las señales punto a punto[37]. Como el lector intuye esta idea está desfasada, anclada a otra generación. Probablemente

37. Otra clasificación posible que se puede realizar sobre los Sistemas de Telecomunicaciones es la basada en el número de usuarios entre los que se establece la transmisión:
    - Sistemas punto a punto. La comunicación se establece solamente entre dos corresponsales.
    - Sistemas punto a multipunto. La comunicación va de un punto a un conjunto limitado de usuarios.
    - Sistemas broadcast. La comunicación se origina en un punto y va dirigida a todo el mundo, sin restricciones.

EL FAX

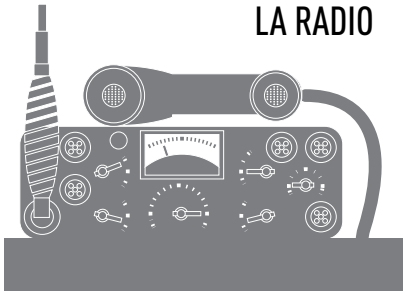
La primera patente de fax data de 1843. Fue Alexander Bain, pero aquella patente, correspondía a una máquina de fax teórica. La primera emisión de un fax, se llevó a cabo en 1851. Este fax, fue desarrollado por el inventor Frederick Blackwell.

Con respecto a su historia comercial, esta data desde 1865, cuando el italiano Giovanni Casselli, creó el primer servicio de emisión de faxes. Este servicio cubría el enlace Lyon-Paris. Para 1906, ya existían servicios de transmisión a distancia de fotografías en Alemania utilizados por los periódicos.

En 1926, se podían enviar imágenes por medio de un fax, de manera trasatlántica, entre las ciudades de Nueva York y Londres. En 1936, el servicio se extendió por toda Europa y algunas ciudades importantes de Sudamérica.

Para mediados del siglo XX, se logró desarrollar una máquina de fax, la cual se podía conectar a cualquier línea telefónica. Pero la revolución definitiva, la llevaron acabo los japoneses, los cuales desarrollaron un fax, que tardaba unos minutos en enviar una hoja. Los anteriores modelos demoraban mucho más en poder transmitir un texto o imagen. Asimismo, lograron reducir aún más el costo de este ya necesario aparato.

LA RADIO



En 1906 comienza la revolución de la Radio con el invento de Lee De Forest quien introduce una rejilla de control en el diodo de vacío de Fleming. Mediante este simple invento el diodo se convierte en un tríodo que podía ser usado para amplificar las señales eléctricas en millones de veces, aparte de su función de válvula es decir dejar fluir o interrumpir el flujo de corriente. La aplicación por excelencia de las válvulas fue la Radio, primero en Radiodifusión y luego para las comunicaciones inalámbricas.

Es a partir de 1947, que un nuevo invento, el transistor, abre nuevos horizontes. Su funcionamiento es parecido al de la válvula, pero con la diferencia de que no se requieren grandes voltajes para su funcionamiento y las cantidades de corriente necesarias para que realice sus funciones son mínimas. Gracias al transistor, las desventajas de las válvulas, es decir su tamaño y el gran consumo de energía que en ellas se desperdicia en forma de calor, desaparecen para permitir la miniaturización de la electrónica.

Aquella ciencia rudimentaria conocida como "La Radio", cambió de denominación en los años 60, y derivó en la sofisticada Electrónica que englobó a todas las técnicas conocidas: radio, televisión, radar, telecomunicaciones, computación, instrumentación, ayudas de vuelo, mando a distancia, telemetría, control, detección, satélites, medicina etc.

si le preguntamos a un adolescente qué es una comunicación telefónica, nos sorprenderíamos. O mejor dicho, nos sentiríamos muy viejos...

Una variante interesante y muy conocida de las comunicaciones telefónicas es el **Fax**. Un fax es un sistema, que permite enviar copias de documentos a la distancia, utilizando por lo general las líneas telefónicas. El nombre fax viene del latín "*fac simile*", que quiere decir **hacer igual**; con ello se identifica de excelente manera, lo que es este equipo. Una máquina que envía a distancia, la copia de un texto o imagen.

RADIO

Consiste en el intercambio de información a través de **ondas radioeléctricas.** La radio ha sido el invento por excelencia del siglo XIX. Todo comenzó con el experimento de Marconi y ha llegado a convertirse en la infraestructura esencial. La radio no solamente sirve para transmitir ideas sino que está presente en un sinfín de dispositivos. Desde el mando a distancia del garaje hasta en los sistemas de seguridad de las centrales nucleares.

TELEGRÁFICAS

Etimológicamente viene del griego "***tele graphos***", ó **escritura a distancia.** Fue el primer elemento de este tipo que se utilizó para aplicaciones prácticas en las comunicaciones de ayuda en las emergencias. Servía inicialmente para transmitir los llamados telegramas, marconigramas o cablegramas. Años después, los telegramas serían enviados a través de **redes de Télex** similares a la red de teléfono, compuesta por teletipos. Enseguida se empleó en enlaces radioeléctricos mediante los **radioteletipos (RTTY)**, pero el hecho de que se precisaran enlaces fiables y constantes limitó su utilidad en las situaciones de emergencia. En la actualidad, se denominan así a las telecomunicaciones en las que la información es transmitida y registrada en el receptor en forma de documento o guardado en dispositivos de memoria para su posterior utilización. Existe una variante, la **radiotelegrafía** o la telegrafía sin cables, la cual transmite mensajes usando la radio, normalmente apoyándose en el **código Morse**. Los telegramas tienen validez legal y son vinculantes como prueba judicial, al igual que ocurre con los informes o "*reporter*" de los faxes.

DE DATOS DIGITALES[38]

Internet es el instrumento más destacado de la comunicación de datos donde se da la transferencia de información, normalmente, entre ordenadores. Las tecnologías digitales avanzadas posibilitaron la evolución de nuevos modos de comunicación de datos que acabaron con los inconvenientes de las redes telegráficas al dividir los mensajes en "**paquetes**" y ceder a los ordenadores la transmisión automática de un acuse de recibo[39] de recepción correcta o la petición de retransmisión si no se ha recibido toda la información esperada.

Los datos se representan como una señal electromagnética, una señal de tensión eléctrica, ondas radioeléctricas, microondas o infrarrojos. Existen multitud de procedimientos y protocolos que consiguen mediante la transmisión analógica, o la digital, lograr llegar la información entre dos destinatarios. Entre los modos más demandados en los últimos tiempos de transmisión de datos, se encuentra la transferencia de video, o **videoconferencia**.

Quizás algún lector encuentre esta clasificación escasa o inexacta. Puede ser, no obstante lo habíamos advertido antes de iniciarla. Conceptos como comunicaciones satelitales, conmutadores, repetidores o internet no aparecen en ella. Pero no es por olvido, es algo premeditado. En nuestro libro queremos que todo sea sencillo, y con esta organización creemos que es suficiente.

Sin embargo ampliaremos un poco más. Vamos a retomar la figura de la **Teoría de la Comunicación** y la vamos a condimentar con una "pizca de técnica". Si allí nos referíamos a un emisor, un canal y un receptor, vamos a ver cuál es el resultado de vestirla con otros "ropajes" más tecnológicos.

DEL "CANAL" AL "SOPORTE"

Nuestra correspondencia la haremos identificando el canal con **el soporte físico a través el cual se propagan las señales** que contienen la información aplicada por el emisor. El soporte admite una o varias transmisiones simultáneamente. Pueden ser soportes radioeléctricos y filares. A continuación los veremos un poco más en detalle.

38. Añadimos el sustantivo "digitales" a la transmisión de datos, pues si somos puristas el telégrafo, anterior al teléfono y a la telegrafía inalámbrica que precedió a la radiotelefonía, fueron en realidad las primeras formas de enlaces de datos.

39. Es conocido como el **código ARQ** *(Automatic Repeat Query)*, el cual genera automáticamente un acuse de recibo o una petición de retransmisión entre dos interlocutores en un momento dado.

SOPORTES RADIOELÉCTRICOS

Son los que emplean las **ondas electromagnéticas radiadas** por un emisor y captadas por un receptor, como vehículo para la transmisión de la información. Su éxito radica en la facilidad e inmediatez para formas "**redes *ad hoc***", sin necesidad de una infraestructura previa. Son por tanto flexibles en su despliegue y escalables.

Este soporte está también limitado en alcance dependiendo de la frecuencia utilizada, y condicionadas por la topografía del terreno. Su mayor capacidad es que son móviles y se pueden portar por una persona o dentro de un vehículo.

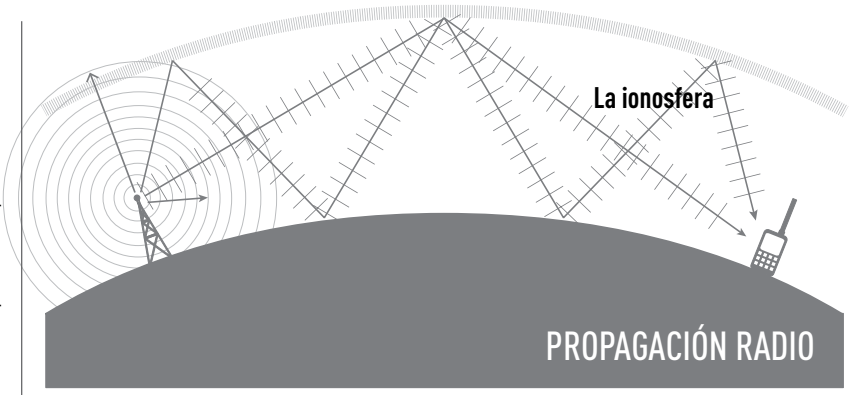
Se caracterizan por su **modo de propagación** y por su **frecuencia**.

El modo de propagación indica la manera según la cual una onda electromagnética se desplaza desde la fuente que la genera. Los modos de propagación existentes son: onda de superficie, onda ionosférica, onda espacial, dispersión troposférica y onda transionosférica. Existe un modo mixto denominado onda de tierra, constituido por la composición de la onda de superficie y por las componentes directa y reflejada de la onda espacial.

Existe un dicho entre los especialistas en el uso de la radio que resume este hecho:

> ***"DIME CUÁL ES TU FRECUENCIA, Y YO TE DIRÉ CÓMO TE PROPAGAS".***

Las **frecuencias** utilizadas en la propagación radioeléctrica se agrupan en bandas de frecuencias, que permiten la transmisión por el modo más apropiado a cada una de ellas. Las más comunes de las empleadas en telecomunicaciones radio son las bandas siguientes: LHF, HF, VHF, UHF y SHF.



Las bandas de frecuencias de trabajo **VHF** y **UHF** son conocidas como las de "**corto alcance**". Las de **HF** y **LF** se las conoce también como de "**medio y largo alcance**" o las llamadas "**onda media**" u "**onda corta**", y su uso resultó fundamental durante la Segunda Guerra Mundial[40]. Ahora están en desuso por culpa de la radio a través de internet. Las frecuencias de **SHF** suelen ser utilizadas para comunicación satélite.

Los **anchos de banda** en LHF, HF y VHF, son **muy pequeños,** lo que se traduce en que prácticamente lo que permite establecer son comunicaciones de voz (fonía) y unas transmisiones de datos muy limitadas y lentas. Es decir que como Responsables TIC debemos apercibir a las autoridades de que con la radio se deben olvidar de servicios tipo videoconferencia, acceso a internet, correo electrónico... Los usuarios normalmente sólo pueden recibir o transmitir, pero no de manera simultánea (modo simplex). Existe la opción de usar estaciones repetidoras para aumentar los alcances, y se precisa una gran disciplina al hablar, ya que muchos de estos sistemas sólo permiten una conversación simultánea en la red.

Las comunicaciones en UHF y SHF proporcionan mayores capacidades como explicaremos más adelante.

LA PROPAGACIÓN DE LAS ONDAS

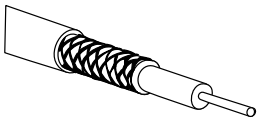
Se llama propagación al conjunto de fenómenos físicos que conducen a las ondas del transmisor al receptor. Esta propagación puede realizarse siguiendo diferentes fundamentos físicos, cada uno más adecuado para un rango de frecuencias de la onda a transmitir. Los modos de propagación más frecuentes son: propagación ionosférica, troposférica, onda de superficie, litosfera y la propagación biosfera.

La ionosfera es la región de la alta atmósfera entre 60 y 400 km de altura. Como el propio nombre indica está compuesta de iones y de plasma ionosférico y es de forma esférica al ser una de las capas de la atmósfera. Es importante para la propagación porque permite reflejar o refractar ondas radioeléctricas por debajo de una frecuencia crítica llamada comúnmente MUF, frecuencia máxima utilizable.

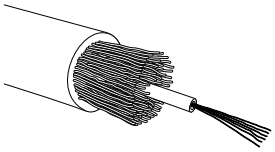
La ionosfera está compuesta de tres capas: la capa D, la capa E, la capa F (durante la noche) que se divide en dos, las capas F1 y F2, durante el día.

40. En el bando Aliado fue más preponderante el uso del soporte radioeléctrico, sobre todo con el radioteletipo, que era la herramienta básica para sus comunicaciones puesto que tuvieron un mejor control sobre el mar y sus costas. Por el lado de los países de El Eje, el dominio sobre el escenario europeo les permitía un mejor control sobre las líneas terrestres que empleaban básicamente también el teletipo pero por soporte filar.

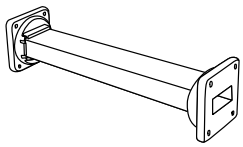
SOPORTES FILARES



CABLE COAXIAL



FIBRA ÓPTICA



GUÍA DE ONDAS

SOPORTES FILARES

Comúnmente conocidos por "**cables**" que conducen señales electromagnéticas o corriente eléctrica mediante una codificación predeterminada de la información que transportan. Pueden transportar una o varias comunicaciones a la vez. Los tipos de soporte filares más conocidos son los siguientes:

- **Cable convencional de pares:** formado por pares de conductores eléctricos, normalmente cobre. Dentro de los mismos está el **cable coaxial** formado por dos conductores cilíndricos concéntricos separados por un aislante y debidamente protegidos. Pueden llegar a proporcionar un número elevado de transmisiones simultáneas a unas distancias limitadas por sus características técnicas.
- **Fibra óptica:** es de los tipos de cable más conocidos y utilizados en la actualidad. Para grandes distancias ha desbancado por completo al cable convencional. Puede estar constituida por una o varias fibras ópticas bajo una envuelta de plástico o caucho resistente. Los cables de fibra óptica permiten la propagación en su interior de señales electromagnéticas en la banda del espectro luminoso y con capacidad para miles de comunicaciones simultáneas por cada conductor óptico. Puede alcanzar mayores distancias que con los cables de pares.
- **Guía de onda:** son las menos conocidas por el público no especializado ya que su aplicación es muy específica. Son unas canalizaciones destinadas a la propagación dirigida y acotada de radiación electromagnética.

Los **anchos de banda** en los soportes filares son **grandes** en comparación por ejemplo con las bandas de frecuencias bajas de los soportes radioeléctricos, lo que se traduce en que aparte de las comunicaciones en fonía tendremos **posibilidad de establecer unas transmisiones de datos muy elevadas** con capacidades para acceder a servicios demandantes de ancho de banda como consulta a bases de datos, correo electrónico o videoconferencia, todo ellos si contamos con los equipos necesarios a los extremos del soporte. De estos equipos vamos a tratar en el siguiente apartado.

DEL "EMISOR & RECEPTOR" AL "EQUIPO TERMINAL"

Visto el soporte que se puede utilizar para transportar la información de un lugar a otro distante nos queda encontrar el ingenio que permita introducir esa misma información en el soporte, y en el otro extremo el equipo que permita recuperarla para poder interpretarla. Nos referimos por tanto a los **Equipos Terminales.** Así el esquema de teoría de la información se transforma en el siguiente.

Equipo terminal es por tanto el ingenio mediante el que se consigue la entrada o la salida de la información por parte de un usuario, o incluso una máquina, adaptando en ambos sentidos las propiedades de las señales que se transmiten, para que a través del soporte se haga efectiva la Teoría de la Comunicación.

Existen diferentes tipos como ya puede intuir el lector.

TERMINALES TELEFÓNICOS

Permiten la conversación simultánea en ambos sentidos. Puede ser usado por **personal sin formación** ya que es de uso cotidiano en nuestra sociedad occidental. Habitualmente comprenden un micrófono y un receptor, también otros órganos tales como un timbre y un dispositivo de marcación. Se emplean para la transmisión de señales vocales.

Existen **teléfonos fijos y móviles**. Los primeros utilizan como soporte las redes de cableado. Los segundos su soporte es radioeléctrico entre terminal y estación base de telefonía. Otra posible variante es el **teléfono inalámbrico,** que utiliza un soporte radioeléctrico entre el terminal y la base telefónica que se encuentra unida físicamente a la red filar telefónica.

Otra posible clasificación se basa en la alimentación eléctrica del terminal. Así hay **teléfonos de batería local** alimentados por pilas situadas en el propio terminal, y los de batería central en los que es la propia central la que alimenta los teléfonos conectados a ella.

Aunque son arcaicos, dado el uso que se puede dar en determinadas operaciones de rescate en cuevas o espeleosocorro, vamos a hacer mención a los **genéfonos** o teléfonos sin batería. Éstos producen la energía eléctrica por medio de la propia energía acústica de la voz. Son sencillos pero su alcance es limitado.

Los teléfonos no permiten conservar copia de la información cursada, a menos que estén provistos de **equipos de grabación**. En determinadas circunstancias se pueden utilizar para mandar mensajes oficiales, precedido por unas acciones de registro y control determinados. En este caso esos mensajes se denominan **telefonemas**. Se le pueden asociar otros equipos adicionales como contestadores automáticos, o secráfonos que permiten cifrar la información.

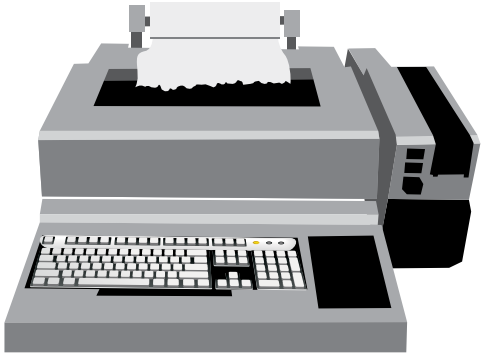
TERMINALES TELEGRÁFICOS

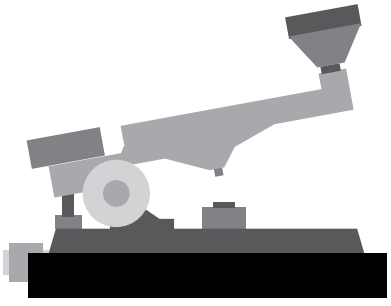
Pertenecen a este grupo los llamados **Teletipos**, aunque en el argot han recibido distintos nombres como TTY, teleimpresor o télex. Precisamente al mensaje se le conoce como télex. Un dispositivo telegráfico es un tipo de transmisión de datos, ya obsoleto, utilizado durante el siglo xx, para enviar y recibir mensajes mecanografiados punto a punto a través de un canal de comunicación simple, a menudo un par de cables de telégrafo.

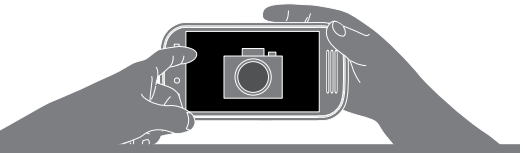
Las últimas formas más modernas de estos equipos fueron ordenadores con emuladores software. El sistema todavía se utiliza

TERMINALES TELEGRÁFICOS

A •-	D -••	G --•	J •---	N -•	P •--•	S •••	V •••-	Y -•--	1 •----	4 ••••-	7 --•••	• •-•-•-
B -•••	E •	H ••••	K -•-	O ---	Q --•-	T -	W •--	Z --••	2 ••---	5 •••••	8 ---••	, --••--
C -•-•	F ••-•	I ••	L •-••	M --	R •-•	U ••-	X -••-	0 -----	3 •••--	6 -••••	9 ----•	? ••--••







LA CÁMARA FOTOGRÁFICA DE LOS TELÉFONOS MÓVILES

FOTOGRAFIAS DIGITALES

La incorporación de cámaras en los teléfonos móviles permite disponer de testimonios gráficos sobre la emergencia en tiempo real, gracias a la colaboración de afectados que envían los videos o fotos recogidos por sus teléfonos móviles para su difusión por los medios de comunicación.

El 7 de Julio de 2005, día de los atentados de Londres, la BBC recibió más de 300 mensajes de correo electrónico incluyendo 900 imágenes, así como 22.000 mensajes de texto que describían lo que estaba sucediendo.

para personas sordas o con serias discapacidades auditivas, a fin de poner por escrito comunicaciones telefónicas.

Igualmente pertenecen a esta subdivisión los "**chilaris**" o **Manipuladores de Morse.** Hoy día se sigue utilizando fundamentalmente por radioaficionados bohemios y en la Marina Mercante incluyendo el Salvamento Marítimo.

TERMINALES FAX

Se emplean para transmitir documentos en modo texto o gráfico. Un fax es esencialmente un escáner de imágenes, un módem y una impresora combinados en un único aparato. El escáner convierte el documento original en una imagen digital; el módem envía la imagen por la línea telefónica; al otro lado, otro módem lo recibe y lo envía a la impresora, que hace una copia del documento original. Un ordenador con fax/módem y el software adecuado es capaz de emular el funcionamiento de una máquina de fax.

La UIT[41] clasifica los faxes en cuatro grupos de menor a mayor capacidad de transmisión..

Al fax se le concede valor legal en España. Correos ofrece servicios de fax y de burofax. El burofax es una comunicación fehaciente con valor probatorio. Este servicio que nació en España como un envío de fax desde una oficina de correos, posteriormente ha ido evolucionando hasta ofrecer la posibilidad de que su imposición sea on-line. Algunas empresas ofrecen como elemento complementario la certificación de texto. Otras incluso dan testimonio notarial de la comunicación. Es ampliamente utilizado en el ámbito del derecho privado porque constituye prueba plena de haberse enviado una comunicación concreta, en la fecha reflejada, a un destinatario identificado.

TERMINALES DE DATOS

Un **equipo terminal de datos o ETD**, es aquel componente de un soporte filar o radioeléctrico que hace de fuente o destino de la información. Es decir es el origen o destino en una comunicación. Un ETD fuente por lo general contiene la información almacenada en un dispositivo de memoria que envía al ETD destino. La información llega inalterada y se almacena. Los ETD son empleados en la transmisión de datos de cualquier tipo (correo, voz, imágenes, etc.). El **ordenador personal o computadora** es el representante por antonomasia.

Pueden ser también elementos de este grupo un **terminal de videoconferencia, un transmisor de mensajes o una impresora.** La característica más reseñable de un ETD es por tanto la función que realiza y no sus componentes internos los que lo definen.

Todos estos medios pueden conectarse entre sí, formando parte de redes de conmutación de datos, constituyendo las famosas **redes informáticas**. Por lo tanto los ETD constituyen la base de los sistemas de telecomunicaciones e información actuales.

TERMINALES HÍBRIDOS SMARTPHONES

El elevado ritmo en los avances tecnológicos provocan una convergencia entre lo que hasta la fecha eran distintos tipos de equipos terminales. Un claro ejemplo son los conocidos como ***smartphone* o teléfonos inteligentes.**

Estos teléfonos son **híbridos entre terminales de datos y terminales telefónicos.** Se trata de teléfonos móviles construidos sobre potentes pero diminutos ordenadores y poseen la conectividad de un teléfono móvil convencional.

41. La UIT ha establecido diferentes normas:
    - Recomendación UIT-T T.2. 1974. Estos faxes tardan de cuatro a seis minutos en transmitir una página, con una resolución vertical de 98 líneas por pulgada, a una velocidad de 2.400 bps. Este tipo de faxes es ya obsoleto y no se fabrican más.
    - Recomendaciones UIT-T T.30 y T.32.1976. Estos faxes tardan 3 minutos en transmitir una página, con una resolución vertical de 100 líneas por pulgada a una velocidad de 9.600 bps. Aunque ya obsoleto y no fabricado más, se siguen empleando estos faxes al ser capaces de comunicarse con los faxes Grupo 3.
    - Recomendaciones UIT-T T.30 y T.4. 1980. Estos faxes tardan entre 6 y 15 segundos en transmitir una página a una velocidad de 14.400 bps.
    - Recomendaciones UIT-T T.563, T.503, T.521, T.6, T.62, T.70, T.72, T.411 a T.417. 1984. Ha sido diseñado para operar a más de 64 kbit/s sobre redes digitales RDSI. Su resolución depende de la recomendación T.6, que recoge todas las de la T.4 ampliándolas. Es capaz de recibir faxes provenientes de un fax grupo 3 o 2, aunque la comunicación debe pasar por un puente entre la red analógica y la digital.

Casi todos estos teléfonos inteligentes permiten además usar múltiples programas, acceso a Internet vía WiFi o 3G, gestión de agenda, reproductor de archivos multimedia, cámara fotográfica y de video digital, sistemas de navegación y tratamiento de ficheros.

EQUIPO TERMINAL RADIOELÉCTRICO TIPO RADIO

Es el soporte radioeléctrico clásico. Dentro de este grupo encontramos una subdivisión inicial, las **estaciones de radio** y los **radioteléfonos**.

Las **estaciones de radio** trabajan en **LF** y **HF**, es decir, lo que hemos llamado con anterioridad onda corta y onda media, estando concebidas para enlaces a larga distancia que requieren potencias de salida elevadas y sus modos de propagación son por onda ionosférica y por onda de tierra. Suelen trabajar en fonía o en datos a baja velocidad por lo que los servicios de telecomunicaciones que ofrecen son por tanto muy básicos. Voz, teletipo, algo de datos (que puede incluir correo electrónico, sólo texto plano), pero en cambio nos permite usar la "Grafía" o el Morse, que cuando el enlace es muy malo y no se entienden las comunicaciones de voz, incluso hoy día, puede ser extremadamente útil.

Aunque están en desuso el lector de este libro, **no deberá descartarlas y echarlas en saco roto**, pues en determinadas circunstancias nos podrán solucionar algún tipo de problema.

Estos tipos de enlaces se suelen usar todavía en zonas montañosas, o sencillamente zonas muy distantes. Son normales este tipo de comunicaciones en la marina mercante (sobre todo empleando el Morse) o desde aviones y helicópteros con sus bases terrenas. Tampoco podemos olvidar el papel tan importante que tuvo la radiodifusión en "onda corta", antes de la aparición de internet, para poder escuchar emisoras radio nacionales desde países remotos al nuestro.

En emergencias siguen teniendo su aplicación. Normalmente en intervenciones nacionales (lejanas de las sedes) o internacionales, se suelen usar estas radios para enlazar con las **Bases Retrasadas** situadas en los territorios nacionales de procedencia, aunque en determinadas catástrofes incluso se pueden llegar a usar para enlazar desde la **Base de Operaciones** con los mismos intervinientes.

La mayoría de las versiones de estas estaciones están pensadas para operar en **instalaciones fijas** como campamentos o edificios. La razón se debe a que necesitan unas fuentes de energía muy importantes para trabajar a altas potencias y así conseguir enlaces de cientos o miles de kilómetros si se sabe usar. Nos explicaremos. El "HF" precisa de unos conocimientos mucho mayores que los radioteléfonos que veremos a continuación de VHF/UHF, en las que con "apretar el PTT[42]" de la radio, prácticamente todo está hecho. Aquí **hay que conocer como se propagan las ondas y por tanto se precisa calcular una frecuencia óptima de enlace** para alcanzar con estas ondas al receptor. Para conseguir un alto rendimiento, aparte de personal especializado tal y como ya hemos señalado en otros capítulos, también precisan de espaciosos campos de antenas. Las antenas son muy grandes y de diversos tipos (varilla, hilo, dipolos, logo periódicas,...) pero en cambio aquí no necesitamos repetidores

Existen versiones para vehículos terrestres e incluso portátiles, cuyos alcances están limitados

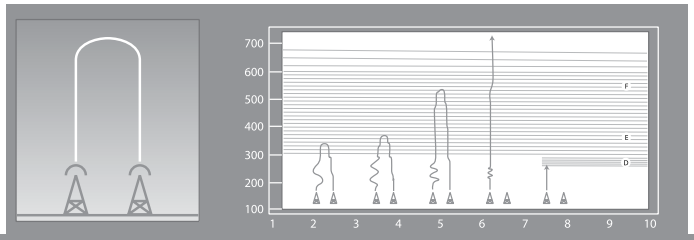
RADIO ONDA CORTA Y ONDA MEDIA

RADIO EXTERIOR DE ESPAÑA

SI ESTÁS LEJOS, SIÉNTENOS CERCA

Hasta la llegada de Internet y de los enlaces satelitales, el enlace HF y LF eran las bandas de trabajo a través de las cuales se establecían las comunicaciones.

42. **PTT:** *Press to talk*. Presione para hablar.



SONDADOR IONOSFÉRICO

EL IONOGRAMA

Esta técnica con pulsos comenzó a utilizarse en 1925 con un sistema desarrollado por el físico ruso, nacionalizado americano, Gregory Breit , quien junto a Merle A. Tuve, hicieron los primeros experimentos para medir el peso y la densidad de la ionosfera.

Para realizar las medidas, emitieron pulsos cortos de ondas de radio, y analizaron las ondas reflejadas que recibían. Esta técnica representó un gran paso para el desarrollo del radar. El producto final de un sondeo vertical es el ionograma, que es la representación del retardo del eco en relación con la frecuencia utilizada.

técnicamente por la potencia[43] que puede suministrar las baterías del vehículo o de la radio portátil. También influye, y mucho, el tipo de antena que se instale en la plataforma vehicular o que puede portar el hombre o mujer encargada de su transporte.

Una estación curiosa, poco común, es el **sondador ionosférico**. La ionosonda o sondador ionosférico es simplemente un radar de HF. La técnica de medida está basada en enviar pulsos electromagnéticos a diferentes frecuencias hacia la ionosfera, medir el retardo del eco y de esta forma evaluar las posiciones de las capas de la ionosfera. Suelen trabajar por parejas, una estación máster y otra esclava que aun estando separadas miles de kilómetros, tras sondear la ionosfera, determinan las frecuencias óptimas de enlace entre ellas para cada momento del día.

Del mismo modo podemos encontrar estaciones HF instaladas sobre aeronaves cuyas antenas van fijadas al fuselaje y de potencias similares a las instaladas en vehículos terrestres. Sin embargo aquí los alcances suelen ser mucho mayores una vez que la aeronave, helicóptero o avión, están en vuelo. Al elevar el horizonte las pérdidas que se producen en una estación terrestre al chocar las ondas con el terreno y obstáculos adyacentes como edificios y/o árboles, son mucho menores.

Las estaciones radio instaladas en barcos son muy similares a las utilizadas en infraestructura fija terrestre por tener características de disponibilidad de espacio y de potencia muy parecidas.

En este apartado se encuentran incluidos los famosos **servicios de radiocomunicaciones marítimas y aeronáuticas,** en el que existen unas frecuencias en las que siempre hay estaciones a la escucha (incluyendo buques y aviones) y que se pueden utilizar para comunicar mensajes vitales en caso de emergencia.

Estas comunicaciones radio seguirán siendo siempre el pilar de las telecomunicaciones radio de emergencia a media y larga distancia como se demostró en los terremotos de Chile o Perú donde los radioaficionados asumieron la responsabilidad de mantener al mundo informado.

Los **radioteléfonos, o radios portátiles** (manpack) por su parte trabajan en **VHF/UHF**, pensados para enlaces de corto alcance, precisando potencias[44] menores y propagándose a través de onda de tierra y por onda espacial. Pueden trabajar en fonía o en datos proporcionando servicios muy básicos y son explotados normalmente por los usuarios **sin necesidad de una formación compleja**. Son por lo tanto de fácil manejo, poco peso y volumen que permiten que los usuarios lo lleven encima, y escaso consumo, lo que permite que sean alimentados con pequeñas baterías, en algunos casos desechables.

Una de las características más comunes es su **corto alcance** si no entran en una red de repetidores o estaciones base, tal y como realizan los terminales digitales de radiocomunicación móvil que corresponden al concepto de **radiocomunicaciones móviles digitales.**

43. Para que el lector tenga una referencia en cuanto a la potencia de las estaciones radio, tómese como referencia que una estación HF portátil (manpack), es menor de 50W (Vatios). Las de los vehículos terrestres y aéreos alrededor de 100W. Mientras que las fijas y marítimas oscilan entre los 100 y 1000W, pudiendo incluso ser superiores.

44. Las potencias de estos equipos en portátil varían entre los 5 y 15 vatios. En plataformas vehiculares rondan los 50W.

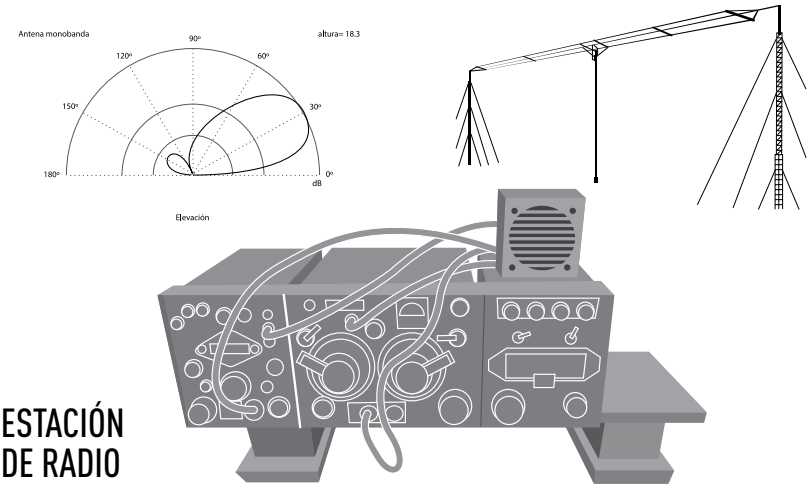
Podríamos decir que este sistema de **redes radio de trunking** permite **compartir un mismo canal de la infraestructura terrestre entre varios usuarios** sin que se mezclen las conversaciones y sin pérdida de información. Permite cubrir grandes zonas de terreno (incluso una comunidad autónoma, una región o un país completo) gracias a las estaciones base repetidoras de radio.

Las principales tecnologías por el momento, a falta de la entrada en el mercado de la **tecnología LTE**[45], son **TETRAPOL** (solución propietaria de la empresa EADS) y **TETRA** (*Terrestrial Trunked Radio*), estándar europeo con más de 1400 redes desplegadas en más de 100 países de todo el mundo, así como variadas tecnologías de radio privada analógica ya obsoletas y en proceso de reemplazo.

El lector puede imaginarse el **coste astronómico** de estos sistemas, ya que son proporcionales a la zona a cubrir. Sirva como referencia que para cubrir una zona equivalente al territorio continental de Portugal, se precisan más de 600 estaciones-base para garantizar una cobertura cercana al 90% del territorio.

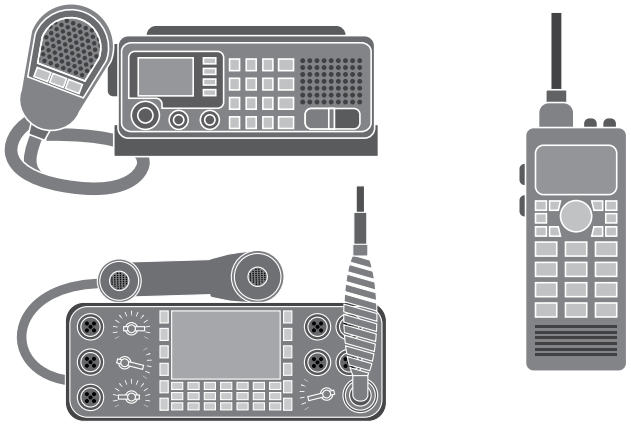
En España existen numerosos ejemplos de exitosas redes de este tipo. Podemos mencionar la

45. La tecnología LTE *(Long Term Evolution)* es un nuevo estándar. Definida para unos como una evolución de la norma 3GPP UMTS (3G), y para otros como un nuevo concepto de arquitectura evolutiva (4G). La especificación LTE soporta un gran rango de frecuencias y proporciona un alto rendimiento a altas velocidades habiendo sido ya adoptada por la telefonía móvil. En estos momentos los fabricantes de PMR están estudiando la evolución y se plantea la duda entre las tecnologías WiMAX, la propia LTE, o una mezcla entre las dos. Todo indica que en el futuro las PMR utilizarán una solución basada únicamente en LTE ya que en los EE.UU. la decisión ya se ha tomado para banda ancha en todo el país y LTE fue la elección, por lo que no tendría sentido usar otra tecnología en Europa.

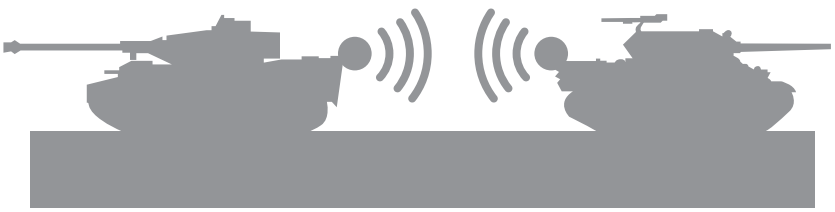


ESTACIÓN DE RADIO

RADIOTELÉFONOS



RADIO VHF. ANTECEDENTES



INICIOS DE LA RADIOCOMUNICACIÓN MÓVIL

Los ingenieros militares de la Werhmacht alemana descubrieron que las ondas de VHF en el rango de 18 a 80 Megahertzios, eran muy apropiadas para seguir las ondulaciones del terreno siempre y cuando se utilizaran las antenas y potencias adecuadas.

Al estar así equipados, los jefes de los carros de combate recibían las órdenes a distancia y las novedades o informes de lo acontecido en los combates. De esta forma podían corregir los movimientos de las tropas o prestarles el apoyo de fuego o aéreo necesario donde fuera requerido.

REDES TRUNKING

Este tipo de tecnología permite compartir vías de comunicación entre estaciones base, añadiendo además toda una serie de beneficios añadidos como son la securización de las comunicaciones y todas las ventajas inherentes a la digitalización de las señales.

Red SIRDEE (Sistema Integrado Radio Digital de Emergencias del Estado) sobre tecnología TETRAPOL, usada por Guardia Civil, Cuerpo Nacional de Policía y la Unidad Militar de Emergencias, con más de un 95% de cobertura de todo el Territorio Nacional, incluyendo aguas territoriales.

Muchas Comunidades Autónomas aparte de las ya mencionadas con anterioridad han optado por la tecnología TETRA, para cubrir sus zonas con resultado muy positivo. Es el caso de Ceuta, Melilla o la Región de Murcia. En otros países de nuestro entorno como Portugal, Irlanda o Dinamarca sí que se ha optado por una red nacional única y compartida por todos los cuerpos de seguridad y servicios de emergencia. Algo que sin duda parece más lógico.

Estos sistemas de **gran fiabilidad,** están diseñados para trabajar en **circunstancias adversas y en modo degradado.** Esto sin duda es un seguro de vida para garantizar el enlace entre intervinientes y la base o centro de control de procedencia.

Los terminales portátiles son pequeños y livianos, tipo "***walkie***" y los vehiculares son de tamaño similar a un equipo de música de un coche. Son los equipos radio más utilizados por los equipos de intervención para enlazar entre sí. La forma normal es establecer enlaces cuando hay "visión directa". Esto no significa que sea mandatorio que se vean físicamente el emisor y el receptor, sino que las ondas emitidas por el transmisor llegan directamente a la antena del receptor. Los radioaficionados también trabajan de manera prolija en estas bandas.

Existen radioteléfonos instalados sobre plataformas aeronáuticas y marítimas con características casi idénticas a las portátiles. La diferencia más sustancial consiste en que en estas instalaciones, al no tener que llevarlas nadie encima, se les suele añadir un amplificador que proporciona mayor potencia y por tanto un mayor alcance.

EQUIPO TERMINAL RADIOELÉCTRICO TIPO RADIOENLACE

Se puede definir al terminal radioenlace, como un sistema de telecomunicaciones que se establece entre dos puntos fijos situados sobre la superficie terrestre, que proporcionan una capacidad de enlace, con características de calidad y similares a la proporcionada por el soporte filar. Típicamente estos enlaces se explotan entre los 800 MHz y 42 GHz. Se los conoce también por **enlaces microondas**.

En realidad el radioenlace lo que crea es un "cable virtual" entre dos puntos distantes, por lo que también se le conoce como **cable hertziano.** A través de ese cable virtual conformado por un soporte radioeléctrico en vez de filar se pueden montar una o varias comunicaciones simultáneas dependiendo de los equipos con los que se asocie el radioenlace. Un radioenlace está constituido por equipos de radio (transceptores), antenas y elementos de supervisión. Si es necesario puede haber incluso repetidores intermedios.

Los enlaces se hacen básicamente entre puntos que guarden entre sí la denominada **línea de visión directa**[46], por lo que suelen

46. La línea de visión directa es conocida como la LOS (*Line Of Sight*, por su acrónimo ingles), es decir el enlace microondas se realiza sólo si existe una vista del receptor. La LOS implica que la antena en un extremo del radio enlace debe poder "ver" la antena del otro extremo.

estar situados en puntos altos de la topografía. Es muy importante en los radioenlaces el estudio de los obstáculos que haya en el medio de la trayectoria (que hay veces que son incluso beneficiosos y es la llamada **ganancia por obstáculo**. Cosas de las "meigas" asociadas a la propagación). También es muy importante el llamado **arranque**, entendido como el espacio libre de obstáculos alrededor de las antenas para que pueda salir el lóbulo de radiación al completo.

Por lo tanto el diseño de un radio enlace supone cuatro pasos básicos: primero, la elección del sitio de instalación; segundo, estudio del perfil topográfico entre origen y destino; tercero, el cálculo de la altura del mástil para la antena y cuarto, el cálculo completo del radio enlace que incluye el estudio de la trayectoria del mismo y los efectos a los que se encuentra expuesto.

Los radioenlaces establecen una comunicación del tipo dúplex, de donde se deben transmitir dos portadoras moduladas: una para la transmisión y otra para la recepción. Al par de frecuencias asignadas para la transmisión y recepción de las señales, se denomina **radio canal**.

Atendiendo al tipo de señal moduladora los radioenlaces pueden ser analógicos y digitales. Estos últimos presentan mayor homogeneización de los materiales, mejor calidad de transmisión y fiabilidad, y un menor coste que los analógicos.

Estos equipos precisan ser utilizados por **personal especializado,** al menos en su instalación inicial.

EQUIPO TERMINAL RADIOELÉCTRICO TIPO SATÉLITE

Estos equipos terminales radioeléctricos para poder ser utilizados precisan de un **repetidor de señal** intermedio que es precisamente el satélite que está en algún punto del espacio relativamente cercano a la atmósfera. Esta situación elevada del satélite permite asegurar la visión directa con cualquier terminal situado en tierra.

La frecuencia de trabajo suele ser **SHF**. Proporcionan enlaces de gran capacidad a grandes distancias, con independencia del tipo de terreno, y del estado de la infraestructura de telecomunicaciones terrena de la zona afectada por la emergencia. Los servicios que ofrecen son en correspondencia con el ancho de banda del terminal en cuestión. Pueden ir desde solamente fonía, hasta una videoconferencia en tiempo real, pasando por el transporte de datos de cualquier tipo.

Si el satélite tiene visión directa con los terminales situados en el suelo el enlace es factible. Estas "estaciones terrenas" pueden ser terminales fijos y transportables.

Los **terminales fijos**, también llamados **estaciones de anclaje**, tienen como misión servir de interfaz entre las telecomunicaciones transmitidas por el satélite y los sistemas fijos de telecomunicaciones terrestres. Es decir, nos van a facilitar el integrarnos en cualquier red telefónica nacional y poder hablar con cualquier abonado telefónico del mundo.

Por el contrario los **terminales transportables** se pueden desplegar en cualquier tipo de plataforma móvil terrestre, aérea o marítima, y por supuesto existen infinidad de modelos portátiles (manpack).

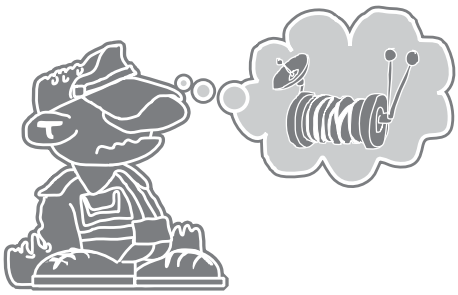
Para todos los terminales, fijos y transportables, hasta hace unos años era obligatorio pararse y enlazar desde la posición estática. Las últimas incorporaciones técnicas apuntan a la capacidad de enlazar con los terminales en movimiento. Son los llamados "***Sat on the Move***" (SOTM). Las primeras plataformas que incorporaron esta posibilidad fueron los barcos, y poco después se le han ido uniendo aeronaves y vehículos terrestres.

Además la utilización de los terminales móviles o transportables es muy similar al del uso de un teléfono móvil al que estamos tan acostumbrados, por lo que no precisa una formación compleja. No ocurre así con las estaciones de anclaje, que sí precisan de personal experto para su operación y puesta en servicio.

Existen en la actualidad dos tipos de proveedores de servicios satélite:

- PROVEEDORES DE SERVICIO SATÉLITE COMERCIALES:

  Son empresas que han puesto constelaciones de satélite en órbita y que alquilan sus servicios a los usuarios. Aquí



HISTORIAS DE "LA MILI"

Una de las bromas o "novatadas" más comunes que se le hacia a los reclutas cuando se incorporaban a filas en los Regimientos de Transmisiones Estratégicas que utilizaban este tipo de radioenlaces, era hacerles ir a buscar al Cuerpo de Guardia, y pedirle al Oficial de servicio las "bobinas" para enrollar el "cable hertziano".

SATÉLITES VS CABLES SUBMARINOS

ROBUSTEZ DE LOS CABLES SUBMARINOS

Los satélites de comunicaciones cubren sólo parte de la demanda de las telecomunicaciones que se producen entre continentes, por la tanto son los cables submarinos de fibra óptica la base en la red mundial de telecomunicaciones.

La fibra óptica que lleva la información, está protegida por vaselina, tubos de aluminio, policarbonato, una barrera resistente al agua, alambres de acero trenzado, cinta de tereflalato de polietileno y una cubierta de polietileno.

encontramos las archiconocidas **Inmarsat, Globalstar, Iridium y Thuraya**[47]**.** Existen otras opciones como el sistema **VSAT**[48]. El servicio es aceptable y ofrecen voz y datos. La videoconferencia o el acceso a Internet es posible aunque con limitaciones de velocidad (no podemos esperar tener las facilidades de nuestra casa o de nuestra oficina). Son los más usados por las organizaciones de emergencias. Son muy caros, tanto la adquisición del terminal portátil, como el tráfico. Suelen dar un buen resultado salvo ocasiones excepcionales en los que los proveedores se ven saturados como ocurrió por ejemplo en Haití, dónde hubo una concentración tal de agencias usando los mismos proveedores que el servicio se vio muy deteriorado.

La mayoría de los sistemas funcionan con procedimientos de facturación mediante **tarjetas SIM** (módulo de identidad del usuario), que facilitan el control y la atribución de los costos de comunicación y de itinerancia internacional por las redes de telefonía móviles con las que los proveedores de servicio hayan establecido los correspondientes acuerdos, pues muchos de estos sistemas suelen ser **duales**. Como las tarifas son relativamente altas, particularmente las que corresponden a las conexiones entre los terminales de satélite de distintos sistemas, las redes públicas por satélite resultan convenientes sólo para la fase de respuesta inicial, pero no deberían utilizarse como medio principal de comunicación en las operaciones a largo plazo.

- PROVEEDORES DE SERVICIO SATÉLITE GUBERNAMENTALES

En este caso en vez de una empresa es una nación la que ha corrido con los gastos de poner en órbita sus satélites para satisfacer necesidades de los respectivos gobiernos. En muchos casos corresponde a los mal llamados "**satélites militares**" porque en muchos países son las Fuerzas Armadas los que hacen uso de ellos. En ocasiones, para rentabilizar la inversión, suelen alquilar servicios a organizaciones ajenas al estado, reuniendo una serie de condiciones de uso y seguridad. La mayor diferencia entre los gubernamentales y los comerciales es que en los primeros los usuarios pueden elegir de una manera inmediata y flexible los servicios de telecomunicaciones o de información, así como las velocidades a implementar para cada uno de ellos. Sin embargo esta opción no suele existir para los proveedores comerciales, y si existe suele ser a precio de oro.

47. Hay otros sistemas que ofrecen cobertura regional, por ejemplo en América del Norte (Motient) y en Asia (AcsS).
48. Los sistemas VSAT, o "terminales de muy pequeña abertura", son redes de comunicación por satélite que permiten el establecimiento de enlaces entre un gran número de estaciones remotas con antenas pequeñas (de ahí el nombre **VSAT:** ***Very Small Aperture Terminals***) con una estación central generalmente conocida como HUB. Al abonarse a una empresa proveedora de servicio VSAT se adquiere un conjunto de canales durante un periodo determinado. Ningún otro usuario podrá compartir esos canales y el abonado está seguro de utilizarlos incluso cuando sistemas como la Red Telefónica Pública Conmutada (RTPC) y el sistema móvil por satélite estén congestionados. Este tipo de sistemas está principalmente orientado a la transferencia de datos entre las unidades remotas y los centros de proceso conectados al HUB o estación de anclaje. También son apropiadas para la distribución de señales de vídeo y, en algunos casos, se utilizan para proporcionar servicios telefónicos entre las estaciones remotas y la RTPC a la que se accede a través de la estación de anclaje.

LA VISIÓN MÁS COMPLETA DE LA "TEORÍA DE LA COMUNICACIÓN TECNOLÓGICA"

Sigue faltando "chatarrería". Es decir, puede que al lector le siga faltando equipación. Si es su caso, no se preocupe que a continuación vamos a exponer algunos equipos más y donde iría, aunque siempre dentro de nuestra figura de la teoría de la comunicación.

EQUIPOS TERMINALES DE LÍNEA

En ocasiones nos podremos encontrar con aparatos instalados en los extremos de los soportes filares. Son los **equipos terminales de línea o de cable** convencional de pares **(ETL).** Éste es empleado para la transmisión y recepción de señales a través de líneas de conductor metálico. En caso de utilizar Fibra Óptica, el equipo **terminal de fibra óptica (TOL)** se emplea para el tratamiento de señales eléctricas a través de fibras, previa conversión de las mismas en señales ópticas. Existen los equivalentes equipos terminales para los cables coaxiales.

Los **Equipos Terminales de Línea (ETL)** pueden ser ópticos o eléctricos y su función es la de adaptar las señales al medio de transmisión a ser utilizados. Consta además de los elementos de supervisión de repetidores o regeneradores así como, en caso de ser necesario, el equipo necesario para alimentar eléctricamente (telealimentar) a estos repetidores o regeneradores intermedios cuando ello se hace a través de los propios conductores metálicos de señal.

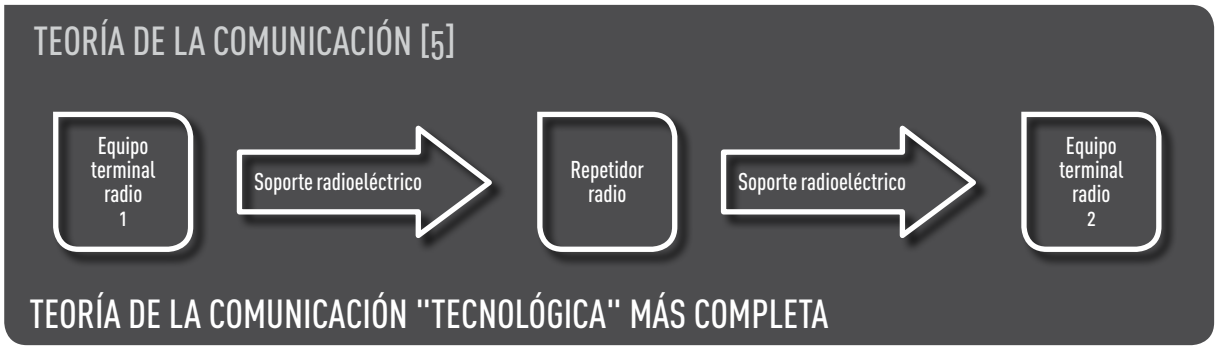
REPETIDORES

Son los equipos que permiten incrementar el alcance de otros medios y salvar obstáculos del terreno. Atendiendo al soporte empleado se clasifican en:

- **Repetidores filares:** amplifican y regeneran las señales que reciben a través del cable de cobre, cable coaxial o fibra para hacerla llegar a su destino.
- **Repetidores radio:** permiten la retransmisión de señales de radio.
- **Satélites de telecomunicaciones:** permiten la transmisión a largas distancias entre sus usuarios situados en la tierra.

MEDIOS DE ADAPTACIÓN

Sirven para unir un equipo terminal con un soporte de transmisión determinado.



A finales del siglo XX se pusieron de moda los **moduladores/demoduladores (módem)** que eran necesarios para unir un terminal de datos (ordenador) con un soporte filar (par de cobre telefónico de los hogares).

También suelen ser útiles los **integradores** que permiten unir entre sí dos soportes de distinta naturaleza, como soportes radioeléctricos con soportes filares (integradores radio-hilo), o dos soportes filares diferentes (conmutadores circuitos).

Otro dispositivo relativamente común es el **mando a distancia** que permite la utilización de un terminal radioeléctrico a cierta distancia de él. Son por ejemplo utilizados por las emisoras de radiodifusión para llevar la señal desde los estudios, que suelen estar en el centro de una ciudad, hasta la antena de emisión que normalmente se encontrará a muchos kilómetros en una zona propicia que permita alcanzar al mayor número de oyentes posible.

MEDIOS DE CONMUTACIÓN

Son los aparatos que permiten sacar el máximo provecho al circuito que se establece entre dos puntos, emisor y receptor, de tal manera que se pueden introducir simultáneamente distintas transmisiones.

Las **centrales de conmutación telefónicas** son las más conocidas, aunque existan otras como las **centrales de conmutación telegráfica** que están ya en desuso. También están en decadencia los **conmutadores de datos**[49] que permiten la transmisión entre dos terminales de datos cualesquiera. Hoy

TEORÍA DE LA COMUNICACIÓN [7]

TEORÍA DE LA COMUNICACIÓN "TECNOLÓGICA" MÁS COMPLETA

día están tomando preponderancia las **centrales IP híbridas** que permiten conmutar sobre protocolo IP terminales telefónicos, telegráficos y de datos.

Las centrales constituyen el elemento básico de los sistemas telefónicos y también el más vulnerable a las averías durante una catástrofe debido a su tendencia a la sobrecarga[50], sin contar los posibles daños que pudiera recibir.

Con la llegada de las redes informáticas se han puesto de moda los **equipos de direccionamiento de terminales de datos**, que son los equipos encargados de poner en comunicación terminales de datos pertenecientes a la red. Nos referimos a los concentradores o **HUB**, puentes o ***bridge***, conmutadores o ***switches***[51] y a los ***routers***.

Los enrutadores (*routers*) permiten la conmutación entre terminales de datos de dos o más redes de área local (con protocolos similares o diferentes) o de distintos segmentos de una misma red de área local, con la particularidad de seleccionar automáticamente la ruta más idónea de las disponibles en su salida.

Aunque no es técnicamente correcto se puede hacer una aproximación para los menos expertos en estas lides, diciendo que un router para los ordenadores es el equivalente a una central telefónica para los teléfonos. Las centrales utilizan números de abonado (número de teléfono) para reencaminar las llamadas, mientras que los routers utilizan direcciones IP.

MEDIOS DE SUPERVISIÓN Y CONTROL

Son aquellos que permiten a los Responsables TIC ejercer el **control sobre los sistemas que proporcionan el enlace.** No vamos a profundizar pues se escapa del objetivo de este libro.

MEDIOS AUXILIARES

Como medios auxiliares pueden considerarse aquellos que, no estando comprendidos en los apartados anteriores, facilitan la explotación de los medios de telecomunicaciones, como por ejemplo las **plantas de energía, grupos electrógenos o cargadores de baterías.**

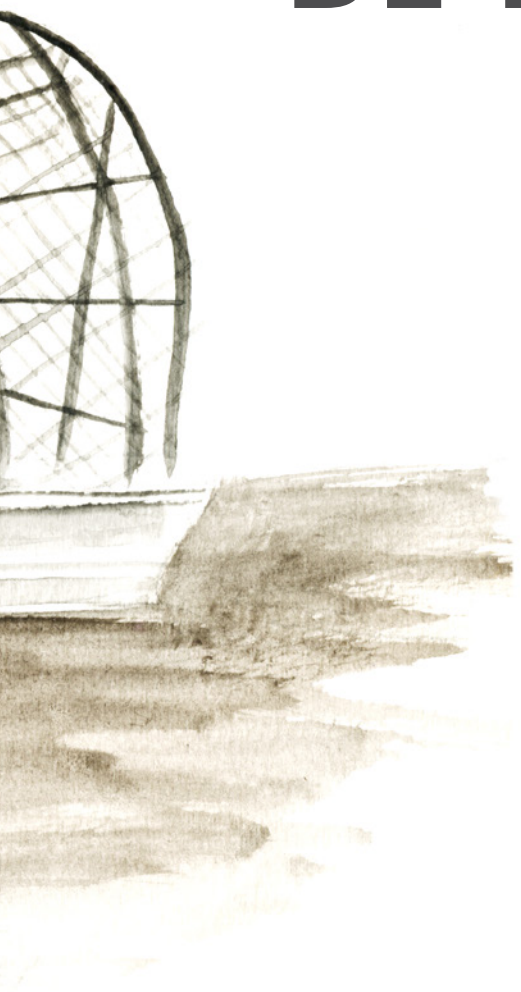
El mayor apagón en la historia de los EE.UU. se produjo el 14 de agosto de 2003 y dejó a aproximadamente 50 millones de personas sin electricidad. Los apagones pueden producirse en cualquier momento, y mucho más en el trascurso de una emergencia por lo que es importante para un responsable TIC estar preparado.

49. Las técnicas de conmutación que suelen utilizarse en las redes de transmisión de datos son básicamente tres:
    - Conmutación de Circuitos.
      Esta técnica permite que el terminal emisor se una físicamente al terminal receptor mediante un circuito único y especifico que solo pertenece a esa unión. El circuito se establece completamente antes del inicio de la comunicación y queda libre cuando uno de los terminales involucrados en la comunicación la da por finalizada.
    - Conmutación de Mensajes.
      Se basa en el envío de un mensaje que el terminal emisor desea transmitir al terminal receptor a un nodo o centro de conmutación en el que el mensaje es almacenado y posteriormente enviado al terminal receptor o a otro nodo de conmutación intermedio, si es necesario. Este tipo de conmutación siempre conlleva el almacenamiento y posterior envío del mensaje, lo que origina que sea imposible transmitir el mensaje al nodo siguiente hasta la completa recepción del mismo en el nodo precedente.
    - Conmutación de Paquetes.
      La conmutación de paquetes surge intentando optimizar la utilización de la capacidad de las líneas de transmisión existentes. Para ello es necesario disponer de un método de conmutación que proporcionará la capacidad de transmisión en tiempo real de la conmutación de circuitos y la capacidad de direccionamiento de la conmutación de mensajes.
50. En una zona residencial, la central se dimensiona de manera que pueda recibir simultáneamente llamadas de entre el 5% y el 15% de los abonados. Cuando la carga es superior a la prevista, la central corre el peligro de quedar inutilizada por la sobrecarga.
51. Equipos de direccionamiento de terminales de datos:
    - Concentrador (HUB): se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola.
    - Puente de red (*bridge*): conecta dos redes como una sola red usando el mismo protocolo de establecimiento de red.
    - Conmutador (*switch*): envía la información por todos sus puertos, al igual que un HUB; cuando hay más de un ordenador conectado a un puerto de un *switch*, éste aprende sus direcciones de tarjeta de red (dirección MAC) y cuando se envían información entre ellos no la propaga al resto como si lo hace el HUB.


20239
GUARDA COSTA

CAPÍTULO 6

SISTEMAS DE INFORMACIÓN DE EMERGENCIAS (SIE)



El escenario actual de las emergencias que combina un mundo plenamente tecnológico con potentes sistemas de telecomunicaciones electromagnéticas da lugar, en ocasiones, a un exceso de información que es recibida por los responsables de la gestión. Por otro lado, simultáneamente la sociedad actual demanda una respuesta inmediata por parte de los dirigentes lo que hace disminuir progresivamente también el tiempo que los gestores de las emergencias tienen para poder decidir.

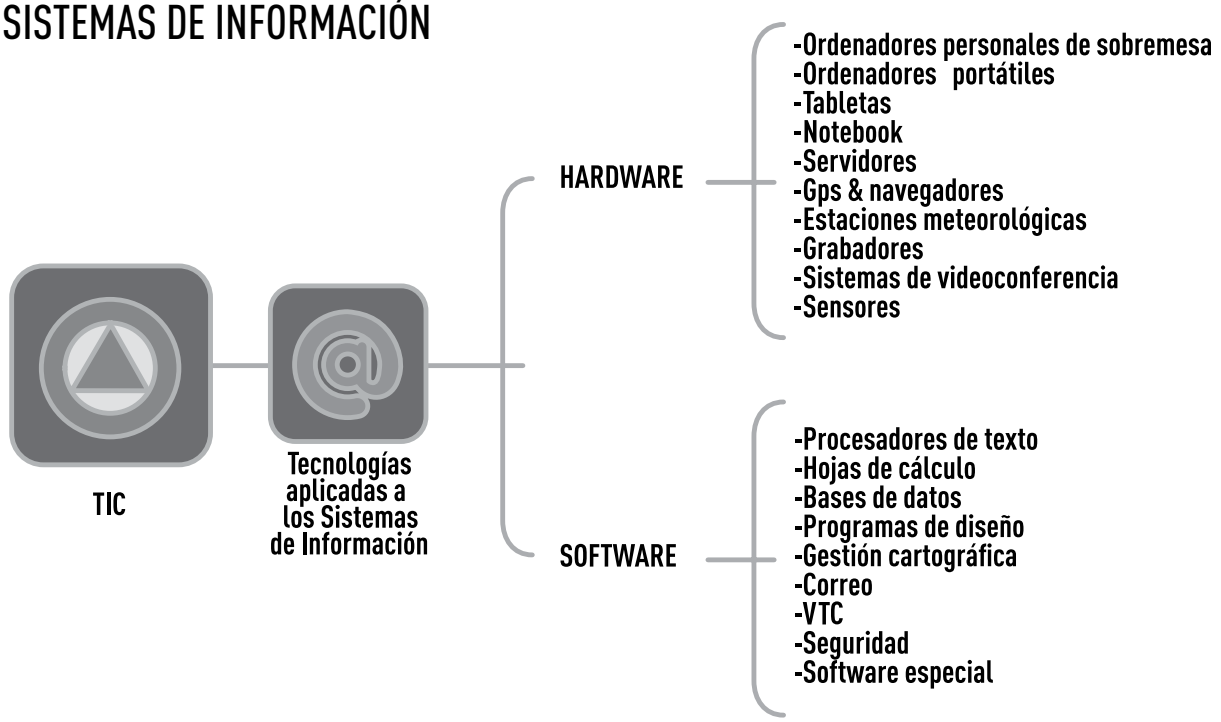
Esta **incompatibilidad entre el poco tiempo disponible y la gran cantidad de datos** pendientes de procesar exige herramientas que faciliten los procesos de selección entre lo banal y lo trascendente, entre lo accesorio y lo fundamental. Cuando dimos nuestra definición de enlace hablamos de procedimientos y medios que debíamos poner en práctica para que los usuarios **pudieran tratar la información.** De entre las herramientas empleadas destacan los **Sistemas de Información (SI)** como una de las más importantes.

Un Sistema de Información de Emergencias (SIE) debe estar diseñado para poder cumplir con los objetivos estratégicos de la organización y por tanto el **objetivo principal** de éstos debe ser el de procesar la información que entra a una organización y permitir su análisis, almacenamiento y presentación, suministrando a los directores de la gestión de la emergencia la información necesaria,

en el tiempo oportuno, para tomar las decisiones más apropiadas en cada momento.

Es evidente por tanto que la información **mejora el proceso de toma de decisiones** con muchas menos incertidumbres que hace unos años. Para ser efectivo, el gestor de una emergencia necesita recabar suficiente información, a fin de entender sucesos ya pasados, identificar lo que está ocurriendo ahora y predecir a tiempo lo que podría suceder en el futuro.

SISTEMAS DE INFORMACIÓN



Por todo lo anterior, se puede entender que la utilización de **sistemas de información aplicados a la gestión de emergencias** o catástrofes es importante ya que es una herramienta que **acelera los tiempos para volver a una situación de calma.** El personal directivo de una catástrofe puede conocer de forma más oportuna las actuaciones de los intervinientes sobre el mismo terreno, o por ejemplo, lo que los damnificados necesitan de manera más apremiante.

No es que nos gusten en exceso, o mejor dicho, **no nos queremos sumar al grupo de "talibanes de las TIC"** que los tienen **sobrevalorados**. Los Sistemas de Información de Emergencias (SIE), en su justa medida, son muy útiles siempre y cuando agilicen las labores de los usuarios y su uso no obligue a las personas a trabajar de una manera diferente a la que se contempla en el **Concepto Operativo**[52] , que por otra parte es para lo que dicho SIE ha debido ser diseñado.

52. Ver Capítulo 3: diseño del sistema

CÓMO DEBE SER LA INFORMACIÓN SUMINISTRADA POR UN SIE

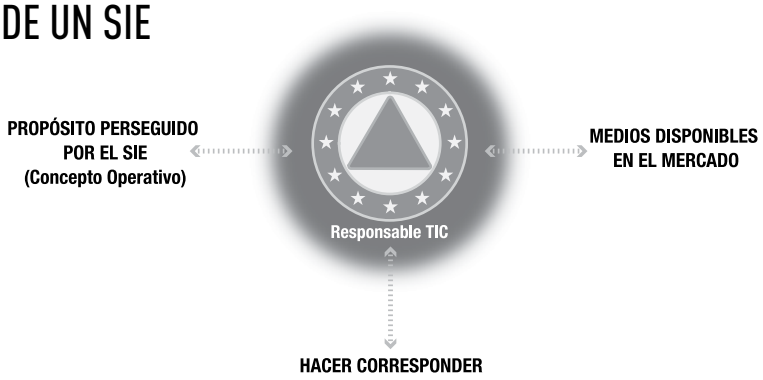
Un SIE debe ser autorregulable y optimizable, es decir en permanente estado de adaptación al entorno de la organización de socorro en el que está instalado. La flexibilidad y facilidad de adaptación debe ser el punto fuerte de los sistemas de información para facilitar el flujo de información dentro de la organización.

Además la información proporcionada por el sistema, debe cumplir con los siguientes requisitos ineludibles:

- **Veracidad:** es imprescindible que los hechos comunicados sean un fiel reflejo de la realidad.
- **Oportunidad:** con el fin de lograr el control de la situación y así tener opción a tomar medidas correctivas en caso de necesidad.
- **Cantidad:** tomar cualquier decisión es sumamente difícil en el transcurso de una emergencia. Tanto la falta de suficiente información, como el exceso de la misma, nos abocará a decisiones erróneas e inoportunas.
- **Relevancia:** la información que se le facilite al usuario de un SIE debe estar relacionada con sus tareas y debe ser del nivel de sus responsabilidades.
- **Completa:** sin pérdidas deliberadas o accidentales.

Cualquier SIE que presente información fuera de estos parámetros obligaría desde nuestro punto de vista a la revisión completa del propio Sistema de Información.

IMPLEMENTACIÓN DE UN SIE



Muchas de las organizaciones de emergencias que trabajan a lo largo y ancho del mundo **no cuentan con un sistema de información** informatizado y sin embargo muchas de ellas realizan unas labores encomiables manteniéndose durante muchos años como referentes internacionales. Puede sonar extraño ya que anteriormente comentamos que los sistemas de información son una herramienta necesaria para la toma de decisiones, pero **¿acaso no se pueden tomar decisiones sin tener que contar con un sistema de información de última generación?** Pues la respuesta es **definitivamente sí,** ya que como mencionamos anteriormente los sistemas de información brindan un apoyo a la toma de decisiones; es decir, la importancia de los sistemas de información no es el contenido de éste sino el grado de uso que se les dé a los datos recopilados y las acciones que se tomen en base a la información obtenida en las diferentes fases de la emergencia. Por lo tanto **los SIE, por sí solos, no tienen valor si no se les complementa con acciones** que permitan precisamente lo que buscan, mejorar los resultados de la organización.

Es difícil justificar la inversión en un sistema de información para una organización que no lo use. Se hace además más complicado si tomamos en cuenta que se han venido tomando decisiones correctas (las organizaciones funcionan sobradamente bien), por lo cual no se requiere invertir en algo que no está haciendo falta hasta este momento. A los beneficios propios de la rapidez de gestión de la información y los diferentes modos de presentación que nos ofrecen los SIE debemos añadir otro punto muy importante que es el de la **interoperabilidad**.

Los sistemas de información juegan un **papel muy importante en el intercambio de información entre organizaciones.** Esta necesidad se acentúa cuando entra en juego el hecho de que salvar vidas se apoya en una información veraz y oportuna. La idea de contar con más potencial, entendiéndolo como la capacidad de tener más información proporcionada por otras organizaciones, implica contar con herramientas que permitan su gestión e integración en el sistema propio.

COMPONENTES DE UN SIE

Un Sistema de Información de Emergencias es el **conjunto integrado de personal, medios y procedimientos,** organizado de tal forma que permita la obtención, tratamiento, presentación y almacenamiento de la información para apoyar las operaciones y la toma de decisiones durante una emergencia.

Veamos dichos componentes en detalle:

- El **personal**. Aquí incluimos tanto al usuario que los explota o utiliza, y al staff técnico TIC encargado de su correcto funcionamiento.
- Los **medios**, integrados a su vez por componentes **hardware** (servidores, estaciones de trabajo, electrónica de red...etc.), y componentes **software**, que serán "la materia gris" del sistema (bases de datos, sistemas operativos, firmware, aplicaciones informáticas...etc.).
- Por último los **procedimientos**, que regulan el uso por parte de los usuarios, y la gestión del sistema por parte del personal técnico.

Los SIE corren sobre Sistemas de Telecomunicaciones, que en nuestro caso los vamos a tomar como un subsistema, aunque cada vez es más difícil distinguir donde acaba el Sistema de Telecomunicaciones y donde empieza el de Información.

TIPOS DE SISTEMAS DE INFORMACIÓN DE EMERGENCIAS (SIE)

En el ámbito de las emergencias podemos distinguir **dos grandes grupos principales**. Aparte podemos distinguir un número importante de subsistemas que suelen estar presente en cualquiera de los dos grupos que vamos a definir.

Ambos tipos de sistemas hacen uso de paquetes ofimáticos integrados, compuestos por procesadores de texto, hojas de cálculo, bases de datos, agendas, gráficos, y otras que tienen como finalidad servir de soporte a los procesos administrativos propios del trabajo de oficina, mediante la automatización de determinadas funciones.

Los dos grandes grupos a los que hacíamos mención son los **SIE específicos y los integrados**. Pasemos a tratarlos.

SIE ESPECÍFICO DE ORGANIZACIÓN

La mayor parte de los servicios de extinción de incendios, Fuerzas y Cuerpos de Seguridad del Estado o autonómicos, policías locales, etc, han apostado, en mayor o menor medida, por algún software de gestión que, soporte, agilice y facilite sus actuaciones y el control de sus recursos.

Estos sistemas suelen estar **diseñados *ad hoc*.** Están hechos a la medida de la organización y sirven para controlar los **procesos de trabajo específicos** de cada organismo. Aunque existen componentes comunes, todos ellos precisan saber el lugar donde ocurre el incidente, contactar con sus elementos intervinientes, conocer qué recursos hay en la zona o están en vías de llegar, y por supuesto cualquier otra información que pueda ayudar a realizar sus tareas.

SIE INTEGRADO

Lo que inicialmente eran organizaciones de socorro aisladas se han visto superadas por la aparición de **entes superiores** de coordinación de las emergencias. Efectivamente, nos estamos refiriendo principalmente a los **Centros de Emergencias 112,** ya mencionados en el capítulo 4.

Estas agencias han apostado por abarcar casi todas las emergencias, y engloban casi siempre las llamadas relativas a seguridad ciudadana, atención sanitaria, extinción de incendios, rescate y salvamento y de protección civil. Este hecho ha llevado parejo el hecho de que **en ellos se integre personal de cada una de las organizaciones, que en muchos casos traían su propio SIE específico de organización.**

Las **agencias 112** pueden tener variaciones en su constitución pero se caracterizan entre otras cosas por realizar la atención a llamadas de emergencia de los ciudadanos en su ámbito territorial, permitir la localización inmediata del llamante, estar adaptados a discapacitados (aceptan atención vía chat, Skype, SMS o Whatsapp), o estar diseñados con criterios de escalabilidad que permiten ir añadiendo operadores y recursos tecnológicos adicionales si se necesitan. Algunos de los centros más innovadores incluso están incluyendo ya la opción de recepción de llamadas realizada mediante la llamada "**Telefonía IP**, o de **Voz sobre IP (VoIP)**[53]".

Para poder atender simultáneamente a una cantidad tan mayúscula de tareas, y a la vez tan

53. Desde el año 2005, la Comisión Federal de Comunicaciones de Estados Unidos (FCC) ha exigido que los proveedores de VoIP proporcionen de manera automática el servicio 911 a todos sus clientes. Antes de que un proveedor de servicio de VoIP interconectado pueda activar sus servicios para un nuevo cliente, el proveedor debe obtener del suscriptor la ubicación física desde la cual el servicio será utilizado inicialmente, con el objeto de que el personal de emergencia pueda localizar a los usuarios de VoIP que efectúen llamadas al 911.

vitales, aparecieron los **sistemas de gestión de emergencias integrados,** representados principalmente por los llamados **CAD** (Computer Aided Dispatching), o **Sistema de Despacho de Recursos.**

Un sistema de despacho o CAD trata de atender las peticiones de los ciudadanos dentro de unos parámetros, normalmente autoimpuestos por los propios 112 en aras de la calidad y la seguridad. Cuentan a la vez con herramientas para la movilización, gestión y coordinación de los recursos de todas las organizaciones que se encuentran integradas en el servicio.

En un sistema de despacho encontraremos al menos los módulos software necesarios para dar respuesta a las siguientes misiones:

- Atención de llamadas.
- Despacho de recursos para atender el incidente.
- Proceso de seguimiento y cierre del incidente.

Aquellos 112 que además hacen gestión del incidente propiamente dicho, cuentan con:

- Módulo de Mando, Control y Coordinación de los incidentes.

SUBSISTEMAS

Aunque los SIE específicos tienden a su desaparición en beneficio de los SIE integrados, unos y otros comparten multitud de subsistemas que pueden complementar y facilitar el trabajo de los profesionales de las emergencias. Repasemos los más comunes.

TELECOMUNICACIONES

Todos los sistemas llevan como soporte del transporte de la información que gestionan, uno o varios de los sistemas de telecomunicaciones que ya hemos analizado en el capítulo anterior.

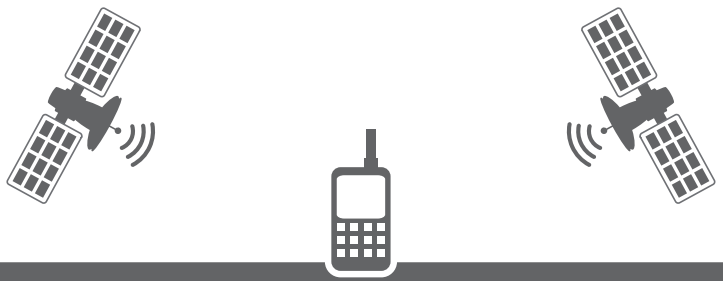
SUBSISTEMA DE LOCALIZACIÓN DE LLAMADAS

Cuando se realiza una llamada a un 112 desde un móvil, ésta ya viene automáticamente acompañada, como mínimo, por los **datos geográficos de la antena base** (la que ha recogido la señal del móvil). Además pueden recibir la ubicación de otras estaciones base próximas al móvil, lo que permite con tres estaciones hacer una triangulación que genera un área dentro de la cual se encuentra el emisor. Cuantas más antenas de un mismo operador haya, más fácil será también determinar la posición exacta de un teléfono móvil, puesto que más pequeña será el área. En las **zonas urbanas** la densidad de antenas es muy alta, y por tanto el área de triangulación es muy pequeña, lo que permite a la plataforma determinar con mucha precisión desde dónde emite su señal un móvil. En las **áreas rurales,** en cambio, las antenas pueden estar mucho más espaciadas, por lo que el área de triangulación puede ser de varios kilómetros cuadrados.

POSICIONAMIENTO DE FLOTAS Y PERSONAL

Aunque ya los hemos mencionado queremos reiterar la importancia que tiene para todos los servicios operativos la **localización de los recursos, personal y vehículos** (terrestres, aéreos o embarcaciones). La tecnología más utilizada es la transmisión de la posición, dada por un **receptor GPS** a través de algún **medio de enlace** (radio, telefonía móvil o satelital). La combinación de estos equipos con **sistemas de información geográfica (GIS)** posibilitan el seguimiento automático de la posición del objeto en un mapa visualizado en la pantalla de un monitor en tiempo real. La señal GPS llega al elemento de la flota o al personal procedente de diversos satélites. El receptor mediante la triangulación de la posición de los satélites captados, nos presentan los datos de longitud, latitud y altitud estimados, al calcular la distancia entre éste y cada uno de los satélites.

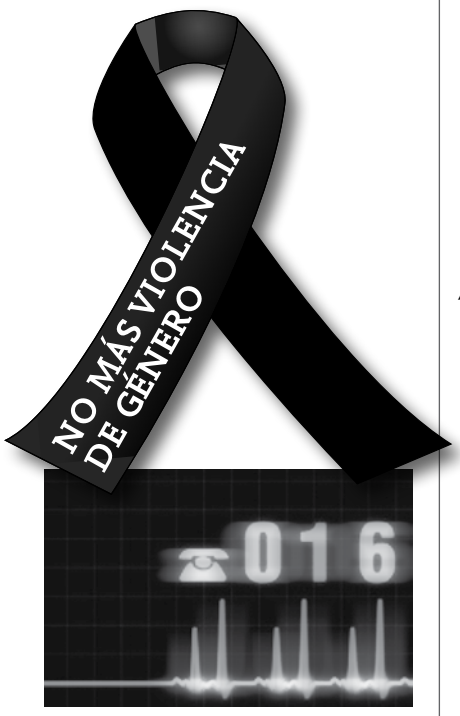
SISTEMAS DE POSICIONAMIENTO TERRESTRE



Un Sistema Global de Navegación por Satélite (GNSS) es una constelación de satélites que transmite rangos de señales utilizados para el posicionamiento y localización en cualquier parte del globo terrestre, ya sea por tierra, mar o aire.

El GPS estadounidense, el GLONASS ruso (básicamente militar) o el Galileo europeo (con una estimable cooperación de China) son los Sistemas más conocidos.

Los receptores pueden recibir la señal de más de 3 satélites (entre 8 y 12) para calcular su posición. En principio, cuantas más señales recibe, más exacto es el cálculo de su posición.



APLICACIÓN TIC QUE SALVA VIDAS

Los programas de prevención de "Violencia de Género" contribuyen a evitar posibles agresiones a las víctimas con rapidez y eficacia, durante las 24 horas del día y con independencia del lugar donde se encuentren. Cuando se sienta amenazada, la posible víctima puede presionar un botón desde su móvil que alertará al personal del centro de control, el cual será informado al instante en su ordenador sobre los datos de la víctima, familiares y del posible agresor, pudiendo contactar con la víctima para su tranquilidad. Mediante GPS, también el sistema permite localizar a la víctima, lo que sirve de ayuda en caso de ser necesaria la asistencia policial o social.

Su importancia en las operaciones de emergencia trasciende el uso cotidiano al que estamos acostumbrados. Estos subsistemas son la base tecnológica por ejemplo de las **radiobalizas de localización de personas (PLB, *Personal Locator Beacon*).** Éstas son de tamaño reducido y de extrema utilidad cuando desarrollamos operaciones de emergencia en zonas desconocidas para nuestro personal o cuando se trabaja en zonas inseguras. Además estos sistemas resultan fundamentales en las tareas de búsqueda y rescate ya que agilizan sobremanera los trabajos.

La navegación por satélite ofrece ventajas evidentes para la **gestión del movimiento de vehículos** de cualquier tipo. No sólo proporcionan la posición, sino que son capaces de dirigir nuestro desplazamiento dentro de un itinerario fijado, contribuyendo a aumentar la seguridad y agilizar el tráfico a nivel terrestre, marítimo o aéreo.

Existen **aplicaciones más especializadas**. Por ejemplo para el control de las aeronaves en incendios forestales podemos encontrar la aplicación "CYGIM" que posibilita visualizar los movimientos, tomas y descarga de los medios aéreos en tiempo real. Da una idea concreta y precisa de la ubicación del incendio y permitiendo acceder a un historial para poder analizar en detalle la progresión de las llamas.

SUBSISTEMA GIS

Los Sistemas de Información Geográfica, o GIS en acrónimo sajón, son los sistemas que se emplean para manipular, analizar, modelizar y representar **datos georreferenciados.** Por otro lado son una de las herramientas que mayor impacto y penetración han tenido en los últimos años en las tareas relacionadas con la Protección Civil y Gestión de emergencias. Suelen trabajar en combinación con otras herramientas asociadas tal y como ya hemos visto en los subsistemas anteriores.

SUBSISTEMA MENSAJERÍA

Hasta la fecha las emergencias en España son gestionadas desde un punto de vista de la mensajería, casi en exclusividad por la **tramitación de faxes.**

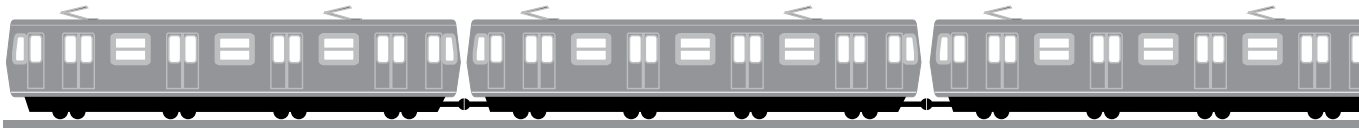
En estos momentos se está en disposición de dar un paso tecnológico importante y superar las bondades del fax, por lo que algunas agencias de emergencias están apostando por la migración a sistemas de mensajería electrónica, tipo **correo electrónico.** Estos nuevos sistemas de intercambio de mensajes escritos prevén la creación de aplicativos que abarquen tanto los **mensajes oficiales**[54] como los **mensajes de relación o interpersonales**[55] entre particulares.

SUBSISTEMAS DE INFORMACIÓN AL CIUDADANO

En España, existen una serie de números telefónicos que en el día a día, o en el periodo "todo tiempo" de las fases de una emergencia están a disposición del ciudadano para informar de diferentes materias. Así encontramos el **060** para preguntar sobre asuntos de la Administración General del Estado, el **010** para ayuntamientos, el **012** para CCAA. En el ámbito de la empresa privada en nuestro país antes de la liberación de las telecomunicaciones solo existía el 1003 de Telefónica. Ahora hay multitud de números 118XX que previo pago ofrecen información a los ciudadanos.

54. La mensajería "oficial ó formal" es aquella en la que todos los usuarios de la misma reconocen la validez de cualquier mensaje de correo electrónico firmado electrónicamente por cualquiera de las personas físicas que, en representación de sus organizaciones, ejerzan sus funciones durante la gestión de las emergencias.

55. Cuando los mensajes tramitados a través de este servicio no vayan firmados digitalmente se entenderá que se trata de mensajería de relación interpersonal (los remitentes y destinatarios de los mensajes son personas físicas, no organismos, cargos o instituciones).



ATENTADOS DE MADRID. 11 DE MARZO DE 2004

En los atentados acontecidos en Madrid del 11 de marzo de 2004, la información a los familiares fue canalizada a través del servicio 112, recibiéndose 40.000 llamadas desde dentro de la Comunidad de Madrid, 15.000 desde fuera y unos 13 millones de visitas a su página web.

Aunque no es una misión que normalmente ejercen, ante grandes catástrofes, y gracias a que sus plataformas tecnológicas lo permiten, las **Agencias 112** suelen dedicar parte de sus instalaciones a recoger datos e informar a los ciudadanos sobre diversos temas, destacando por encima del resto la búsqueda de desaparecidos y la información sobre el estado de salud de heridos. Algunos 112 facilitan información de modo cotidiano sobre tráfico o meteorología.

SUBSISTEMAS DE CONTROL Y GESTIÓN DE RECURSOS

Estos subsistemas nos permiten realizar una gestión y control de los recursos humanos y materiales que se están utilizando en los incidentes o emergencias. De este modo se puede optimizar su uso y se detectan los momentos más críticos desde el punto de vista de la disponibilidad. Un ejemplo podría ser la aplicación "Silvano" utilizada por la Junta de Andalucía.

SUBSISTEMA AUDIOMÁTICO[56]

Este subsistema nos permite la realización de **avisos masivos telefónicos** mediante grabaciones, envío de correos electrónicos o SMS a la población y a organismos.

SUBSISTEMA DE INFORMACIÓN CORPORATIVA

Como todos los SIE, integrados y específicos, funcionan sobre una red de área local de la organización, se les dota de un acceso a la intranet que proporciona a los operadores del sistema información complementaria, documentación, zonas de almacenamiento y otros servicios de valor añadido.

SUBSISTEMA E-CALL

Se trata de proporcionar ayuda rápida a los automovilistas accidentados en cualquier parte de la Unión Europea. Un dispositivo instalado en el vehículo envía en caso de accidente al 112 de la región datos sobre el vehículo, propietario, coordenadas del accidente y dirección de marcha.

SUBSISTEMA DE TELEASISTENCIA

Organizaciones como Cruz Roja Española, ONG, y por supuesto los 112 han incorporado subsistemas de este tipo. En la actualidad convergen tres conceptos con enfoques interrelacionados, la **Teleasistencia domiciliaria**[57], el **Telecuidado**[58] y el **E-salud**[59].

SUBSISTEMA DE INCIDENTE ÚNICO

Estos aplicativos realizan una agrupación de incidentes que forman parte de una misma emergencia u operación. Vienen a realizar una fusión de eventos, lo que permite que diferentes organizaciones puedan referirse al

56. Estos subsistemas han conservado esta denominación inicial de audiomático, aunque hagan otras tareas diferentes a la transmisión automática de mensajes de audio como es envío de mensajes escritos.

57. Teleasistencia domiciliaria: es un recurso que permite la permanencia de los usuarios en su medio habitual de vida, así como el contacto con su entorno socio-familiar, evitando el desarraigo y asegurando la intervención inmediata en crisis personales, sociales o médicas para proporcionar seguridad y mejor calidad de vida.

58. Telecuidado: programas de prevención, ayuda y orientación según su correspondiente entorno, a cargo de profesionales de la psicología y de la salud. Es la práctica de prescribir la información en salud indicada, a la persona indicada, en el momento indicado para satisfacer sus necesidades específicas y apoyarla en el proceso de toma de decisiones.

59. E-Salud: alude a la práctica de cuidados sanitarios apoyada en tecnologías de la información y las comunicaciones (TIC). La aplicación más conocida es la Telemedicina.

mismo hecho. De esta manera se consigue una **Vista Unificada operacional de la situación**[60] (COP, *Common Operational Picture*). Con ello se alcanza a representar en un único plano todos los eventos, todos los medios y todas las misiones desempeñadas por todas y cada una de las agencias participantes.

SUBSISTEMA DE ANÁLISIS DE EFECTOS

Estas aplicaciones tratan de modelizar los **distintos dominios del riesgo,** por ejemplo dominio del transporte de hidrocarburos, red eléctrica, red ferroviaria, etc. De esta manera se determinan los nodos críticos por dominio y la relación entre nodos, dentro de su dominio pero también con los adyacentes.

El objetivo es el de obtener los posibles efectos directos, indirectos y en cascada (**efectos dominó**) a partir de las alertas recibidas. Muchos de estos subsistemas recurren a la **Inteligencia Artificial** para el análisis y fusión de datos provenientes de diferentes fuentes. Cada dominio afectado y cada dominio de riesgo requiere la gestión de informaciones específicas, y esa información debe combinarse con modelos de conocimiento experto y mecanismos de inferencia y planificación. Al final el resultado es que el subsistema prevé peligros y propone soluciones.

El Sistema SIADE es un ejemplo de este tipo de sistemas que está desarrollando el INFOCA de Andalucía, para proporcionar al responsable de la extinción de los incendios forestales posibles líneas de acción a tomar.

SUBSISTEMA DE PLANIFICADORES

Cuando los staff de las organizaciones no son potentes a veces se ven obligados a recurrir a herramientas que faciliten la realización de grandes planes como por ejemplo los necesarios para **evacuar un barco, un edificio o incluso una población.** Estos programas suelen generar listas de tareas a realizar, lista de posibles actividades a desarrollar de modo paralelo y secuencial sin interferencias, y tienen opción de introducir distintas variables como agencias participantes, tiempo y recursos disponibles.

SUBSISTEMA DE SIMULADORES

Son un conjunto de herramientas, para simular en ordenador los resultados de inundaciones, incendios forestales, seísmos, erupciones volcánicas o derrames de productos tóxicos. La simulación puede jugar un papel importante a lo largo de la gestión de la crisis. Permite hacer predicciones sobre cómo los acontecimientos podrían desarrollarse y poder analizar el resultado con antelación de posibles decisiones operativas.

Un desafío clave de estos sistemas es definir el grado de utilidad y las limitaciones de los modelos resultantes de cada simulación. Es decir tiene que estar comprobado que el resultado de la simulación coincide con lo que ocurre en la realidad. De esta manera servirá para dos asuntos muy importantes. Primero: tomar medidas preventivas en las emergencias reales. Segundo: nos servirá para la capacitación y entrenamiento de personal que luego tendrá que tomar decisiones.

En combinación con el subsistema GIS suelen ser empleados para realizar los llamados **Análisis de Riesgos**, que nos permiten la identificación de peligros, el cálculo de efectos y consecuencias.

60. En ocasiones la COP es considerada como un subsistema independiente sin estar integrado en el subsistema de incidente único. También puede aparecer como CROP, añadiendo la "R" de *Relevant* (relevante en español).

SUBSISTEMA C2

Estos Subsistemas de **Mando y Control** (*Command & Control-C2*) proporcionan apoyo a las autoridades responsables en las actividades de planeamiento, dirección, coordinación y control del empleo de las personas y los medios en las emergencias. Nos dan una visión común de la zona de la emergencia y facilitan el planeamiento compartido entre las organizaciones participantes mediante el intercambio de información en todos los niveles de gestión de la emergencia, y para todas las áreas funcionales. En general, los usuarios se corresponden con el personal que desarrolla sus actividades en los centros de coordinación, puestos de mando avanzado o cuarteles generales de las agencias de socorro.

SUBSISTEMAS DE RESPALDO

Por último en este apartado haremos mención a los subsistemas que **garantizan la prestación de servicio aún cuando se produzcan fallos** en los sistemas principales. Se aplican criterios de redundancia y fiabilidad en los equipos más sensibles cuyo fallo puede paralizar la prestación de los servicios. Otra opción es la de crear **centros alternativos** que pueden entrar en funcionamiento en caso de caída del principal, ofreciendo unas prestaciones reducidas de la capacidad de atención y gestión. El lector puede imaginar lo costosa que resulta esta última opción.

SISTEMAS DE INFORMACIÓN DE EMERGENCIAS FUNCIONANDO EN ESPAÑA

En la mayoría de los casos los **servicios de emergencia** en general, y los Centros 112 en particular, deben estar necesariamente **ligados a las TIC** para realizar su labor eficientemente. Existen en España numerosas empresas que han desarrollado productos a la medida de estas organizaciones que ofrecen soluciones más o menos integradoras.

Todas las Agencias 112 tal y como ya hemos mencionado tienen concepciones similares, aunque no idénticas, y tienen asumidos unos roles que precisan potentes herramientas para gestionar las emergencias y recursos.

En nuestro país podemos hablar de poco más de una docena de **"soluciones integrales"** promovidas fundamentalmente por las Comunidades Autónomas. Muchas de ellas comenzaron como productos específicos de cuerpos u organismos, que poco a poco fueron ampliando incorporando herramientas adicionales, o como vimos anteriormente, subsistemas complementarios.

A modo ilustrativo podríamos señalar, de manera no exhaustiva, los siguientes:

ECHO

El Centro de Emergencias 1-1-2 Región de Murcia utiliza desde finales del 2012 la herramienta ECHO (Emergencias: Control Holístico[61] Operativo). Consiste en una plataforma software, diseñada por la empresa TISSAT que brinda un soporte a la gestión y coordinación de todos los servicios intervinientes en una emergencia en esta Comunidad. Esta plataforma como era de esperar hace uso extensivo de herramientas GIS, y permite identificar el lugar exacto de la persona que solicita la intervención de los servicios de emergencias en cualquier punto de la Región. Incorpora posicionamiento de todos los recursos incluyendo por ejemplo la localización de los medios de la Unidad Militar de Emergencia, cuando ésta actúa en la Comunidad Autónoma. Cuenta con una supervisión constante aplicando herramientas de auditoría, control de calidad en la atención de llamadas e incorporada en la misma plataforma la formación de los operadores.

La coordinación entre los organismos y agencias participantes en la atención de los incidentes, es otro de los aspectos de la plataforma ECHO. Para ello, traslada la información en tiempo real y de forma automática a los servicios de emergencias y seguridad de las diferentes Administraciones Públicas, siendo el primer sistema de estas características que se integra plenamente en la RENEM (**Red Nacional de Emergencias[62]**) impulsada por el Ministerio de Defensa a través de la UME.

COORDCOM

Es el producto ofrecido por ERICSSON en España. Procede de la organización SOS ALARM que gestiona las urgencias y emergencias en Suecia. Es la Generalitat Valenciana la que utiliza la versión **G4** de esta plataforma en nuestro país. COORDCOM permite la integración de sistemas de localización de vehículos por GPS, así como la información proveniente de sistemas GIS. También integra otros subsistemas complementarios como los de grabación, comunicaciones y gestión de bases de datos.

61. Holístico: Proviene del Holismo. Doctrina que propugna la concepción de cada realidad como un todo distinto de la suma de las partes que lo componen.
62. En el Anexo 2 se amplía la información sobre esta red.

SITREM

El SITREM (Sistema Integral de Tratamiento de Emergencias) es la solución de ATOS-Siemens Business Services para Centros de Coordinación y Emergencias. Es un sistema de despacho que integra todo tipo de comunicaciones y que abarca todas las fases de operación, desde que se recibe la llamada en el centro, el despacho, el seguimiento, la gestión integral de recursos y medios, hasta que la incidencia ha sido finalizada. Entre los usuarios más destacados de este sistema se encuentra el 112 de Extremadura o el Cuerpo de Bomberos del Ayuntamiento de Madrid.

POSITRON

Se trata de un sistema que se emplea exitosamente en Canadá y en centros 911 de los Estados Unidos. Está instaurado en la Comunidad Foral de Navarra que permite integrar en una misma plataforma llamadas de teléfono y radio, movilización de recursos, mapas y sistemas de información territorial y localización de medios mediante GPS. El puesto de trabajo llamdo "Power 112" integra tres aplicativos: la parte de comunicaciones de la aplicación de FedeTec, el despacho de incidente y recursos a través de la herramienta llamada Dispatch, y con SIGANE consigue ayuda para interpretación geográfica.

SmartCICUS

Ha sido desarrollado por la empresa CYBERINSA SISTEMAS, y soporta las funciones habituales: la recepción de las llamadas, su tipificación, propuesta automática de recursos, y mando y control de los mismos. Integra diferentes plataformas de telecomunicaciones (telefonía analógica, telefonía digital, GSM, radio PMR, Trunking o TETRA, etc). Se encuentra funcionando en varias centrales de coordinación de **urgencias sanitarias** españolas de Valencia, Asturias, Castellón, Islas Canarias, Alicante y Ceuta.

GEMYC-FEDETEC

FEDETEC empresa absorbida por AMPER en el año 2007, desarrolló el GEMYC 112, que es un sistema de **gestión e integración de comunicaciones** de gran parte de los centros de control 112 de España. Actualmente utilizan esta tecnología las agencias 112 de Navarra, tal y como ha sido señalado anteriormente integrado en el POSITRON, el 112 de Madrid, Canarias, Castilla La Mancha, Baleares y La Rioja[63]. Policía Nacional, Guardia Civil y multitud de policías locales también utilizan tecnología FEDETEC en sus centros de control.

SICECAT

Las siglas SICECAT responden a Sistema de Información CECAT (Centro de Coordinación de Operativa de Catalunya (CECAT) para la gestión de emergencias). Es un programa desarrollado por la empresa INSA de forma específica para incluir los requerimientos lógicos y funcionales que se precisan en un centro de coordinación de emergencias. Permite disponer de forma centralizada de toda la información necesaria para una toma de decisiones eficiente y óptima en caso de grave riesgo colectivo, calamidad pública o catástrofe, y también en el seguimiento preventivo, cotidiano y continuo de los acontecimientos ordinarios. Está enfocado a

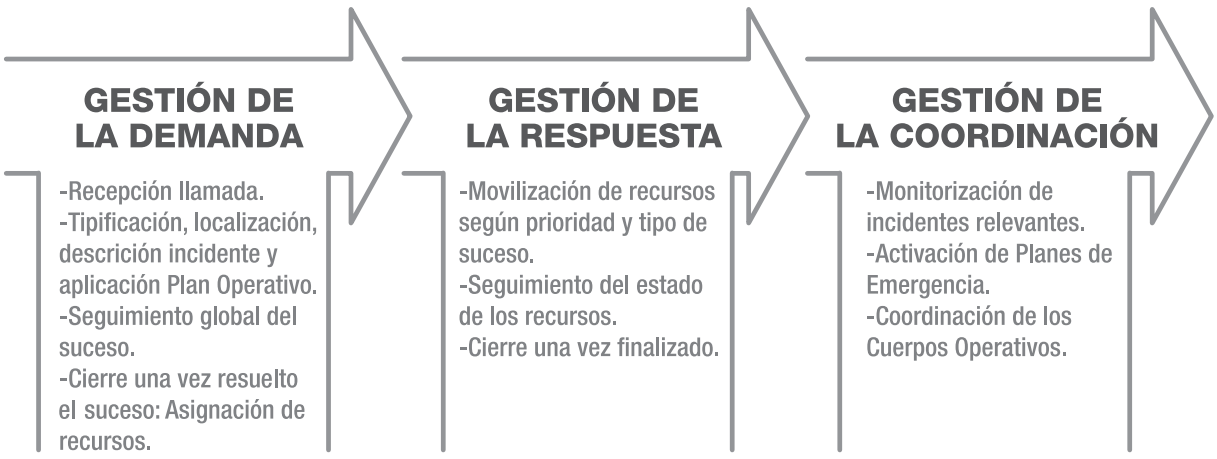
63. Otros organismos que poseen productos FEDETEC son: los Bomberos de Logroño, Diputación de Albacete, Diputación de Vizcaya, Cáceres, Consorcio de Bomberos de Castellón, en los Centros de Información y Coordinación de Urgencias Sanitarias (CICUs) de Alicante, Castellón y Valencia, Policía Local de Elche, Ciudad Real, y los Servicios de Incendios Forestales de Guadalajara, Toledo, Cuenca, Albacete, Ciudad Real, Agencia Medio Ambiente Andalucía en Cádiz y Departamento de Medio Ambiente de Aragón, el 061 de Ceuta y el centro de control del Metro de Madrid.

gestión de información y específicamente a la difusión multicanal (voz, fax, mail, SMS). Para ello se integra con un proveedor específico de telecomunicaciones que ofrece continuidad de servicio por encima del 99%. SICECAT se maneja en entorno web securizado accesible solo desde la sala CECAT. En relación a la integración de aplicaciones de los diferentes organismos que trabajan en el CECAT (Protección Civil de la Generalitat y del Ayuntamiento de Barcelona, Bomberos de la Generalitat y de la ciudad de Barcelona, Mossos d'Esquadra, Guardia Civil, Servicio Catalán de Tráfico, servicio 112, Diputación de Barcelona, Agencia Catalana del Agua, Servicio Meteorológico de Cataluña, Agencia de Residuos de Cataluña, Servicio de Emergencias Médicas, Dirección General de Carreteras de la Generalitat y del Estado, Cruz Roja, la Dirección General de Calidad Ambiental y empresas como Endesa, Renfe, FGC y Acesa) el departamento dispone de un BUS interno para la integración de datos, el cual permite poner a disposición de las diferentes aplicaciones departamentales los datos y actuaciones del resto.

SÉNECA

Es la solución de TELEFÓNICA SOLUCIONES, del Grupo TELEFÓNICA, especializada en el desarrollo de software de gestión de emergencias y se ha consolidado en el sector de la seguridad pública de la mano de la implementación de su producto en el centro MADRID 1·1·2, cuya capacidad y eficiencia frente a catástrofes han quedado por desgracia bien demostradas en los últimos años. Otras Comunidades donde funciona son Castilla y León, Cantabria, Andalucía, y en las ciudades autónomas de Melilla y Ceuta. Esta aplicación tuvo su origen en una petición realizada por el Consorcio de Bomberos de Cádiz allá por el año 1991 (por ello lleva el nombre del Sabio Andaluz). Sus diferentes versiones, refinadas para cada uno de los clientes, han hecho un producto solido y consolidado en el mercado tecnológico de las emergencias. Contempla los procesos básicos: atención de la demanda del ciudadano; despacho del incidente, activación o alerta; mando y control de los recursos; seguimiento y cierre del incidente; y explotación de la información relacionada. Consta de un elemento de telecomunicaciones, uno de GIS llamado de localización y soporte y otro módulo denominado de interoperabilidad para recibir o intercambiar información con otros sistemas.

PROCESOS DE UN CENTRO DE GESTIÓN DE EMERGENCIAS



En muchas Comunidades Autónomas la gestión de los incendios forestales no está integrada en los 112 correspondientes, y son las **Consejerías de Agricultura y/o Medio Ambiente** las que han desarrollado sus propios SIE, que vienen a ser una panoplia de pequeños programas que ayudan al **Director de Extinción.**

Entre las aplicaciones más destacadas actualmente en uso se encuentran las siguientes: XeoCODE, InfoGIS, SIGYM, FIDIAS, FARSITE, EMERCARTO y CARDIN (Simuladores de Incendios Forestales); Telemaq+, CYGIM y HORUS (aplicaciones informáticas de localización y posicionamiento de medios aéreos y de medios terrestres); CONDOR (Visor 3D de planificación durante la extinción de incendios forestales); SIADEX (Sistema de inteligencia artificial de apoyo a la Dirección de Extinción); Sistema Bosque (detección automática de incendios mediante cámaras de infrarrojos y ópticas).

Pasemos a dar algunas características de los más importantes desde nuestro punto de vista.

XEOCODE

XeoCode es una aplicación que permite la introducción de alarmas e incendios en un entorno visual y que suministra una información global de su estado en Galicia. Este software forma parte de un conjunto compuesto por otras dos aplicaciones (XLumes Codificador y XLumes Informes). Estas aplicaciones proporcionan un servicio de gestión y control de los incendios forestales. Esta herramienta informática permite georreferenciar los incendios y conocer sobre una ortofoto y mapa topográfico la superficie y recursos amenazados en cada incendio, así como la localización de los medios y personal desplegados. Hace una gestión en tiempo real a nivel de Distrito, con la interacción de los servicios contraincendios provinciales y centrales. Incorpora capas raster (fotos aéreas SIGPAC, PNOA, imágenes de satélite, mapas topográficos) y capas vectoriales (unidades administrativas, núcleos de población, vías de comunicación, red hidrográfica, puntos de agua, puntos de vigilancia, puntos de encuentro, bases de medios aéreos, espacios de especial protección, etc.), medición de distancias y áreas, radios de acción, así como envío de SMS al responsable de la unidad afectada y al teléfono de contacto para emergencias del ayuntamiento implicado.

INFOGIS-FIRESPONSE

El InfoGIS es un sistema de gestión del operativo de extinción de incendios forestales y asesoramiento en las diferentes estrategias de ataque. Ha sido desarrollado íntegramente por la empresa leonesa Tecnosylva. También utiliza la denominación de FIRESPONSE en EEUU, e incluye todas las fases de gestión de incendios forestales desde su prevención, gestión y evaluación final. Se aplica como sistema de gestión en comunidades de Andalucía, Extremadura, Aragón y Murcia. También se ha implantado un simulador de esta empresa en el sistema de información de la Unidad Militar de Emergencias llamado WILDFIRE Analyst.

EMERCARTO

Desarrollada por la empresa estatal TRAGSA, la aplicación cuenta con un potente Visor GIS que permite el control y optimización de los recursos de extinción mediante técnicas y equipos GPS/GPRS, ofreciendo al gestor la posición georreferenciada de los medios de extinción con la posibilidad de transferir información entre el lugar del incendio y el centro de coordinación. Además tiene herramientas de Gestión de la información. Sobre plataforma Web, accesible desde cualquier parte del Territorio Nacional, permite a los técnicos disponer in situ de ortofotos y de una serie de capas cartográficas con información de utilidad tanto para la planificación como para la extinción. Por ejemplo el Consorcio para el Servicio de Prevención, Extinción de Incendios, Protección Civil y Salvamento de la Provincia de Guadalajara (CEIS) utiliza "Emercarto-Sigueme".

FIDIAS

Los Centros Operativos Provinciales (COP) y los Centros Operativos Regionales (COR) de Castilla y La Mancha tienen operadores que actualizan en tiempo real la información de los incendios de su Comunidad en el sistema de gestión de incendios FIDIAS. Desde éste pueden seguir la evolución, los medios que participan y las diferentes tareas que se están realizando.

SIGYM

El Sistema de Información Geográfica y Meteorológica (SIGYM) es utilizado por diferentes CCAA, como Madrid, Andalucía o Castilla la Mancha, para la gestión de los incendios forestales. Incorpora un servicio de localización de impacto de rayos, predicciones de temperatura y precipitaciones, información espacial y un simulador de incendios. De este modo, en caso de aparición de algún foco los técnicos sólo tienen que introducir

las coordenadas y el sistema informa entre otros parámetros de la predicción de las características del viento, de la temperatura, probabilidad de precipitación, temperatura y la humedad. Del SIGYM se obtienen las predicciones para un período de entre 7 y 10 días.

Pero no sólo existen SIE integrados en los 112. Otras organizaciones se han dotado de herramientas similares para llevar a cabo sus tareas. A modo de ejemplo, y por el papel que juegan en las emergencias en España podríamos comentar la existencia de otros sistemas como los de la Dirección General de Protección Civil y Emergencias del Ministerio del Interior, o el de la Unidad Militar de Emergencias del Ministerio de Defensa.

Los SIE más importantes disponibles en la DGPCyE son:

SIGE

El Sistema Integrado de Gestión de Emergencias dispone de funcionalidades relacionadas son la gestión de alertas y de recursos empeñados en una emergencia. SIGE fue desarrollado inicialmente por Indra, aunque la mayor parte de los módulos actualmente en uso (que son los que componen el llamado SIGE2) han sido desarrollados por TRAGSATEC. SIGE2 utiliza una base cartográfica, y un visor SIG, que ha venido cobrando importancia creciente. Facilita la recogida, la gestión y la presentación de la información relativa a emergencias.

Los módulos del SIGE permiten gestionar los distintos tipos de riesgo compartiendo la misma infraestructura y los mismos procedimientos genéricos, pero permitiendo un tratamiento diferenciado de cada uno.

El módulo de Incendios Forestales permite la localización geográfica del área del incendio, así como sus datos de inicio (situación del foco, hora de detección), los participantes en la extinción, los medios utilizados, incidencias, etc.

El módulo de Fenómenos Meteorológicos Adversos tiene un funcionamiento similar, aunque en este caso es primordial la carga automática de datos meteorológicos que se realiza a partir de la información que diariamente envía la Agencia Estatal de Meteorología (AEMet).

Otros módulos de SIGE son el de Transporte de Mercancías Peligrosas, y los de Riesgo Químico y Riesgo Nuclear. Estos dos últimos, de reciente implantación, permiten, además de la gestión de emergencias, su planificación y previsión a través de diversas herramientas de inventario, simulación, etc. incluidas en el sistema. Además tiene previsto la integración del Catálogo Nacional de Recursos[64] (CNR).

SIGAME

El Sistema de Gestión de Ayudas con Medios en Emergencias tiene por objeto intercambiar información entre CCAA sobre los recursos que se ponen a disposición en una emergencia determinada. Actualmente está en desuso.

ARCE

Esta Aplicación en Red para Casos de Emergencia ha sido desarrollada por la Universidad Carlos III de Madrid a iniciativa de la DGPCyE, para crear un soporte de intercambio de información para gestionar las emergencias debidas a catástrofes naturales dentro de la Asociación Iberoamericana de Organismos Gubernamentales de Defensa y Protección Civil.

64. De acuerdo a la Ley y Norma Básica de Protección Civil, le corresponde al Ministro del Interior elaborar el catálogo nacional de recursos movilizables de emergencias, integrando en el mismo los que resulten de los planes territoriales especiales.

SISTEMA INTEGRADO MILITAR DE GESTIÓN DE EMERGENCIAS

El objetivo es ofrecer las herramientas informáticas que:

- **Sistematicen** las actividades de una forma coordinada.
- **Automaticen** en lo posible esas actividades.
- Mantengan un **histórico** de las operaciones realizadas.
- Permita **auditar** la operativa del sistema a todos los niveles, desde la información recibida hasta las órdenes ejecutadas, de forma que puedan justificarse fehacientemente todos los pasos dados en la gestión de una emergencia.

SIMGE

Por su parte la Unidad Militar de Emergencias del Ministerio de Defensa utiliza el llamado SIMGE.

SIMGE

El Sistema Integrado Militar de Gestión de Emergencias es un SIE para el Mando y Control de una fuerza militar especializada en el mundo de las emergencias que tiene **vocación integradora** al igual que los SIE de las CCAA. Utiliza como base un consolidado sistema de Mando y Control militar utilizado por las fuerzas terrestres británicas, el **Sitaware** construido por la empresa SYSTEMATIC, y adaptado por INDRA a las particularidades de esta unidad militar.

El SIMGE se diseñó sobre la base de las Operaciones Basadas en Efectos (EBAO) y una arquitectura orientada a servicios (SOA), con un protocolo estándar basado en servicios WEB denominado CESAR, que le permiten, a través de un **nodo de interconexión entre la red WAN PG del Ministerio de Defensa y el mundo de Internet,** interoperar y federarse con cualquier otro sistema de gestión de emergencias de otra organización[65]. La iniciativa de la UME ha supuesto un punto de encuentro de los sistemas de emergencias de las 17 Comunidades Autónomas y 2 ciudades autónomas, y de hecho hoy toda esta ARQUITECTURA es la referencia de las TIC en los Planes Estatales de Emergencia Nacional en España, que regulan una emergencia nacional de nivel 3, tal y como se va oficializando en las diversas publicaciones del Boletín Oficial del Estado, y de los que hablaremos en el último capítulo de este libro.

OTROS DESTACADOS SIE FUNCIONANDO FUERA DE ESPAÑA

Sin ánimo alguno de ser exhaustivo debemos hacer mención al menos a los siguientes SIES, por la posible relación que pudiéramos tener con ellos dado el caso de una intervención internacional que se pudiera producir dentro o fuera de nuestras fronteras:

65. Esta situación contrasta con otras partes del Ministerio de Defensa u otros Ministerios de la AGE, que ni sus propios sistemas son interoperables ni se atisba solución a largo plazo. No parece lógico que se haya empleado la más moderna metodología militar de la OTAN para el diseño de los CIS de la UME desde 2006, y que ningún Ministerio (incluso el de Defensa) no empleen el mismo camino para modernizar las TIC específicas. Al mismo tiempo, no se comprende que otras naciones como Francia, Austria, Portugal, Marruecos o la mayoría de las iberoamericanas hayan mostrado su admiración sobre el modelo CIS español de adaptación de los CIS militares a las emergencias y nuestros propios Ejércitos y el Órgano Central no muestren excesivo interés en 2013 en aplicar las lecciones aprendidas en esta singular iniciativa.

CECIS

En Europa, y enmarcada en el Mecanismo de Protección Civil de la Unión Europea encontramos el ***"Common Emergency Communication and Information System"*** (CECIS). Es decir el sistema TIC de emergencias comunitario con el que se han dotado los países miembros para facilitar la comunicación entre el **Centro de Respuesta de Emergencias (Emergency Response Centre** [ERC][66]) y los centros designados por los países europeos para proporcionar una respuesta rápida y eficaz a los desastres que se produzcan dentro y fuera del territorio europeo. Esta conexión facilita el intercambio de información y experiencias entre las autoridades responsables de la protección civil y contaminación marina para hacer frente a las diferentes fases de las emergencias.

Su tarea principal es organizar una **base de datos de expertos y de medios de protección civil** para gestionar las solicitudes de ayuda o asistencia que realicen los países afectados por catástrofes.

GLOBAL DISASTER ALERT AND COORDINATION SYSTEM (GDACS)

Dentro del marco de las Naciones Unidas destaca el **Sistema Global de Coordinación de Alertas provocadas por Desastres (GDACS).** Este sistema es un portal web, en el que también participa la Comisión Europea, y que está a disposición de los responsables de la gestión de las grandes catástrofes que se producen a lo largo y ancho de la Tierra. Al igual que el resto de SIE su objetivo es el de mejorar la interacción entre actuantes mediante un fluido intercambio de información y coordinación en las primeras fases de la emergencia. Destaca sobre manera en este sistema el llamado **OSOCC[67] Virtual.** Se trata de una plataforma para coordinar equipos de respuesta UNDAC[68], incluyendo equipos USAR[69], que despliegen tras un desastre de gran magnitud. El sistema está administrado por el GDACS y está bajo la cobertura de la OCHA[70]. Permite la recepción de alertas por correo y SMS, y la movilización de personal y medios. También permite entrenamiento y reuniones virtuales y posee una gran base de datos fotográfica.

EMERGENCY SUPPORT SYSTEM (ESS)

También dentro del marco de la Unión se está desarrollando un proyecto muy ambicioso, que aunque todavía pueda tener tintas de "ciencia ficción", se está acometiendo con mucha seriedad. Este proyecto se denomina **Sistema de Apoyo a la Emergencia** *(Emergency Support System* [ESS]), y está financiado por la Comisión Europea en virtud del tema 'Seguridad' del Séptimo Programa Marco (7PM/7FP). ESS pretende reunir un conjunto de tecnologías de datos en tiempo real que proporcionen información de utilidad práctica a los gestores de emergencias. El proyecto integra comunicados con **centro de fusión de datos** (DFMS) que se ocupa de tareas como la comunicación entre los sensores y la base de datos; la armonización de los datos procedentes de distintos sensores pertenecientes a una misma categoría; la fusión de datos procedentes de distintos tipos de sensores; y la localización espacial de los datos. El portal WEB del ESS proporcionará a todos los implicados, una vez finalizado, una plataforma común, uniforme y ubicua para la obtención, el análisis y la difusión de datos en tiempo real para la adecuada toma de decisiones.

66. La antigua denominación, aún muy utilizada de este centro era "**MIC**" (*The Monitoring and Information Centre*), es decir Centro de Información y Monitorización de Emergencias
67. Se trata de un Centro de Coordinación de las Operaciones *in situ* (OSOCC por sus siglas en inglés, *On-site Operational Coodination Center*) que se crea con el fin de ayudar a las autoridades locales de un país afectado por un desastre para coordinar la ayuda internacional. El OSOCC debe ser establecido con la máxima celeridad tras el desastre por el primer equipo internacional de USAR o de equipo UNDAC que llegue sobre el terreno enviado por OCHA.
68. UNDAC: Equipo de las Naciones Unidas de Evaluación y Coordinación en Casos de Desastres *(United Nations Disaster Assessment and Coordination Team).*
69. USAR: *Urban Search and Rescue*
70. OCHA: *United Nations Office for the Coordination of Humanitarian Affairs.*


VALIANT

CAPÍTULO 7

GESTIÓN DE LA INFORMACIÓN Y DEL CONOCIMIENTO EN LAS EMERGENCIAS

Ya vimos en el capítulo anterior que la información que deben entregan los Sistemas de Información de Emergencias (SIE) debe ser **veraz, oportuna, relevante** para el receptor de la misma **y en cantidad adecuada.** Sin embargo también sabemos que no son los SIE los únicos medios a través de los que los gestores de las emergencias pueden recibir información, que incluso pudiera llegar en cantidades ingentes.

Si de nuevo nos remontamos a la **definición de enlace** nos seguiremos hallando en el tratamiento de la información. En este capítulo lo que vamos a hacer es adentrarnos en el detalle de cómo hacemos el procesamiento de la información, que para muchos constituye el Centro de Gravedad[71] de las emergencias.

Es importante que el responsable de la gestión reciba la información del modo en como él, o la organización han decidido que quieren que llegue. De la gran cantidad de información que producen las operaciones de emergencia no toda resulta importante, ni tampoco es útil para todo el mundo por igual. Es necesario meter ciertos filtros para conseguirlo.

La organización debe establecer los criterios pertinentes para que la información de la emergencia que llegue sea **relevante**, la reciba únicamente quien la necesita en el momento oportuno, en el formato que le sea más útil, y todo ello en cada nivel de mando o dirección. Esta tarea conforma lo que se denomina **Gestión de la Información**[72] (*en inglés Information Management* [IM]).

71. Carl Von Clausewitz definió el Centro de Gravedad como "el centro de todo poder y movimiento del cual todo depende". Para Clausewitz el Centro de Gravedad constituye una fuente de fortaleza, tanto física como moral, que "arrastra todo lo demás".

72. En algunos casos la Gestión de la Información es referida también como "Fusión de la Información". La definición más extendida de este concepto es el proceso mediante el cual se realiza la adquisición de datos de múltiples fuentes, la integración de estos datos en información utilizable y accesible en cantidad y forma, para su posterior interpretación.

JERARQUÍA COGNITIVA

Hemos visto que los gestores o directores de las emergencias precisan estar informados para tomar decisiones que hagan que las labores se desarrollen por el mejor de los caminos. Estas decisiones se basan en la **comprensión de la situación,** comprensión que es resultado de **múltiples factores,** algunos de ellos **objetivos**, pero otros muchos totalmente **subjetivos** ya que el entendimiento que cada persona haga sobre unos mismos hechos puede depender de experiencias pasadas, de la propia personalidad del individuo o del contexto en el que los acontecimientos se desarrollan.

La principal tarea de la Gestión de la Información es **recolectar los datos y transformarlos progresivamente añadiendo significados y contenidos adicionales** que le permitan ir subiendo en el nivel de la jerarquía cognitiva. De este modo el valor y la calidad de la información que le llegará a las personas que toman las decisiones (jefes y responsables) serán considerablemente mayores que si se la diéramos sin depurar.

Este proceso permite ir subiendo niveles en la **pirámide de la jerarquía cognitiva,** pasando del nivel más bajo, el dato, hasta el vértice superior donde se alcanzará el entendimiento o la compresión de la situación en cada momento de la emergencia. Ver figura adjunta.

Los **datos** como hemos dicho están en la base de la pirámide. Se puede tratar por ejemplo de **señales capturadas** o un dato (quizás una señal eléctrica o un puñado de bits) provenientes de una red de alerta o vigilancia. Sin el consiguiente procesado o interpretación, estos datos apenas tienen valor. Los datos son obtenidos por los **medios de obtención** o captura, que a su vez pueden ser casi infinitos. Una sonda sísmica, un bombero dentro de un edificio o una cámara de televisión instalada en un helicóptero.

Durante la crisis volcánica acaecida en el año 2011 en la isla de El Hierro en el archipiélago canario, inicialmente los datos obtenidos no eran más que pequeños temblores detectados por la Red Sísmica Nacional del Instituto Geográfico Nacional.

La **información** son los datos que una vez **procesados** obtienen un significado mayor. Aquí encontraremos acciones como la **fusión, filtrado, organización, formateo, correlación o clasificación**. Este paso es realizado por diverso personal. Los **operadores** de sistemas específicos que recopilan los datos, lo operarios que están en el terreno y recogen muestras o retransmiten vía radio lo que ven. También puede ser un ordenador que recoge señales y las muestra en pantalla traducidas por ejemplo en colores.

Los temblores de nuestro ejemplo en la isla de El Hierro son archivados y clasificados mediante programas informáticos. Se crean tablas con su duración, intensidad, coordenadas geográficas y profundidad a la que han tenido lugar.

Llegamos al **conocimiento**. La información es cambiante, varía en el tiempo, el darle valor, mediante el **análisis y la evaluación** es lo que se conoce ampliamente como conocimiento. El conocimiento individual se hace colectivo a través de la propia gestión de la información. El conocimiento alude a la capacidad para **interpretar informaciones** aisladas **y relacionarlas** con otras. Los elementos principales que hacen posible la gestión del conocimiento son el personal, la organización y la tecnología. Lo ejecutan **Técnicos Superiores y Expertos** en los distintos campos de las emergencias.

A partir de este escalón de la jerarquía cognitiva, se obtiene ya un producto utilizable para la toma de decisiones, ya que permite deducir interrelaciones y obtener conclusiones.

Los expertos en sismología y vulcanología del archipiélago canario recogen esas tablas de información creadas en la etapa precedente, las estudian analizan y evalúan concluyendo que la frecuencia e intensidad de los movimientos sísmicos apuntaban que en un plazo determinado se podría producir una erupción volcánica.

Por último alcanzaremos la cima de la pirámide, la **comprensión**, cuando partiendo del conocimiento se aplican razonamientos, se establecen relaciones entre factores (externos e internos) y se pueden anticipar consecuencias ante unos hechos. Es el **conocimiento refinado**, mezclado con el estudio de otras informaciones que ayudan a comprender lo que puede alterar la situación. La comprensión es una abstracción que nos permite inferir resultados de posibles acciones. Lo deben llevar a cabo los **máximos gestores de la emergencia,** que unos casos serán políticos y en otros técnicos. Ahora se pueden sacar conclusiones mucho más completas y por ende **tomar decisiones** más ajustadas a la realidad.

Dada la alta frecuencia de los movimientos sísmicos, la inquietud y alarma generada en la población y habiéndose detectado la emisión de lava en el fondo marino en La Restinga, se ordena el 28 de septiembre de 2011 la intervención de la Unidad Militar de Emergencias para montar varios campamentos de damnificados a los que acudirían la población de El Hierro una vez se ordenara la evacuación de sus casas, como paso previo a la evacuación a otra isla vecina. Además se ordena el refuerzo de

LA JERARQUÍA COGNITIVA

PIRÁMIDE COGNITIVA: PASO DEL DATO A LA COMPRENSIÓN

los sistemas de telecomunicaciones ante una eventual evacuación masiva y se movilizan buques para efectuar los traslados.

La utilidad de la información radica en su conversión a conocimiento a partir de la selección y la evaluación de la gran cantidad de información disponible. De ahí que la necesidad de la gestión no se limita al ámbito exclusivo de la información, sino que se extiende al del conocimiento.

El conocimiento también debe ser correctamente administrado a través del **juicio intelectual o raciocinio,** para que se convierta en el mejor producto posible para que el responsable correspondiente tome la decisión más adecuada. Pero ¡Ojo! Esto no significa que el responsable vaya acertar siempre. Mediante estos procesos disminuiremos la probabilidad de que se equivoque, dándole una base más sólida para que la decisión esté **basada en hechos y no en "corazonadas".**

EL FLUJO DE LA INFORMACIÓN EN LAS EMERGENCIAS

Por lo tanto podemos concluir que la Gestión de la Información son todos los procesos que se hacen para poder subir por la pirámide de la jerarquía cognitiva, y que por tanto se llevan a cabo de manera continuada mientras la emergencia esté activa.

La información que se genera en algún instante de la catástrofe, se puede almacenar, consultar, trasmitir o incluso se puede perder o extraviar. Podemos por tanto afirmar que la información circula o fluye. Además a continuación podremos comprobar que el flujo de gestión de la información tiene naturaleza cíclica.

Veamos las fases que forman parte del mencionado ciclo.

DEFINICIÓN DE LAS NECESIDADES DE INFORMACIÓN

Cualquier profesional de las emergencias conoce sobradamente su trabajo y sabe perfectamente qué datos tienen que llegarle para hacerse una idea de la situación. Este hecho es extensible a cualquier nivel de la jerarquía, desde el interviniente hasta el más alto responsable. El hecho más habitual es que estén procedimentadas o definido **qué información debe transmitirse** por la cadena de mando. Estas son las llamadas **necesidades de información.** Si la organización dispone de un staff o plana mayor, cada uno de los componentes en sus respectivas áreas (logística, seguridad, operaciones) tendrán también sus propias necesidades o habrá momentos en los que el personal marcará requisitos de información adicionales, fuera de los habituales, o que no estén contenidos en los procedimientos de la organización. Una tarea importante a desarrollar es **priorizar estas necesidades** si no se tienen suficientes elementos de obtención o captura de información.

NECESIDADES DE INFORMACIÓN ANTE UNA GRAN CATÁSTROFE [I]

INFORMACIÓN GENERAL

- Zonas y poblaciones afectadas
- Hora a la que ha ocurrido la catástrofe
- Densidad de población y tipo de construcción en la zona afectada
- Condiciones meteorológicas actuales y previstas en la zona
- ¿Se esperan problemas secundarios a raíz del suceso principal? (fuego, derrames de sustancias tóxicas, problemas de orden público, etc.)
- Informes o valoraciones que se han hecho hasta el momento sobre el desastre
- ¿Quién los ha hecho? Fiabilidad de los informes realizados
- Necesidades de información no disponible hasta el momento
- Organismos oficiales y personas de contacto
- ¿Quién está actualmente al mando de la respuesta?
- Lugar en el que se han establecido los puestos de mando
- ¿Cuál ha sido la respuesta de las distintas administraciones hasta el momento?
- ¿Cuál es el papel asignado a las distintas administraciones y organismos?
- ¿Quién está dirigiendo la información pública?
- Capacidades disponibles en la zona para responder a la situación planteada
- Estado de las TIC

CAPTURA

Puede haber elementos especializados en satisfacer las necesidades de información, aunque no es lo más común. En la mayoría de las ocasiones los únicos elementos para obtener la información provienen de los mismos intervinientes. Esto presenta un importante inconveniente ya que el operativo es distraído constantemente por los Directores de la Emergencia, los CECOP o por los Puestos de Mando Avanzados (PMA).

Una vez obtenida o capturada la información solicitada tenemos que hacerla llegar a quien la requirió. Aquí entrarán de nuevo a funcionar los **medios de enlace disponibles** teniendo muy presente que el **ancho de banda**, siempre finito, será nuestro caballo de batalla. Lógicamente contaremos que la petición de información va en línea con el medio de enlace al alcance de la fuente de información,... aunque quizás sea mucho suponer.

Para atender una solicitud de fotografías, vídeos o ficheros, debemos contar con medios de telecomunicaciones que nos permitan la transferencia en un tiempo admisible. Si por ejemplo disponemos sólo de una radio analógica, la petición además de inviable es estúpida. Por tanto aquí la labor de **asesoramiento del Responsable TIC** de la organización será fundamental para que no se soliciten "peras al olmo".

TRATAMIENTO

Una vez obtenida la información y remitida al que la solicitó o a quien le puede ser de utilidad, se inician los procesos para que ese dato elemental obtenido se transforme en conocimiento que sirva de base para la comprensión de la situación. Incluye acciones implementadas por las **máquinas** a través de las que pasa, pero sobre todo el **análisis y la evaluación** de los datos obtenidos por **personas expertas** en la materia y su transformación en información.

El punto de mayor discontinuidad en el flujo de información está en la captura y el tratamiento de la misma. La **información tratada** es útil, pero el "**sobretratamiento**" puede terminar por enterrar el valor de la información obtenida y por ende del conocimiento, ya que ésta queda camuflada en la selva de la "**sobreinformación**". En los procesos donde se da gran prioridad a documentar al máximo no se suele observar una realimentación eficaz de intervinientes y gestores.

LA JERARQUÍA COGNITIVA 2

QUIÉN HACE QUÉ EN LA JERARQUÍA COGNITIVA.

PRESENTACIÓN DE LA INFORMACIÓN

Tras ser tratada la información, el siguiente paso es distribuírsela y presentársela al que va a hacer uso de ella. El **formato** puede ser cualquiera (audio, visual o papel...o cualquier otro), **pero preferiblemente en el que la autoridad se sienta más cómoda.** Lo primordial es que sea un formato comprensible y manejable. En cualquier caso, con independencia del método de presentación empleado es sumamente útil que dicha presentación esté **normalizada**, es decir regida por unas reglas conocidas por todo el mundo, para que todos sepan dónde buscar la información, facilitar su asimilación y tener la certeza de que **toda la información relevante está incluida.** Luego expondremos los métodos más comúnmente utilizados.

COMPRENSIÓN DE LA SITUACIÓN

Los pasos anteriores aseguran que se han conseguido datos para satisfacer las necesidades de información que tienen los responsables. Además los datos se han transformado en información gracias a la depuración y aportación realizada por máquinas y personal experto. Sin embargo estas acciones previas resultarían yermas sin la **imprescindible aportación mental que tienen que realizar los responsables de la gestión de la emergencia.**

Son mucho los factores que pueden influir en esta fase. El grado cultural, el compromiso personal y profesional, el estado anímico. Pero sobre todo influyen el adiestramiento y la práctica previa, por lo que una vez más los ejercicios, simulacros y experiencia en la gestión de situaciones similares pasan a desempeñar un

papel básico. La información, mucha o poca, sin interpretación no es nada. En todo caso, y sea cual sea el camino para llegar a la comprensión, **el resultado será una decisión,** que se debe traducir en acción. La información que no se traduce en acción tiene poco valor.

Tras la decisión se suelen plantear **nuevas necesidades** de información para apoyar las próximas órdenes. Así se reanuda de nuevo el **ciclo de la gestión de la información.**

PROCEDIMIENTOS DE GESTIÓN DE LA INFORMACIÓN EN LAS EMERGENCIAS

Son **abundantes y diversos** los procedimientos que se pueden emplear en la gestión de la información. Algunos de los procedimientos de gestión han sido ya identificados en capítulos precedentes. Los sistemas de enlace están presentes en mucho de esos procedimientos. Examinaremos a continuación los más habituales e importantes.

CONTACTO PRESENCIAL

Son tres los modos más habituales. **La yuxtaposición de centros de trabajo, el intercambio de oficiales de enlace entre organizaciones y las reuniones.** De los dos primeros ya hemos hablado en capítulos anteriores. Vamos a detenernos un poco en el tercer procedimiento, las reuniones.

Las **reuniones de trabajo** son el claro ejemplo de un sistema analógico que no se le da la importancia que tiene. Se pueden hacer reuniones para compartir opiniones, fijar criterios, decidir líneas de acción, poner en común proyectos o para homogeneizar ideas. Es evidente que una reunión bien organizada y bien dirigida facilita el flujo de información. Las reuniones hay que prepararlas con seriedad y se deben convocar cuando haya una razón que lo justifique. No se puede frivolizar convocando reuniones sin objetivos porque suponen una pérdida de tiempo para todo los asistentes. Se debe convocar con tiempo suficiente para que todos los asistentes se la puedan preparar y fijar un orden del día que todos los asistentes deben conocer. La gestión de la información implica también fijar un tiempo estimado de duración.

CONTACTO A DISTANCIA

Es manifiesto el papel de los medios de enlace a distancia o telecomunicaciones. Desde una llamada por **radio** de cuatro o cinco segundos de duración, hasta una llamada por **teléfono** de horas, todo es intercambio de datos y/o de información entre al menos dos personas. Si aumentamos el número de participantes tenemos que hablar de lo que vienen a ser **reuniones virtuales o teleconferencias.**

La **audioconferencia** es la interacción, usando **telefonía**, entre grupos de personas desde dos o más lugares distantes en tiempo real. Es la modalidad más antigua y sencilla de teleconferencia y no utiliza medios visuales, siendo por lo tanto menos costosa (desde el punto de vista del precio del material necesario y del ancho de banda necesario) que una videoconferencia. La denominación de **reunión virtual** no es nimia, y deben prepararse tan concienzudamente como las reuniones presenciales para conseguir el correcto flujo de la información. Al realizar audioconferencias, el responsable debe cuidar que la conexión telefónica se realice en el horario previamente acordado, verificar

NECESIDADES DE INFORMACIÓN ANTE UNA GRAN CATÁSTROFE [II]

POBLACIÓN AFECTADA

- Número de fallecidos, heridos, desaparecidos, desplazados, sin hogar…
- Situación, mecanismos de respuesta activados, capacidad de alojamiento disponible

SALUD PÚBLICA

- Estado de la red hospitalaria
- Riesgos potenciales para la salud de las fuerzas intervinientes (fuga de gases, etc.)
- Apoyo sanitario necesario para las fuerzas intervinientes
- Disponibilidad de artículos básicos de higiene personal y material de limpieza

ALOJAMIENTO

- Porcentaje de viviendas y alojamientos públicos afectados
- Tipo de vivienda en la zona afectada (de piedra, de planta baja, edificios altos)

AGUA Y SANEAMIENTO

- Daños en el suministro de agua y disponibilidad de agua potable
- Daños en el sistema de saneamiento y efectos en la recogida de basuras y residuos
- Implicaciones para la salud pública

INFRAESTRUCTURA DE TRANSPORTE

- Daños en vías de comunicación, puentes y túneles
- Formas de acceso a la zona afectada
- Puertos o aeropuertos en funcionamiento más cercanos. Capacidad de *handling*

que el volumen de voz de los participantes sea el adecuado así como sus intervenciones, ya que éstas deben ser oportunas, tener contenido y exentas de trivialidad.

La **videoconferencia** es un sistema de comunicación bidireccional de audio, vídeo y datos en tiempo real. Se precisan comunicaciones de banda ancha y en comparación con las audioconferencias son más caras, pero juega a su favor el poder ver las caras de los interlocutores.

En combinación con la videoconferencia suele utilizarse la llamada **conferencia de datos.** En estos sistemas se suele exponer una presentación para acompañar las intervenciones de los interlocutores o hacer uso de herramientas de dibujo mediante una pizarra electrónica. Existen versiones mucho más complejas mediante las cuales a través de aplicaciones específicas se puede trabajar sobre hojas de cálculo o documentos de texto de manera colaborativa.

Los **portales Web** juegan un papel fundamental. Llevan asociadas multitud de herramientas que incluso incluyen algunos de los procedimientos que acabamos de nombrar como videoconferencia, pizarra compartida, motores de búsqueda, sala de chat o repositorios documentales.

La tecnología actual de los portales web reúne características que la hacen muy adecuada a las finalidades de la gestión de la información en el ámbito de las emergencias ya que permite la publicación de información de manera descentralizada sin necesidad de contar con ningún experto TIC del tipo "webmaster[73]".

Y por supuesto el **intercambio de mensajería,** bien física, bien electrónica. Entre el primer grupo encontraremos tanto el **correo postal** a través de agencias de correos, como el de envío de información (en forma de paquete) a través de **empresas de mensajeros.**

Entre el segundo grupo de mensajería no física, encontramos el fax y el correo electrónico. Ya hemos analizado las bondades de los **faxes**. El **correo electrónico (**en inglés *electronic mail* [e-mail]) es similar al correo postal y es utilizado para enviar cartas o cualquier otra información a terceras personas. La diferencia radica en que el correo electrónico es un servicio que funciona por medio de una red de ordenadores permitiendo enviar y recibir mensajes rápidamente mediante sistemas de enlace electromagnéticos. Actualmente, el correo electrónico es una herramienta fundamental por ser un recurso barato que permite comunicarse con rapidez, seguridad y desde cualquier parte del mundo.

DOCUMENTACIÓN ESCRITA

Un **documento** es una información fijada sobre un soporte y susceptible de ser recuperada. Es decir, incluye soporte papel, soporte digital o cualquier otro que se nos ocurra. La importancia del documento es enorme, máxime en la llamada sociedad de la información, en la sociedad del conocimiento.

Un documento es el elemento en el que se transporta y difunde la información o en el que se vierte el conocimiento. Son muchas las clasificaciones o tipos de documentos que se pueden encontrar en el mundo de las emergencias, pero destacan por encima del resto **los informes, las actas y los procedimientos.**

El **informe** es la aportación al entendimiento de una determinada situación. En nuestro ámbito es un escrito que tiene por objeto

73. Un *webmaster* es la persona TIC responsable de mantenimiento, diseño o programación de un sitio web.

NECESIDADES DE INFORMACIÓN ANTE UNA GRAN CATÁSTROFE [III]

VÍVERES

- Impacto en la disponibilidad de comida y acceso a la misma
- Disponibilidad de medios de distribución de alimentos y agua

SUMINISTRO DE ENERGÍA

- Estado de la red de suministro de energía (electricidad, gas, combustibles)
- Disponibilidad de generadores de emergencia en instalaciones críticas
- Disponibilidad de los distintos tipos de combustible y medios de distribución

NECESIDADES DE BÚSQUEDA Y SALVAMENTO

- Porcentaje de colapso estructural que ha causado el desastre
- Tipo de estructuras que han colapsado (hospitales, escuelas, edificios públicos, fábricas de productos potencialmente peligrosos, etc.)
- Necesidad de rescates por medio de helicópteros (personas a las que no se puede evacuar por otros medios)
- ¿Quién está coordinando los medios aéreos implicados y quién está fijando las prioridades de los rescates aéreos?

ORDEN PÚBLICO

- ¿Se han producido o son previsibles problemas como consecuencia del desastre?
- ¿Qué y con qué grado hay que proteger?
- Necesidades de fuerzas militares para colaborar con las FCSE

dar cuenta de una situación desde una perspectiva técnica. Los tipos de documentos a emplear en cada situación suele estar regulado por cada una de las organizaciones, así son muy conocidos los informes de misión (o post-misión).

Las **actas** son documentos que reflejan el desarrollo de una reunión: puntos tratados y decisiones o acuerdos adoptados que a veces pueden tener implicaciones legales o de responsabilidad. Sirven de resumen y recordatorio para todos los implicados en un determinado asunto.

Los **procedimientos** no son una herramienta "pura" de gestión de la información. Cuando una organización decide poner negro sobre blanco, cómo se realiza de manera pormenorizada una tarea, lo que hace es abordar la redacción de un procedimiento técnico. Éstos describen la secuencia y responsabilidades de llevar a cabo las acciones necesarias para alcanzar una meta. Describen al personal, maquinaria y equipos, pero también marcan los flujos de información que se precisan para llevar a cabo la tarea. Sin embargo los procedimientos donde juegan un papel clave es en la **gestión del conocimiento.** Nos explicaremos. El personal experto encargado de redactar los procedimientos vuelca todo su saber en un documento que luego sirve para que otros adquieran esa "sabiduría".

DEFINICIÓN DE FLUJOS

Una parte muy importante de la gestión de la información es que **ésta llegue a todo el que la debe conocer, o quien la tenemos que compartir.** Por ello es sumamente útil definir, normalmente mediante los ya mencionados procedimientos, cual es el **camino de los datos o información cuando llegan a una organización,** y su paso por las distintas dependencias. Lo que es importante para uno, puede que no lo sea para otros y viceversa. La definición del recorrido permite automatizar el diseño de procesos y actividades, identificar al personal responsable de su realización y mejorar el rendimiento detectando **"cuellos de botella".** Estos flujos pueden servirse de herramientas electrónicas, como por ejemplo la publicación en un tablón de anuncios web, o amanuense, una simple chincheta en un tablón de corcho. Una vez más lo importante es el fin, no el medio. Estamos hablando de **difusión** de la información, pero también de **complementación** de la misma por parte de los diferentes gestores de la emergencia.

RITMO DE ACTIVIDADES

En algunas agencias han optado por emplear para este procedimiento el argot militar donde en lugar de "**ritmo de actividades**" se le denomina "**ritmo de batalla**". En ambos casos se trata de la organización de la secuencia de desarrollo de otros procedimientos de gestión de la información tales como desarrollo de reuniones, videoconferencias, remisión y recepción de informes de carácter periódico.

Es decir es un **procedimiento para regular lo rutinario** y no lo extraordinario. Con él tratamos de organizar el tiempo, principalmente el de los responsables de la gestión de la emergencia. Cuando los acontecimientos alteran nuestra agenda nos adaptaremos a ellos de manera flexible y el "ritmo de actividades" nos servirá para no olvidar citas que puedan aportar algo positivo. Nosotros como Responsables TIC deberemos tener muy presente esta agenda ya que ciertos servicios como audioconferencias o

EL CORREO ELECTRÓNICO

En los años setenta se popularizaron principalmente dos símbolos para separar el nombre personal del propietario del correo electrónico y el nombre del dominio o servidor en el cual este correo operaba, los cuatro puntos [::] y [at]. La empresa Digital empezó a utilizar cuatro puntos [::]. Así, las direcciones se configuraban como "nombre::servidor". IBM, en cambio, optó por un lenguaje más natural y con solo dos letras, at. Ellos escribían "nombre at servidor".

El uso de la arroba se atribuye a Ray Tomlinson, inventor del correo electrónico, quien necesitaba una forma de separar el nombre del usuario del nombre del dominio (partes fundamentales de todo correo electrónico). Para ello Tomlinson requería de un carácter que nunca formaría parte del nombre del usuario. Así, eligió la arroba [@] como el símbolo idóneo.

El símbolo arroba tiene distintos nombres según el país. En inglés la arroba es conocida como el símbolo "at", y en otros países tienen otros nombres; muchos de estos países asocian el símbolo a nombres de alimentos o animales.

videoconferencias exigirán unas medidas extraordinarias de gestión de ancho de banda y de uso de especialistas que de no producirse podría llevar a la congestión de los sistemas.

HERRAMIENTAS ELECTRÓNICAS COLABORATIVAS

Aunque perfectamente las podríamos haber integrado dentro de los procedimientos que hemos denominado de contacto a distancia, nos hemos decidido por hacer un apartado específico por su profusión.

Podemos empezar hablando de la **gestión del tiempo** como calendarios o agendas. Los sistemas de **gestión de documentos electrónicos** (EDMS, *Electronic Document Management System*) aprovechan las ventajas del tratamiento de la información electrónica o digital para ofrecer soluciones técnicas que aseguren la actualidad y consistencia de la documentación al tiempo que faciliten su uso compartido y el acceso simultáneo de diferentes usuarios a ella. Otras pueden ser las de **gestión de proyectos** que permite hacer el seguimiento de tareas complejas o aplicación de técnicas de **Minería de Datos**[74] (*Data Mining*) en determinados momentos.

GESTIÓN DEL CONOCIMIENTO DENTRO DE LA PROPIA ORGANIZACIÓN

El conocimiento tiene un valor incalculable para una empresa y ocurre lo mismo para las agencias de emergencia. Sin embargo no se suele prestar la atención necesaria y con demasiada asiduidad vemos como expertos, en los que hemos invertido grandes cantidades de dinero en su formación, se van de la organización llevándose consigo el saber y la experiencia.

Existen muchas maneras de intentar que ese conocimiento sea de utilidad para el resto. Ya hemos mencionado los procedimientos donde se reflejan las técnicas. Del mismo modo podríamos hablar de las "***job descriptions***" o descripciones de los puestos de trabajo que debemos obligar a redactar por el personal de nuestra organización y donde se debe reflejar, no sólo lo que hacen, sino el cómo lo hacen. Esta descripción de los trabajos debe hacerse una vez que el personal sea experto en el mismo, sobre todo en aquellas vacantes que hayamos detectado como básicas o fundamentales.

Otras formas de tratar de conseguir la permanencia del conocimiento en la organización es procedimentar los **relevos**, tanto de puestos como de turnos. Un buen relevo es vital para la continuidad de la organización o del desarrollo de la emergencia.

Finalizamos este capítulo, no sin antes volver a recordar al lector que el **éxito o fracaso del enlace** en una emergencia está altamente condicionado por una adecuada gestión de la información que circula a través de la diversidad de medios que pongamos al servicio de los responsables, que por otro lado serán los que deban hacer la gestión del conocimiento.

74. El *Data Mining* (DM) es aquella parte de la estadística que se usa para problemas que se presentan en el análisis de grandes cantidades de datos, donde las técnicas estadísticas clásicas no pueden ser aplicadas. Generalmente, el Data Mining es el proceso de analizar datos desde diferentes perspectivas con el objetivo de resumir los datos en segmentos de información útiles. Esta idea de DM lleva a la siguiente estructura de conocimiento:

Datos + Estadística → Información

El símbolo → tiene el siguiente sentido: los datos están bien recogidos y la estadística bien aplicada.

CAPÍTULO 8

LA INTEROPERABILIDAD EN LAS EMERGENCIAS

La interoperabilidad es un tema muy antiguo. Cuando nuestros ancestros comenzaron a hablar un mismo dialecto, sin saberlo ya están resolviendo problemas de interoperabilidad. No se trata pues de una traba advenida con la llegada de las nuevas tecnologías, si bien es cierto que su aparición y el ritmo de avance que las sostienen han provocado que sea un campo conocido aunque por el momento **lejos de estar solventado.**

Muchas de las emergencias acaecidas han revelado deficiencias tecnológicas que **impiden el correcto trasvase de información entre intervinientes** de distintas organizaciones. Sanitarios que no pueden hablar con cuerpos policiales; bomberos locales que no tienen modo de comunicarse con otros cuerpos de bomberos de ciudades limítrofes; y todo ello a pesar de la retórica de todas las agencias que reconocen la necesidad de compatibilizar sus medios para resolver la cooperación interinstitucional.

La **interoperabilidad** en las grandes crisis permite la comunicación efectiva entre las agencias que acuden al lugar de la tragedia. Es decir, **articula el enlace** de acuerdo a nuestra definición. Lo que además es muy relevante ya que los esfuerzos necesarios para integrar las telecomunicaciones en una gran emergencia se complican por el hecho de que un incidente a gran escala tiene muchas dimensiones.

La interoperabilidad es la columna vertebral de la respuesta a los incidentes. Sin comunicaciones interoperables entre la policía, los bomberos, los servicios médicos... las vidas de los ciudadanos y

de los profesionales están en riesgo. Para el Responsable TIC de las organizaciones de emergencia los problemas de interoperabilidad serán una preocupación constante.

Aunque pueda resultar obvio debemos señalar que para que exista un problema de interoperabilidad existe como requisito previo que los medios de enlace funcionen correctamente. Un ejemplo clarificará al lector. En las lecciones aprendidas Post-Huracán Katrina publicadas en el 2005, en el apartado Comunicaciones, se señala que en aquellos días no se llegaron a producir problemas de interoperabilidad porque ni tan siquiera funcionaron las telecomunicaciones básicas debido a la destrucción física de los sistemas.

Desde el punto de vista del usuario la interoperabilidad consiste en la capacidad de utilizar aparatos o sistemas, sin tener que preocuparse de los aspectos técnicos. **Desde un punto de vista más formal la interoperabilidad en el enlace de las emergencias** se refiere a la habilidad de las organizaciones implicadas de poder comunicarse en tiempo real entre ellas cuando se precisa, en condiciones óptimas y de la manera preestablecida, teniendo como efecto un conocimiento común y compartido de la situación entre todos los participantes y sus cadenas de mando. Es decir que la interoperabilidad o **interoperatividad** es la condición que permite que sistemas o productos diferentes puedan relacionarse entre sí, para coordinar procesos o intercambiar datos durante una emergencia.

La **solución formal** promovida desde los más altos estamentos gubernativos pasa por el **desarrollo de estándares de tecnología abiertos** que hagan posible que productos y plataformas heterogéneas se comuniquen entre sí, y se intentan dar a conocer mediante la **publicación de Normas o Estándares.**

La Interoperabilidad en general, y en el mundo de las emergencias en concreto, busca la eliminación de las barreras que bloquean el intercambio de información entre instituciones y sistemas. **Los resultados no son buenos.** Se lleva años hablando de la resolución de problemas de interoperabilidad y sin embargo se ha avanzado bastante poco en comparación con el tiempo y el esfuerzo invertido.

Los sistemas de gestión de las agencias de respuesta a emergencias deben ser compatibles tanto dentro (Intraoperatibilidad) como fuera de la propia institución (Interoperabilidad). Aunque normalmente la inquietud se focaliza en la compatibilidad con otras agencias, el primero de los problemas a afrontar es la total compatibilidad de sistemas dentro de la propia organización. Esta problemática intra agencia tiene las mismas características que de cara al exterior. Lo más distintivo es que normalmente el volumen de medios y sistemas que hay que hacer compatibles suele ser menor, y a nada que haya habido algún Responsable TIC que haya puesto algo de cordura en la compra y diseño de sistemas, la solución será viable. Por tanto superado este trámite se acometerá la problemática inter agencias.

INTEROPERABILIDAD EN UN CONTEXTO DE EMERGENCIA

En abril de 1999, dos estudiantes de 16 años de edad, entraron en el Columbine High School en Littleton, Colorado, y comenzaron un tiroteo que dejó 15 muertos y decenas de heridos. A los pocos minutos de los primeros disparos, la policía local, paramédicos, y bomberos llegaron al lugar. En las horas siguientes, se les unieron casi 1.000 agentes de 20 departamentos de policía de la zona, 12 cuerpos de bomberos, 46 ambulancias y 2 helicópteros. Sin embargo, no existía un único sistema de telecomunicación que permitiera a los diferentes organismos coordinarse entre sí. Cada agencia trató de utilizar su propio sistema de radio por lo que a los pocos minutos aquellas agencias que inicialmente tenían su sistema establecido se deterioraron rápidamente. Los teléfonos móviles tampoco pudieron ser una alternativa, ya que cientos de periodistas se apresuraron a informar con sus celulares a sus cadenas y colapsaron las estaciones base.

La interoperabilidad es muy difícil de garantizar en un contexto de emergencia por muchas razones. Entre ellas se encuentran las siguientes:

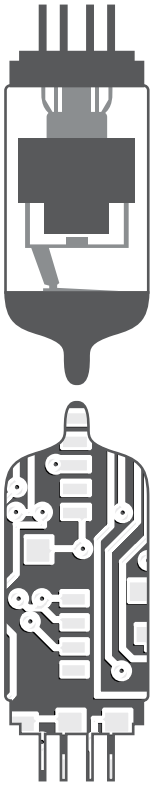
- **Incompatibilidad tecnológica**. Encontramos agencias cuyos intervinientes acuden a la emergencia con modernísimos sistemas de telefonía móvil digital, frente a otros que llevan *walkie- talkies* comprados en bazares orientales.
- Incluso usando sistemas similares, pongamos el caso de equipos de radiofrecuencia, la incompatibilidad es manifiesta por multitud de razones:
  - El **problema técnico** fundamental es que los organismos tienen sistemas que usan diferentes frecuencias y formas de onda, distintos protocolos, bases de datos incompatibles, y equipamientos de multitud de fabricantes.
  - La **falta de frecuencias** de funcionamiento comunes. Por razones históricas, agencias de servicio público como la policía, los bomberos, emergencias médicas han utilizado diferentes bandas de

frecuencia para las comunicaciones de sus radios. Una solución a la interoperabilidad, pobre aunque puede que efectiva en ocasiones, es la de intercambiar equipos entre organismos.

- **Equipos analógicos frente a otros digitales.** Todavía hay muchas organizaciones de socorro que se basan principalmente en la tecnología analógica. Aunque las tecnologías analógicas tienen algunas ventajas frente a las digitales. En el día a día estos sistemas analógicos funcionan adecuadamente y cubren las necesidades de enlace. Esto implica que la motivación para la adquisición de nuevos y más modernos sistemas digitales es baja. Sin embargo, generalmente son incapaces de absorber el gran volumen de tráfico que caracteriza los incidentes graves. Las deficiencias de estos sistemas no pueden suplirse por ejemplo con la mera adición de más canales. Aunque se pueda aliviar el problema de forma temporal, el espectro y el ancho de banda es limitado. Un uso más eficiente del espectro se puede conseguir mediante la utilización de sistemas digitales. En Nueva York el 11 de septiembre de 2001, las comunicaciones del Departamento de Bomberos[75] se basaban en dos tipos de radios diferentes, unas digitales con ocho años de antigüedad y otras analógicas con quince años, que por supuesto no eran compatibles entre sí.

- **Aislamiento entre agencias** en la adquisición de sistemas de enlace. No existen normas o leyes que les obliguen, por lo que por regla general los organismos compran o definen sus sistemas de forma independiente **sin tener en cuenta un escenario de cooperación** con otros actores. Además, las soluciones a la interoperabilidad técnica son "*ad hoc*" y no suelen valorar otros condicionantes operacionales. La naturaleza de las misiones de las diferentes agencias y el clima político en el que tradicionalmente operan hacen aún más difícil plantearse el cambio de sus sistemas por otros interoperables con organismos vecinos. Por lo tanto, es poco probable que las agencias estén alguna vez motivadas para resolver los problemas de cooperación interinstitucional, al menos que por decreto de un ente superior, les obligue a olvidar las rivalidades entre agencias y las luchas políticas internas. Los esfuerzos para lograr la interoperabilidad deben trabajar dentro de esta realidad de la resistencia organizacional como ampliaremos más adelante.
- Tenemos también que nombrar la **incapacidad para anticipar todos los posibles escenarios comunes de operación** entre los organismos. Por ejemplo ante un accidente en un aeropuerto puede que aparezcan agencias que jamás hayan tenido la necesidad de ser interoperables. Ya hemos mencionado en otros capítulos lo difícil que resulta elegir o identificar qué sistemas TIC son más apropiados en cada momento. Una dificultad que se multiplica en un entorno incierto.
- **Inclusión de los sistemas heredados.** Cuando en una organización se decide hacer una migración hacia otras TIC más modernas, en muchas ocasiones no se hace a la vez para todos sus componentes. Esto obliga a trabajar simultáneamente con dos sistemas: los nuevos y los heredados. Éstos últimos, que serán bastante antiguos, casi con toda seguridad que no fueron diseñados para ser fácilmente integrables en los actuales.

ANALÓGICO VS DIGITAL



VENTAJAS DE LAS COMUNICACIONES ANALÓGICAS

- Los dispositivos de comunicaciones analógicos son más fáciles de hacer interoperables porque sólo es necesario hacer coincidir las frecuencias de comunicación de aparatos de radio, mientras que los sistemas digitales requieren el paso adicional de hacer coincidir sus protocolos de comunicaciones.
- Los problemas en dispositivos de comunicaciones analógicas son más fáciles de diagnosticar y de solucionar que en los sistemas digitales.
- El número de técnicos y usuarios experimentados en el uso de los sistemas analógicos hasta la fecha es mayor.
- Las comunicaciones analógicas ofrecen un mejor comportamiento ante la degradación que la ofrecida por sistemas digitales ante la presencia de ruido.
- La comunicaciones analógicas a baja frecuencia están menos sujetas a restricciones de línea de visión directa y por lo tanto tienen una mayor probabilidad de penetrar en la mayoría de las paredes o escombros.

75. Los oficiales de bomberos habían informado previamente y en reiteradas ocasiones de que en los incendios que se producían en edificios de gran altura siempre se presentaban problemas insalvables de telecomunicaciones.

DIMENSIONES DE LA INTEROPERABILIDAD

Las primeras propuestas para contrarrestar los problemas de interoperabilidad en el campo de las emergencias se basaron en una **perspectiva puramente tecnológica.** Es decir se trataron de definir estándares a los que los diferentes fabricantes debían acogerse para asegurar el correcto funcionamiento entre equipos de distinta procedencia. El éxito de este primer intento es más que cuestionable ya que las empresas en su mayoría trataron de imponer sus patrones, resultando vencedora la empresa que ganaba el mercado. Pero no fueron todo fracasos, aunque no está relacionado directamente con las emergencias el ejemplo más notable es quizá la arquitectura TCP/IP desarrollada a partir de diversas normas de la Internet *Engineering Task Force* (IETF), que permitió la interconexión de un gran número de redes distintas para conformar Internet.

Un segundo intento fue la imposición del concepto de **Trabajo en Red**. El concepto **NEC**, por su acrónimo inglés (*Network Enabled Capability*), comenzó promoviendo la conexión física de todos los colectores de información, uniendo en un mismo entorno los responsables que tomaban decisiones con quienes las ejecutaban. De esta manera se conseguía unidad, coherencia y sincronismo en los efectos deseados y se multiplicaba así el potencial de las organizaciones intervinientes. Todo el mundo estaba en la misma red física y sólo había que aplicar reglas de seguridad, el llamado "***need to Know***", es decir la información está accesible si se tiene necesidad de conocerla y el propietario da permiso para que acceda, por ejemplo proporcionándole un usuario y una password. Este concepto tuvo su eco y al menos se consiguió que dentro de la propia organización todos estuvieran en la misma red. Es decir, se resolvió el problema "Intraoperacional", sin embargo no se alcanzaron buenos resultados en la cooperación entre diferentes agencias.

Para tratar de mitigar este fracaso se decidió ampliar este concepto de interoperabilidad basado en el trabajo en red y se añadieron **dos dimensiones adicionales.** A la dimensión técnica, se sumaron la dimensión social y la del conocimiento.

Por tanto este nuevo planteamiento para afrontar la interoperabilidad contempla tres dimensiones:

- Como ya hemos reflejado la dimensión tecnológica impulsa la conectividad física. Es la que aboga por crear una red o al menos un canal de comunicación basado en la tecnología que dé el soporte para generar, adquirir, distribuir y manipular la información. Esta dimensión es imprescindible.
- Tener dos organizaciones unidas tecnológicamente no significa que puedan o quieran interoperar. Como hemos visto existe resistencia organizacional a cooperar con otros. La dimensión social incita a crear redes de personas con intereses similares o interrelacionados, que interactúan para conseguir mutuo apoyo formal o informal. Es la dimensión humana de toda relación que resulta clave para contribuir a confiar en otras personas o en otras organizaciones. Es una manera de quitar reticencias y desconfianzas.
- Por último la dimensión del conocimiento. Se sitúa en la mente de la gente y es donde residen la percepción, la conciencia, la comprensión, las creencias y los valores. Es la que como seres racionales nos ayudará a obviar otros condicionantes añadidos en aras de un objetivo común, la compartición total de la información que sirve para alcanzar el conocimiento global.

En la intersección de estas tres dimensiones es donde a priori se conseguirá una mayor interoperabilidad.

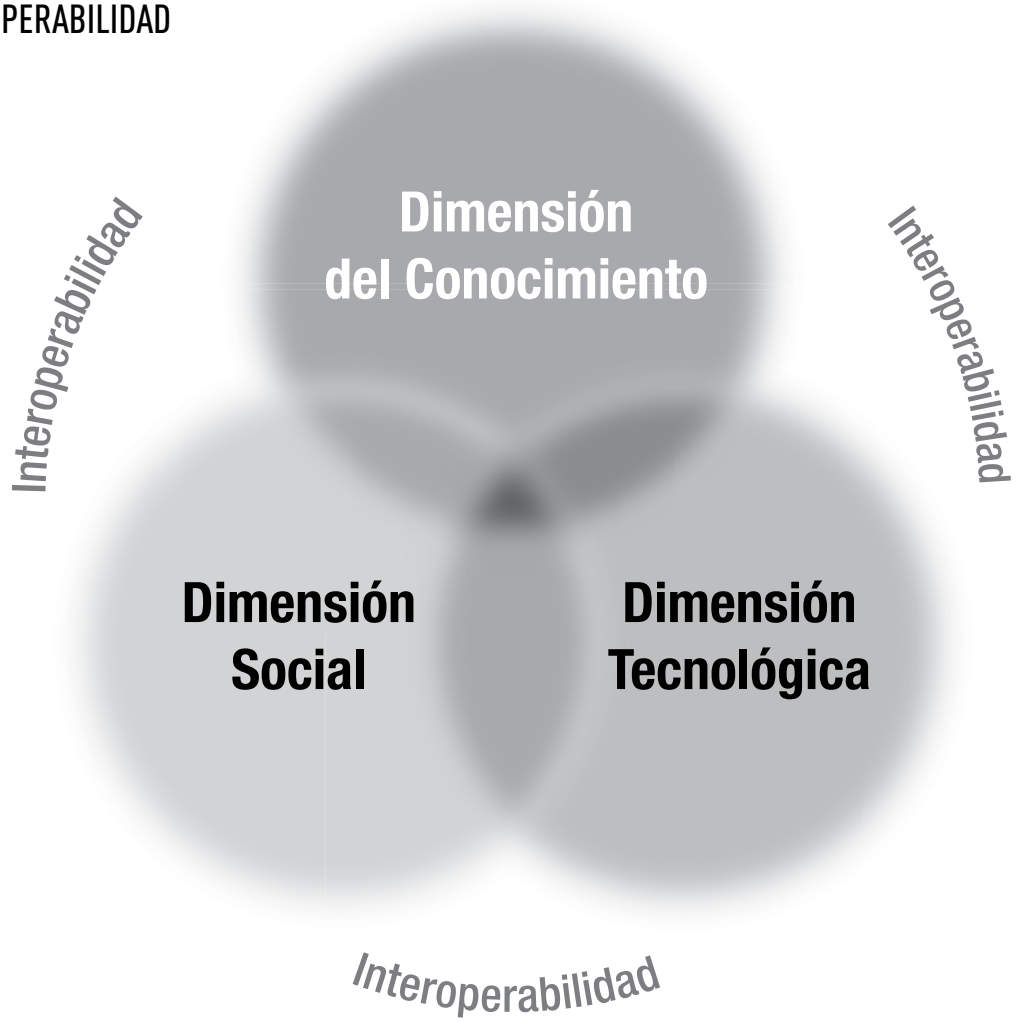
Sin embargo el lector se dará cuenta rápidamente que este concepto se olvida un tema capital como es el de los **intereses económicos,** que a la postre va a resultar determinante para no llegar a la deseada interoperabilidad.

La Interoperabilidad comienza a ser una **preocupación acuciante para las Administraciones Públicas** en todo el mundo. Los gobiernos en la actualidad entienden la interoperabilidad como un concepto más amplio. En este sentido, la **Comisión Europea** define interoperabilidad como la habilidad de organizaciones y sistemas dispares y diversos para interaccionar con objetivos consensuados y comunes y con la finalidad de obtener beneficios mutuos. La interacción implica que las organizaciones involucradas compartan información y conocimiento a través de sus procesos de negocio, mediante el intercambio de datos entre sus respectivos sistemas TIC. Vemos por tanto que va muy en línea con las tres dimensiones antes expuestas.

En España la **Ley 11/2007**, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos[76], reconoce el protagonismo de la interoperabilidad y se refiere a ella como uno de los aspectos en los que es

76. En su artículo 42 crea el Esquema Nacional de Interoperabilidad. El Esquema Nacional de Interoperabilidad (ENI), regulado por el Real Decreto 4/2010, de 8 de enero, establece el conjunto de criterios y recomendaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad. El ENI se encuentra alineado con la Estrategia Europea de Interoperabilidad y el Marco Europeo de Interoperabilidad.

DIMENSIONES DE LA INTEROPERABILIDAD



obligado que las previsiones normativas sean comunes y debe ser, por tanto, abordado por la regulación del Estado.

En **Estados Unidos** han ido mucho más allá. En 2007, a través de su Dirección de Protección Nacional y Programas, el Ministerio de Interior o Departamento de Seguridad Nacional (*Department of Homeland Security-DHS*) decidió establecer la **Oficina de Comunicaciones de Emergencia (OEC)** para reforzar la capacidad de los servicios de emergencia de los estados federales para acelerar y alcanzar la interoperabilidad de las telecomunicaciones en caso de catástrofes naturales, desastres, actos de terrorismo, u otro desastre hecho por el hombre. Desde su creación, OEC ha operado bajo el principio de que cualquier esfuerzo para mejorar la interoperabilidad en las comunicaciones de emergencia debe tener en cuenta los puntos de vista de todos los servicios de emergencia, desde el nivel más bajo de intervinientes desplegados en la misma zona de emergencia hasta los más altos escalones federales de dirección.

Como se indica en el **Plan de Comunicaciones de Emergencia Nacional (NECP),** lograr la interoperabilidad, las metas, los objetivos y las iniciativas prioritarias no es una tarea que pueda alcanzar por sí solo el Gobierno Federal, sino que exige un esfuerzo de coordinación entre todas las partes interesadas.

Es evidente que aunque desde estas páginas **aboguemos por imitar en nuestro país la línea marcada por el gobierno estadounidense, tanto a nivel central como de las Comunidades Autónomas,** nos queda un largo camino por hacer.

ANALÓGICO VS DIGITAL

VENTAJAS DE LAS COMUNICACIONES DIGITALES

- Las comunicaciones digitales ofrecen una mayor fidelidad y menor susceptibilidad a la interferencia en comparación con las comunicaciones analógicas
- Las comunicaciones digitales son inherentemente más seguras y más fácilmente codificables que las comunicaciones analógicas
- Los canales (frecuencias) pueden ser compartidos entre usuarios, aumentando así el número de usuarios que pueden hacer uso de un mismo canal
- Como los canales pueden ser compartidos, varios usuarios pueden hablar a la vez en una misma frecuencia, aumentando así la cantidad de información que puede ser intercambiada de manera simultánea.

INTEROPERABILIDAD OPERACIONAL Y TÉCNICA

Vaya por delante que **no nos gusta esta clasificación o distinción,** sin embargo la comentaremos por aparecer recurrentemente cuando se habla de interoperabilidad "operativa", entendida como la que se lleva a cabo en las operaciones de emergencia. Nos referimos a la interoperabilidad en los niveles técnicos y operacionales.

La **interoperabilidad técnica** se refiere a la capacidad de los sistemas para el intercambio de información o servicios directamente entre usuarios. La interoperabilidad técnica implica intercambiar "datos" entre equipos, sin que ello signifique que necesariamente la información transferida pueda ser interpretada correctamente por los usuarios. Es evidente que nos estaríamos refiriendo a la **perspectiva puramente tecnológica** de las tres dimensiones que componen la interoperabilidad según lo explicado en el párrafo anterior.

Por el contrario, la **interoperabilidad operacional** se refiere a la capacidad de los diferentes organismos (policía, bomberos, búsqueda y rescate, servicios sanitarios, etc.) de intercambiar información con otras agencias y utilizarla en apoyo de sus propios objetivos. Por lo tanto la interoperabilidad operacional va más allá de la interoperabilidad de equipos, e incluye personas y procedimientos. Aquí vemos que se aproxima a las otras dos dimensiones mencionadas, la social y la del conocimiento, aunque si bien desde un punto de vista mucho menos preciso.

LA RESISTENCIA ORGANIZACIONAL

Una vez más regresamos a la mañana del 11 de septiembre de 2001. Minutos después de la caída de la Torre Sur del World Trade Center, helicópteros de la policía inspeccionaban la Torre Norte. Una de las conversaciones grabadas de los pilotos indicaba que "unos 15 pisos por debajo desde la azotea, se ven las vigas metálicas de la estructura al rojo vivo. El colapso es inevitable". Unos segundos después, otro piloto informó: "Yo no creo que esta torre aguante mucho más. Ordenad evacuar la torre inmediatamente".

Estos mensajes fueron transmitidos 21 minutos antes del derrumbe de la segunda torre, y fueron recibidos por casi todos los agentes de policía, la mayoría de los cuales lograron escapar. Sin embargo, los 121 bomberos que se encontraban en esos momentos en la torre norte nunca escucharon las advertencias. El sistema radio del Departamento de Bomberos había demostrado ya ser poco fiable esa mañana, incluso para asegurar sus propias operaciones; y por supuesto no era compatible con el de la policía de Nueva York.

Una respuesta eficaz a un incidente terrorista como el de aquel día, **debería haber exigido una respuesta multi-agencia coordinada.** Las barreras técnicas seguramente eran conocidas para superar la interoperabilidad, pero de ningún modo podrían llegar a justificar por qué las agencias no cooperaban eficazmente.

Efectivamente, es necesario tener en cuenta que el carácter y la idiosincrasia de los cuerpos de emergencia tienen un profundo impacto en su capacidad y voluntad de cooperar. Las "guerras" o rivalidades entre organizaciones son comunes. Aunque todas reconocerán la necesidad de la

cooperación con otros organismos, la realidad es muy diferente de la retórica, y en la práctica se revelan graves deficiencias en el alcance y la naturaleza de la cooperación interinstitucional.

Durante la jornada del 11S se manifestaron una serie de barreras culturales que dificultaron sobre manera la cooperación entre Policía y Bomberos:

- Los helicópteros de la policía, aunque hubieran podido proporcionar valiosísima información a los bomberos acerca del progreso del fuego en las partes superiores de los edificios, así como cierta capacidad de rescate aéreo de aquellos que se subieron a las azoteas, nunca fueron utilizados para esos fines. Uno de los oficiales de bomberos trató de solicitar a la policía que los helicópteros les pasaran información, pero ni tan siquiera pudo contactar con su puesto de mando. Tampoco los puestos de mando de ambas agencias estaban solapados. Los bomberos pusieron el suyo en el hall de una de las torres, mientras que la policía lo hizo en otro edificio situado a doscientos metros.
- Aunque la Policía y Bomberos tenían firmado un acuerdo desde 1993 para compartir helicópteros de la policía durante los incendios en edificios de gran altura, jamás llegaron a realizar una sola práctica.
- Si bien la mayoría de los estados y el gobierno federal tenían firmados acuerdos entre agencias para dirimir quien lidera la resolución de una emergencia, tal documento no existía en la ciudad de los rascacielos.
- Los Bomberos culparon a la Policía, y ésta culpó a los Bomberos de la falta de voluntad para cooperar. Algunos policías pensaban que era sumamente difícil trabajar con los bomberos porque eran poco disciplinados, mientras que los bomberos afirmaron tras la catástrofe que la policía decidió por si sola que ella debía liderar la crisis sin contar con nadie más.
- Tras la desgracia, un funcionario de Bomberos de alto rango dijo que "no hay duda de que hubo algún problema de comunicación", mientras que un alto representante del Departamento de Policía afirmó que "en aquel momento yo no era consciente de que ese día estábamos teniendo dificultades de coordinación".

No hay respuestas fáciles para salvar abismos culturales entre agencias que no interactúan en el día a día o realizan simulacros y ejercicios de manera regular. Diferentes agencias con diferente historia, misiones distintas y aisladas en el día a día, normalmente darán como producto diferentes políticas, distintos procedimientos y puede que hasta filosofías de trabajo diferentes ante unas mismas circunstancias.

La cultura organizacional y las características de cada organización puede que funcionen correctamente aisladas. Pero en una crisis, ante situaciones extremas, la diferencia interinstitucional no puede ser superada por decreto. Tenemos por tanto que buscar alternativas. Y los Responsables TIC en medio de este dilema. Quizás sea mucho pedir que seamos nosotros los que rompamos tan gran resistencia, pero lo que no permite ningún género de dudas es que, a nuestro nivel, y hablando con nuestros homólogos TIC "del otro lado de la colina" deberemos aportar nuestro granito de arena.

PROPUESTAS PARA ALCANZAR LA INTEROPERABILIDAD EN EL SIGLO XXI

A tenor de lo expuesto en este capítulo, un reto decisivo para los gestores de las emergencias en general, y para los Responsables TIC a su nivel, es la **creación de las condiciones necesarias para asegurar la interoperabilidad** tanto dentro como fuera de nuestra agencia.

Las soluciones a la interoperabilidad en las emergencias no pueden centrarse únicamente en los equipos o tecnología, con exclusión de los otros factores que también son fundamentales para el éxito. Esto sería atacar las resistencias sólo en una de las tres dimensiones que componen este problema. Al igual que ha hecho Estados Unidos se deben identificar los campos donde trabajar para irle ganando terreno a la falta de coordinación.

Propondremos por tanto una serie de iniciativas multidisciplinares que abarquen las tres dimensiones de la interoperabilidad, y a la tecnológica le sumaremos la social y la del conocimiento.

CREACIÓN DE UN COMISIONADO NACIONAL TIC DE EMERGENCIAS

Este asunto es tan serio y de tanta trascendencia que entendemos que en la **Secretaria de Estado de Telecomunicaciones del Ministerio de Industria** se debería crear un organismo que dirigiera y coordinara a nivel Estado todos los asuntos relacionados con las TIC en emergencias.

REGULACIÓN NORMATIVA DE ALTO NIVEL

La configuración autonómica del Estado favorece la regulación regional de muchas materias y por tanto la tendencia es incluir también las TIC cuya repercusión excede a nuestro entender los ámbitos fronterizos de cada Comunidad. Sería por tanto necesaria la promulgación de leyes de obligado cumplimiento que regularizaran criterios mínimos de cumplimiento en materia de equipación, configuración y administración de los sistemas de gestión de emergencias. El objetivo sería la materialización de un **Plan Nacional de Interoperabilidad.**

TECNOLOGÍA

Por supuesto se debe seguir avanzando en la cuestión tecnológica, pues como vimos sin ella la interoperabilidad se convierte en utópica. Los precios de mercado de los productos TIC condicionan la instalación de unos productos u otros, pero deberían marcarse, bien por ley, bien por pactos, **las tecnologías a diez años** que se pueden utilizar, para que así todo el mundo se adhiriere a las mismas.

Dejando un poco de lado el concepto filosófico y yéndonos a fines prácticos, estas observaciones sugieren que cuando se requiere una respuesta multiagencia ante una gran catástrofe, todos los sistemas, propios y ajenos, deben concebirse o **tener previsto migrar hacia una estructura de red interoperable en la trabajen los organismos involucrados,** y que dicha transición se lleve a cabo con la mínima interrupción posible.

Al trabajo en red se le suman otras iniciativas como la investigación en la definición de nuevos protocolos y desarrollos de tecnológicos que puedan facilitar la interconexión y la interoperación de diversas fuentes. Por

ejemplo, las radios programables por software pueden (en principio) permitir que una sola radio pueda interoperar con una gran variedad de equipos a priori incompatibles. Un segundo ejemplo es una arquitectura de comunicaciones que traduzca la información de cada agencia a un formato común consensuado y que de esta manera todos puedan acudir a **este "cesto" de información.**

Téngase en cuenta también que los nuevos enfoques técnicos no son la única opción para ayudar a facilitar el enlace cuando la interoperabilidad está en entredicho. Por ejemplo, se pueden implementar políticas de priorización en las redes públicas tal como aboga el Convenio de Tampere, o reservar parte del espectro dedicado a los servicios de emergencia y exigir por ley que se utilicen estas frecuencias. Una tercera opción sería exigir configuraciones exactas para los equipos (radios, informáticos, etc.) de los servicios de emergencia para que sean interoperables. Estas políticas por supuesto que no serían mutuamente excluyentes.

PROCEDIMIENTOS OPERATIVOS

No nos referimos en exclusiva a los procedimientos que cada organización seguro que tiene y practica para automatizar sus intervenciones en las emergencias. Nos estamos centrando en procedimientos operativos de cooperación entre distintas agencias que están predestinadas a actuar juntas en las emergencias.

ENTRENAMIENTO Y EJERCICIOS

Prácticamente unido al apartado anterior está la puesta en práctica de los procedimientos de colaboración redactados entre las organizaciones, porque si no se testan, se adaptan y actualizan periódicamente, acaban convirtiéndose en papel mojado.

Estos procedimientos operativos y estos simulacros en los que se llevan a la práctica **favorecen el clima de confianza y disminuye los recelos entre organismos.** De esta manera se podrá llegar al entendimiento común de la situación que es la base para llevar a cabo la gestión de la emergencia con unidad de esfuerzos y confianza recíproca entre intervinientes.

Los directores o mandos de la emergencia deben establecer conexiones humanas, construir confianza, y crear y mantener la comprensión compartida. La colaboración eficaz proporciona un foro, permite diálogo en el que los participantes informarán de los cambios, y las organizaciones podrán aprender una de la otra, y crear soluciones conjuntas.

El **establecimiento de una cultura de colaboración** es difícil pero necesario. La creación de una comprensión compartida de los problemas, preocupaciones y habilidades de los mandos, subordinados y socios lleva una inversión de tiempo y esfuerzo. Los líderes con éxito hablan con la gente del staff, con los líderes subordinados, y con los organismos que trabajan en la emergencia codo con codo. A través de la colaboración y el diálogo, los participantes comparten información y perspectivas, hipótesis, preguntas e intercambian ideas para ayudar a crear y mantener un entendimiento compartido y el propósito común. Como el lector observará esta **filosofía aboga por cambio de disposición.**


112

CAPÍTULO 9

CENTROS DE GESTIÓN DE EMERGENCIAS

Las TIC que sustentan en la mayoría de las ocasiones el enlace aparecen en infinidad de escenarios. Llevamos ocho capítulos desmenuzando las características del enlace, los diseños y fases de una emergencia. Hemos visto los sistemas de telecomunicaciones y de información de los que nos valdremos, y también nos hemos concienciado de lo mucho que hay que trabajar en la gestión de la información y en la interoperabilidad. Sin embargo hasta este momento sólo hemos hablado tangencialmente de los **escenarios y lugares** desde donde se dirige la emergencia.

La gestión de la emergencia se realiza en distintos niveles y desde distintas ubicaciones. Por supuesto los equipos intervinientes aportan su trabajo desde el mimo lugar de los hechos, pero también encontramos puestos de mando que se despliegan en los alrededores y centros que llevan a cabo sus tareas desde la distancia. La ayuda que proporcionan los medios de enlace a los usuarios es muy valorada y las organizaciones no han sido inmunes a este "virus" y se han equipado con distintas **infraestructuras que albergan los medios tecnológicos** más adecuados a cada uno de sus respectivos cambios de actuación. Al conjunto de la infraestructura la vamos a denominar **Centro de Gestión de Emergencias.** Y al grupo de medios TIC contenidos en estos centros les pasaremos a denominar **Plataformas Tecnológicas de Gestión de Emergencias**.

Por tanto, en este capítulo haremos un recorrido por los diferentes tipos de centros de gestión que nos podemos encontrar empezando por mencionar las principales características de las plataformas tecnológicas que los sustentan.

PLATAFORMAS TECNOLÓGICAS

Las Plataformas Tecnológicas son una exigencia de eficacia en el sector de las emergencias. Los Centros de Gestión de Emergencias pueden hacer el trabajo sin ellas, pero no con los mismos resultados. Estas Plataformas Tecnológicas se han convertido en sumideros de información que sirven de apoyo a los gestores de las emergencias.

Están equipadas con medios para asegurar el enlace (fundamentalmente TIC), y **dotadas de personal altamente cualificado.** Las Plataformas se caracterizan por su valor estratégico en la gestión de situaciones de emergencia y su alta disponibilidad y especialización justifican en un porcentaje muy alto el coste de su implantación.

Las principales actividades que se desarrollan en los Centros de Gestión están basadas en estas Plataformas Tecnológicas, destacando como ya hemos visto en capítulos anteriores del libro, la gestión de la información para facilitar a los responsables la comprensión de la situación durante el trascurso del incidente.

Las Plataformas Tecnológicas Españolas han surgido en algunos casos como resultado de la aplicación de normativa europea (caso de los 112) o como herramienta para cubrir las necesidades específicas de organizaciones. Por lo tanto podemos decir que en nuestro país han sido fundamentalmente promovidas por las **Comunidades Autónomas y Ayuntamientos** con importantes recursos económicos. Han contado en su diseño con la participación con los agentes científicos y tecnológicos, muchas veces procedentes de las universidades. Un caso especial son las plataformas de otros colectivos, como el militar que suelen contar con sus propios diseñadores y recursos mucho más limitados, al menos en España.

CLASIFICACIÓN DE LOS CENTROS DE GESTIÓN DE EMERGENCIAS EN BASE A LA MOVILIDAD

Las principales características de las Plataforma Tecnológicas están orientadas a garantizar un soporte eficaz a la gestión de las emergencias. Destacan las siguientes:

INSTALACIONES FIJAS

- Anclados al terreno
- Alejados normalmente del lugar de la emergencia

PLATAFORMAS DESPLEGABLES

- Despliegan cerca de la emergencia. Operan en parado. Cambios de asentamiento "no programados".

PLATAFORMAS MÓVILES

- Se mueven por la zona de la emergencia.
- Operan en movimiento.
- Cambios de asentamiento continuos.

CENTROS DE EMERGENCIA CLASIFICADOS SEGÚN SU MOVILIDAD

- Disponibilidad, para garantizar su funcionamiento durante todas las fases de la emergencia.
- Capacidad, para atender el nivel máximo de esfuerzo para el que esté diseñada.
- Escalabilidad, para poder crecer o decrecer en tamaño y servicios según la necesidad.

Vista la plataforma que sustenta el enlace nos vamos a adentrar a continuación en los Centros de Gestión de Emergencias propiamente dichos. Se pueden tomar distintos **criterios** para clasificarlos (propietario, función, tecnologías implementadas,...). Sin embargo nos hemos decidido por la **movilidad de la plataforma en la que van instalados** por ser, a nuestro entender, el hecho que marca mayor diferencia entre unos y otros.

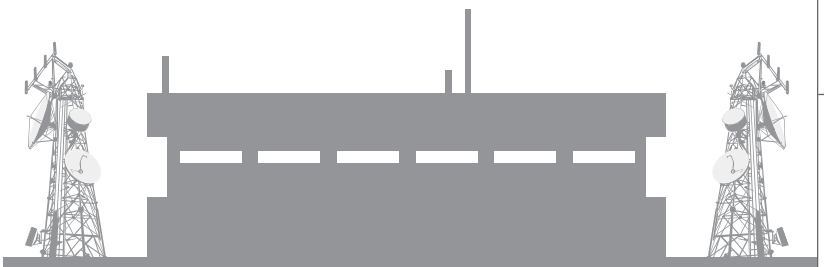
CENTROS DE GESTIÓN FIJOS.

Son aquellos que **no se pueden mover**, situados en el suelo y que se encuentran albergados en construcciones más o menos robustas. Son por tanto **vulnerables** a las fuerzas de la naturaleza o a los accidentes provocados por la mano del hombre, sólo por el hecho de estar anclados al terreno.

La mayoría de ellos se diseñan para prestar un servicio **24 horas** al día los **365 días** del año. Emplean la **redundancia de medios y sistemas** para alcanzar un alto grado de disponibilidad en situaciones de normalidad o afectadas por algún tipo de catástrofe. Tienen **asegurado el suministro de energía** mediante múltiples puntos de acometida exterior, provenientes a su vez de distintos proveedores de electricidad. Cuentan con potentes grupos electrógenos con capacidad de soportar y redundar las necesidades energéticas de la Plataforma Tecnológica, o incluso de todo el Centro al que atiende dicha plataforma.

Para asegurar la disponibilidad cuentan con toda o parte de la **plataforma tecnológica duplicada.** Unos lo hacen dentro del mismo centro y otros apuestan por llevarlos a lugares distantes y así asegurar que un mismo hecho (inundación, terremoto...) no pueda dejar fuera de servicio la plataforma tecnológica principal y de respaldo. Así por ejemplo la Junta de Andalucía tiene su plataforma distribuida en tres centros provinciales, y la Región de Murcia y las Islas Canarias tienen acordado respaldarse entre sí en caso de fallo de las respectivas plataformas.

Estos Centros Fijos son muy **caros** de construir y de mantener. Exigen una **supervisión** constante y un personal muy preparado, tanto para la gestión como para



CENTROS DE GESTIÓN
DE EMERGENCIAS FIJOS

CARACTERISTICAS PRINCIPALES

- "Máximas" capacidades de enlace y comodidades
- Anclados al terreno
- Vulnerables
- Se soluciona con la redundancia en la plataforma tecnológica
- Importante el diseño y dimensionamiento inicial
- Muy Caros
- Mantenimiento y supervisión constante
- Alta disponibilidad

la administración de los sistemas TIC. Es muy importante el **diseño inicial y su dimensionamiento**, ya que la flexibilidad para modificar lo inicialmente planeado es muy limitada.

Los ejemplos más conocidos y evidentes de este tipo de centro fijo son los Centros de Emergencia 112 de las CCAA, aunque existen otros similares en organismos especializados como pueden ser Red Eléctrica de España, CLH o Enagás.

CENTROS DE GESTIÓN DE EMERGENCIAS DESPLEGABLES.

Son aquellos centros que tienen **capacidad de moverse, se aproximan y despliegan cerca de la emergencia.** Sin embargo **no pueden operar en movimiento** por lo que están obligadas a operar en parado. Por lo tanto son menos vulnerables que los fijos al no estar anclados al terreno.

La mayoría de ellos se diseñan para prestar un **servicio 24 horas al día, durante la duración de la emergencia.** Es decir, no están diseñados, ni en medios materiales ni en personal, para operar 365 días al año.

Se intenta y se consigue **cierta redundancia** de medios y sistemas de la plataforma tecnológica, pero las dimensiones reducidas de los vehículos en la que van instaladas la constriñe. Por lo tanto la **disponibilidad es menor**.

Si tienen opción pueden operar enganchados a la red eléctrica, aunque en la mayoría de los casos lo hacen con grupo electrógeno.

Las **capacidades** en servicios **TIC son menores** que en los centros fijos.

Realizan **cambios de asentamiento** "no programados". Es decir, suelen llegar a las proximidades de la emergencia y buscan un asentamiento con la idea de continuidad. Sólo cambian de ubicación por problemas mayores. Por ejemplo en los incendios forestales hay veces que el viento cambia de dirección y puede llegar a amenazar el puesto de mando del Director de Extinción.

Es fundamental su diseño y dimensionamiento, aunque las modificaciones son posibles, más sencillas y económicas que en un centro fijo.

Sólo el movimiento hasta el lugar de la emergencia condiciona la operatividad de los medios ya que pueden sufrir movimientos involuntarios y vibraciones que dañen o desconecten componentes electrónicos. Esto exige un **mantenimiento y una supervisión muy exigente** para mantener la operatividad.

Los Centros de Gestión de este tipo más conocidas son los

CARACTERISTICAS PRINCIPALES

- Se pueden desplazar
- "Menores" capacidades de servicios TIC
- Se intenta una mínima redundancia en la plataforma tecnológica
- Fundamental diseño y dimensionamiento
- Menor grado de disponibilidad
- Sólo el movimiento hasta la emergencia condiciona la operatividad de los medios
- Mantenimiento y supervisión exigente para mantener operatividad

CENTROS DE GESTIÓN DE EMERGENCIAS DESPLEGABLES

llamados camiones PMA donados por la Fundación La Caixa a las CCAA, o los que usan importantes ayuntamientos como el de Madrid o Barcelona.

CENTROS DE GESTIÓN MÓVILES.

Son aquellos centros que instalados sobre diferentes tipos de vehículos **llegan a la zona de la emergencia** y además se mueven por ella pudiendo **enlazar en movimiento.**

Permiten conocer el estado de la emergencia desde primera línea y en primera persona a los usuarios que se desplazan dentro de dicha plataforma. Pueden también operar parados pero normalmente realizan por tanto **cambios de asentamiento continuos.** Son por lo tanto tan **vulnerables** como lo puedan ser los desplegables, pero mucho menos que los fijos.

Están diseñados para prestar su servicio sólo **en momentos puntuales** de la conducción de la emergencia. Pueden alcanzar el **24 horas al día,** pero como la comodidad es mínima y los **servicios TIC proporcionados son mínimos** su personal se ve muy afectado por una operación prolongada en el tiempo en este tipo de centros. **El mantenimiento y la supervisión son vitales.**

Tienen una **redundancia mínima o nula** en muchos casos. La Plataforma Tecnológica recibe la alimentación eléctrica de las **baterías** de los vehículos cuyos alternadores han sido modificados para dar la tensión necesaria a los equipos. También es normal que cuenten con conversores de corriente, de alterna a continua y viceversa. Algunos están dotados de Grupos Electrógenos.

Podemos encontrarnos diversidad en la plataforma vehicular sobre la que se instalan. Existen centros móviles sobre plataformas aéreas, avión o helicóptero. Plataforma acuática sobre algún tipo de embarcación. Y por descontado sobre vehículos terrestres. Estas últimas varían desde una moto equipada con un sistema radio, hasta un vehículo todo terreno dotado de los más modernos sistemas de transmisión por satélite en movimiento (SOTM).

Los ejemplos más básicos podían ser la motocicleta de un Guardia Civil de la Agrupación de Tráfico o vehículo de apoyo de alguna organización sanitaria.

ÁREAS DE UN CENTRO DE GESTIÓN DE EMERGENCIAS

Una vez vistos los distintitos tipos de Centro de Gestión de Emergencias según su movilidad,

CARACTERISTICAS PRINCIPALES

- Mínimas capacidades TIC
- Muy escasa redundancia
- Uso limitado en el tiempo
- Permite conocer el estado de la emergencia en primera persona
- Mantenimiento y supervisión exigente para mantener operatividad
- Alimentación eléctrica de las baterías o alternadores de las plataformas vehiculares sobre las que se instalan

CENTROS DE GESTIÓN DE EMERGENCIAS MÓVILES

vamos a establecer las zonas que lo componen o pueden llegar a formar parte de él. Es precisamente el vehículo sobre el que se instale la plataforma tecnológica el que marcará las mayores diferencias.

ÁREA DE OPERACIONES

En esta zona es en la que se realiza la mayor parte del trabajo que se hace en estos Centros. Es lo que hemos llamado ya con anterioridad el sumidero de información porque es donde se reciben y desde donde se emiten las órdenes que permiten la gestión de la emergencia.

Aunque existen Centros en los que esta zona de operaciones realiza todas las funciones que a continuación se detallan, hemos decidido separarlas por sub-áreas pues en ocasiones se separan en algunas organizaciones.

- SUB-ÁREA DE GESTIÓN DE LLAMADAS

  Apartado del Centro en el que los teleoperadores de emergencias reciben, atienden y gestionan las llamadas telefónicas o avisos. Su misión es activar a los servicios precisos que tienen que resolver la emergencia en base a la información obtenida de cada llamada. Sólo existen en los Centros de Gestión Fijos.

- SUB-ÁREA DE GESTIÓN DE ALERTAS

  Es similar a la zona anterior, pero dedicada en exclusiva a atender las alertas y avisos originados normalmente por sistemas de alerta o vigilancia automáticos. En ocasiones reciben el sobrenombre de "**Centro de Seguimiento**" o "**Centro de Situación**". Precisan mucho menos personal para su gestión que el de recepción de llamadas ya que los sistemas suelen estar informatizados. Sólo existen en los Centros de Gestión Fijos. Algunos Centros Desplegables pueden llevar terminales remotos para hacer seguimiento de ciertos sistemas de alerta, pero no se realizan las funciones propias de un centro anclado al terreno.

- SUB-ÁREA DE DISPACHING

  Es la zona determinada dentro de un **Centro para la movilización y gestión de recursos.** En muchos Centros 112, es el propio personal de los organismos de intervención directa en la emergencia los que proceden a la activación de los recursos adecuados para la resolución de la emergencia desde la propia sala. Sólo existen en los Centros de Gestión Fijos. Algunos Centros Desplegables pueden llevar terminales remotos para hacer seguimiento, pero no se realizan las funciones de despacho propias de un centro anclado al terreno.

- SUB-ÁREA DE GESTIÓN DE LAS EMERGENCIAS

  Es el lugar dentro del Centro en el que se llevan a cabo las acciones necesarias para resolver o mitigar, desde que se producen hasta que se acaban, las consecuencias producidas tras el acontecimiento que ha provocado la situación de emergencia o urgencia (médica).

Como veremos más adelante existen dos versiones diferentes al referirse a las acciones que se llevan a cabo en estos Centros. Unos dicen que es el lugar donde se realiza el **Mando y Control** de la emergencia. A estos Centros se les suele denominar "Puestos de Mando" o "Centros

de Conducción de Operaciones". Si por el contrario en lugar de Mando y Control, otros prefieren hablar de la realización de la **Dirección o Coordinación** de la emergencia, en este caso se les denomina "Centros de Dirección o Coordinación".

En los Centros Fijos existe por descontado. A veces está asociado con el propio operador de Dispaching que además de movilizar organizaciones y recursos hace seguimiento de la emergencia hasta su finalización.

Otros centros prefieren ceder la gestión a operadores diferentes si la gestión es extraordinaria. En este caso se suelen nombrar personas expertas. Suelen contar con **salas de reunión** anexas o incluso con salas específicas dotadas de los más diversos sistemas TIC.

Estas áreas de Gestión existen tanto en los Centros Desplegables como en los Móviles, aunque proporcionadas a sus dimensiones. Incluso las salas de reunión se suelen sustituir en estos últimos tipos de Centro por tiendas de campaña que se instalan en los aledaños de los vehículos.

ÁREA TIC

Es la zona del Centro que alberga el núcleo duro (core) de los sistemas de telecomunicaciones e información. No se corresponde exactamente con la Plataforma Tecnológica ya que ésta es mucho más amplia y se extiende hasta cada puesto de operador.

En los Centros Fijos es muy voluminosa y suele denominarse "Sala de Servidores" o "Centro de Proceso de Datos (CPD).

En los Centros Desplegables corresponde normalmente con un rack que alberga los equipos, aunque existen organizaciones, sobre todo las militares, que emplean vehículos específicos. En este caso despliegan en las proximidades del Centro de Gestión y se denominan "**Centro de Transmisiones**".

En los Centros Móviles suele estar integrada en el chasis del vehículo y se corresponde con el cableado y terminales de telecomunicaciones y de información distribuidos por los puestos de operación.

ÁREA DE VIDA

Zona en la que reposa y vive el personal que no está de servicio. En los Centros Fijos suele corresponder con **salas de descanso, dormitorios y cafeterías.** En los Centros Desplegables se suelen montar cuando el periodo de tiempo es importante apoyándose en alguna instalación cedida por alguna administración local. Hablamos de polideportivos, casas de la cultura, etc. Pueden tener zonas de descanso, dormitorios montados con literas de campaña y si no hay bares en las inmediaciones se suelen montar pequeñas cantinas itinerantes. En los Centros Móviles no existe, limitándose a lo que "quepa" en la plataforma vehicular.

ÁREA LOGÍSTICA

Es el lugar donde se disponen los servicios de mantenimiento y abastecimiento necesario para cubrir las necesidades del personal y medios. En los Centros Fijos corresponde con las Salas de Mantenimiento y/o Repuestos. En los Centros Desplegables suele haber una o varias personas encargadas de estas tareas (dependiendo de la entidad del Centro). Los más comunes son los mecánicos de automóviles y grupos electrógenos, y los técnicos TIC que pueden hacer pequeñas reparaciones in situ con la herramienta que portan, que suele estar contenida en una caja. Existen talleres móviles itinerantes. Estas Áreas Logísticas no existen en los Centros Móviles, estando limitadas a las operaciones de mantenimiento preventivo que puedan hacer los propios conductores u operadores de los sistemas.

ÁREA DE OFICINAS

Son aquellas zonas dedicadas a la gestión administrativa que permite a la organización las funciones básicas para mantener su existencia. Confluyen aquí desde el personal de recursos humanos, sección económica financiera o marketing. Sólo existen en los Centros de Gestión Fijos.

ÁREA DE APARCAMIENTOS

Zona destinada al estacionamiento de los vehículos de los trabajadores del Centro y de los visitantes. Existe en los Centros Fijos y debe existir en los Centros Desplegables para evitar problemas de seguridad sobrevenidos si no existe una disciplina de lugar y modo donde aparcar los vehículos.

CAPÍTULO 10

EL RESPONSABLE TIC

Llevamos varios capítulos de este libro hablando de los **Responsables TIC,** y sin embargo todavía no nos hemos detenido a analizar quiénes son estos personajes y que intrincadas circunstancias de la vida han ocurrido para que alguien acabe desempeñando este papel en una organización de emergencias.

Nos estamos refiriendo a los profesionales de perfil tecnológico con mayor salida en el mercado laboral actual. Personas que desarrollan labores complejas, incluso extrañas, y casi siempre desconocidas por la inmensa mayoría de la organización. Configuración de routers, instalación de firewalls, auditorías de seguridad, cálculo de frecuencias, reseteo de fleximux...

Son administradores de *networking,* ingenieros de sistemas, planificadores de innovación tecnológica, analistas de servicios telemáticos, consultores de sistemas, arquitectos de redes o especialistas en criptografía. Hacen un **trabajo ingrato** que desempeñan porque tienen en su mente la idea de que las cosas pueden funcionar mejor y que su trabajo es necesario aunque poco comprendido. Son **diferentes tipos de expertos** que se encargan de mantener vivos los sistemas utilizados para garantizar el enlace y así facilitar la dirección, el mando y el control de las emergencias.

EL RESPONSABLE TIC EN UNA ORGANIZACIÓN

Reciben diferentes nombres. Directores TIC, Coordinadores CIS, Jefe de Departamento de Nuevas Tecnologías, Jefe de Transmisiones, Jefe de Informática, o **Responsable TIC,** tal y como le hemos estado denominando a lo largo del libro. Debe quedar constancia de que nos quedamos con ganas de llamarle "**Responsable del Enlace**". Sin embargo daremos nuestro brazo a torcer y aceptaremos la de Responsable TIC al ser la más conocida y extendida.

La operatividad de las agencias dedicadas al socorro y la asistencia en emergencias dependen en gran medida del éxito en la aplicación de nuevas tecnologías. Disponer de unos profesionales bien cualificados en el campo de las TIC se está convirtiendo en una premisa ineludible para garantizar el correcto funcionamiento de una organización. Los Responsables TIC han evolucionado en las grandes organizaciones de **meros técnicos** a ser una de las figuras clave en los diferentes organismos, incluidos los relacionados con las emergencias. De este modo, se demandan técnicos que a sus virtudes profesionales ahora se les exige un conocimiento exhaustivo del funcionamiento de sus agencias. La figura del Responsable TIC tiene ahora un **perfil directivo** de mayor relevancia dentro de las organizaciones.

En España, aunque de forma lenta, los responsables del enlace van adquiriendo mayor peso en los procedimientos, en las tomas de decisión, o incluso en el reparto de fondos, si bien aún queda un largo camino por recorrer.

El camino desde técnico hasta el perfil de directivo se ha desarrollado en dos períodos. En una **primera fase,** el Responsable TIC de las organizaciones se encargó de las **compras de los sistemas y de su puesta en funcionamiento.** En esta época muchos de ellos no eran ni expertos. Alguien de la organización decidía la compra de, por ejemplo radios, y este señor iba al mercado, adquiría el equipo y explicaba al resto de miembros como se usaba. En la **segunda fase** el Responsable TIC se acerca en la actualidad, o al menos debería acercarse, a la colaboración mediante las TIC a los procesos de optimización de las técnicas utilizadas en su organización.

El Responsable TIC en una organización de emergencias tiene que **combinar de forma equilibrada cualidades personales con conocimientos técnicos.** Entre las primeras destacaremos la capacidad de trabajo en grupo, la paciencia, la comprensión y la visión práctica de la situación. Con respecto a los conocimientos tecnológicos éste debe saber las diversas tecnologías y sistemas existentes, sus tendencias y las posibilidades que aportan al modo de trabajo establecido en su organización.

Son cada vez mayor el número de habilidades que se le exigen al profesional TIC. Esto está obligando bien a "multiplicarse" asumiendo nuevas tareas, bien a buscar la especialización añadiendo más expertos TIC a la plantilla de la organización cuando hay respaldo económico suficiente.

El responsable TIC no debe ser una isla en el estadillo de la organización. **Debe estar plenamente integrado con sus compañeros usuarios** para que se llegue a buen puerto.

SELECCIÓN DEL RESPONSABLE TIC DE LA ORGANIZACIÓN

Depende de la entidad de la organización, pero lo ideal es que el Responsable TIC sea un **profesional con dedicación exclusiva.** El perfil que hemos definido en el apartado anterior reclama un compromiso y una dedicación que exige que la persona designada se especialice en este complejo y cambiante mundo.

Uno de los primeros pasos a dar en nuestro proceso de selección será el de decidir si queremos un TIC con **perfil técnico, con perfil directivo o con los dos.** Lo ideal sería que combinara las dos opciones, pero esto sólo suele funcionar en pequeñas organizaciones.

Los aficionados o amantes de las nuevas tecnologías pueden hacer un buen papel si su hobby acaba por profesionalizarse, sobre todo en pequeñas organizaciones con sistemas reducidos. Cuando subimos de nivel y planteamos sistemas permanentemente trabajando (régimen H24), la competencia y la alta cualificación es imprescindible.

Cuando la organización busque en el mercado de trabajo debe orientar su proceso de selección a encontrar un profesional con el conocimiento previo de los sistemas ya implantados en nuestra organización. La experiencia profesional anterior será muy importante sobre todo si a la tecnológica se le añade el haber trabajado en el mundo de las emergencias. El conocimiento de la organización podrá adquirirse con el tiempo. Para finalizar **no se deben olvidar las singularidades personales del individuo,** hombre o mujer,

que seleccionemos. De nada nos vale el mejor TIC, si es incapaz de enseñar a los usuarios cómo funcionan los sistemas por falta de dotes docentes, o si entra en ira cada vez que un operador tiene un problema.

La formación y experiencia del Responsable TIC será muy importante. **¿Queremos un licenciado, un Técnico Superior, o un operador de sistemas?** El lector no debe confundir licenciado con nivel directivo y técnico con operador. Todas las combinaciones son posibles y no existe una regla concreta. Existen ingenieros en informática que son operadores, al igual que existen directivos sin formación universitaria. Lo que sí está claro es que cada cual tiene su background y sus capacidades son muy diferentes.

En muchas ocasiones aparece el síndrome de la **"navaja suiza"**, y tenemos el "**chico o la chica TIC para todo**". El papel que la propia organización haya decidido darle al Responsable TIC tiene que marcar el currículo a elegir. Quizás un ingeniero superior pueda llegar a administrar una red de área local, pero tal vez el administrador de bases de datos no esté capacitado para diseñar un sistema de información al completo.

Una pregunta frecuente en la contratación de un TIC es ¿"**Teleco" o informático**? Pues una vez más dependerá del contexto donde vaya a ejercitar su trabajo y por supuesto de las tareas que tenga que desarrollar. El intrusismo, o siendo más diplomático, el transvase de expertos entre disciplinas, está muy de moda, y es normal encontrar a matemáticos ejerciendo de magníficos ingenieros informáticos, operadores de radio cambiando direcciones IP, o "telecos" diseñando páginas web.

TIPOS DE RESPONSABLES TIC

Visto quiénes son, a qué se dedican y con qué criterio debemos seleccionarlos, llega el momento de ponerlos delante de un espejo. Siempre es bueno conocerse a uno mismo, o al menos hacer acto de contrición, aceptar las virtudes y asumir los defectos de cada cual.

La experiencia nos da esta clasificación de responsables TIC teniendo en cuenta las cualidades personales y técnicas:

- **El siniestro.** Muchos de los responsables TIC suelen ser gente tímida que prefiere una "relación" con su ordenador a una conversación con una persona de carne y hueso. Prefieren la soledad de su oficina a la vorágine de un CECOPI o de un Puesto de Mando. Son personas capacitadas técnicamente, pero su aislamiento les ocasiona, al no tener un contacto directo con sus usuarios, desconocer sus problemas y falta de confianza para congeniar con ellos. No se integran en la organización y tampoco tienen fácil mejorar sus procesos con las TIC.
- **El listo.** Elevados conocimientos técnicos. Lo sabe "todo" de su trabajo. Desprecia al usuario porque no puede entender que algo tan fácil como son las nuevas tecnologías resulten un problema para nadie. No suele tener buena relación con los usuarios porque les trata de demostrar continuamente que son unos ignorantes tecnológicos. Aunque suelen estar integrados en la organización acaban generando animadversión en los usuarios y las TIC pierden protagonismo a pasos agigantados en la organización.
- **El descolocado.** Por suerte este estereotipo es cada vez menos frecuente. No sabe nada de este

LAS MUJERES Y LAS TIC

Según un estudio realizado por la institución Feria, el porcentaje de mujeres que trabaja en el sector TIC alcanza el 34,5%.

La distribución de hombres y mujeres en las áreas funcionales de las empresas no es homogénea, ya que mientras que en el área de atención al cliente de las compañías trabajan prácticamente la misma cantidad de hombres que de mujeres, son muchos más los hombres, el 82%, los que desempeñan su labor en el área de la informática.

Las mujeres en el área de sistemas de información sólo alcanza el 20,4% del total.

Estos mismos datos indican que las mujeres directivas destacan por su mayor presencia en áreas funcionales como calidad, atención al cliente, auditoría y organización, mientras que son menos numerosas en las áreas de informática, servicios generales y producción.

negocio pero le ha correspondido en suerte hacerse cargo de las TIC de su organización. Si es responsable aprenderá con el tiempo o se rodeará de gente que le haga el trabajo. Si no lo es, se presentará un grave problema. Si al menos proviene de otro departamento de la organización puede aportar esta visión.

- **El cumplidor.** Es un compendio de capacidades medias, de conocimientos propios de su oficio, y de facilidad de relación con el usuario que le permiten desarrollar sus misiones con eficacia totalmente integrado en la organización.

ESTRUCTURA ORGÁNICA TIC DE LA AGENCIA

Ante la personalidad y los conocimientos TIC del Responsable de esta materia en nuestra organización, una vez ya contratado, podemos hacer poco más que mejorarle la formación. Sin embargo sí que podemos aplicar otras medidas como puede ser la de adoptar una **organización TIC** que favorezca dentro de la agencia nuestro trabajo.

De nuevo la entidad de la organización será la que marque la posibilidad de poder organizar y distribuir las tareas relacionadas con el enlace. Partamos de la base de que un Responsable TIC, y por ende su organización que le soporta **no tiene horarios.** Si la organización de emergencias tiene sistemas corporativos TIC H24, esto implica que nosotros también. Y si no los tiene... también da igual, porque si algún sistema se viene abajo dentro o fuera de las horas de trabajo habituales, deberemos echar el resto para volverlo a poner operativo ya las emergencias pueden ocurrir en cualquier momento.

Si se trata de **una única persona,** esta mujer o este hombre se organizarán para mantener sus sistemas operativos y a pleno rendimiento. Si por el contrario la organización tiene la suficiente entidad habrá por algún tipo de estructura orgánica TIC. Veamos algunos ejemplos.

Antiguamente en las organizaciones **se diferenciaba entre las telecomunicaciones y la informática,** de hecho todavía hay organizaciones que mantienen responsables separados. Esta separación hoy día no es recomendable puesto que ya hemos visto como ambos temas casi se han solapado.

Existe también la tendencia a separar entre **TIC fijas,** entendidas como la que dan servicio a un Centro de Gestión de Emergencias anclado a una infraestructura fija; y las **TIC desplegables**, entendidas estas como las que los intervinientes desplazan hasta el lugar de la emergencia. Este reparto del trabajo sólo tiene sentido cuando los medios TIC desplegables representan un gran volumen. Aquellas opciones que apuestan por esta organización acaban destinando al personal que atiende al material desplegable al centro fijo, ya que estos últimos mantienen una actividad constante, mientras que los TIC desplegables, son utilizados tan esporádicamente como la misma ocurrencia de la emergencia.

La tendencia actual es hacer una división de tareas y **una estructura TIC asociada a la operación y mantenimiento de sistemas completos.**

Un ejemplo podría ser el siguiente. Un Jefe o Responsable TIC, que conoce sus tareas, está integrado perfectamente en los procedimientos de su organización, que además conoce su personal y los sistemas TIC, decide hacer la siguiente organización por sistemas:

- **Redes Radio**: que incluiría la operación de tantas redes radioeléctricas como use nuestra organización.
- **Redes Satélite:** lo que significa operar o mantener operativo los terminales de los diferentes sistemas gubernamentales o de operadores públicos.
- **Redes Telefónicas**: se encargan aparte de los terminales telefónicos, de toda la parte de tendidos de cableado de cobre, coaxial o fibra óptica. Como es el personal con más experiencia en este campo incluso suelen ser ellos los que hacen los tendidos de las redes informáticas.
- **Sistemas de Mensajería**: son los encargados de mantener el registro de la entrada y salida de la documentación oficial y de la correspondiente transmisión por los sistemas que tenga a su alcance (fax, correo electrónico, mensajeros, Morse, etc.).
- **Sistemas de Información**: aquí podremos hacer tantas subdivisiones como sistemas tengamos. Dependerá mucho de la carga asociada a cada uno de ellos: *Back-up*, GIS, servidores de correo, portales web, bases de datos, dispaching, etc.
- **Multimedia y Videoconferencia (VTC):** dada la importancia que está adquiriendo este tipo de medio y la complejidad del tratamiento de imágenes obliga a plantearnos el tener personal muy especializado.
- **Energía & SAI:** aunque no sea algo específico TIC se precisa tener experta en este campo para garantizar el suministro en todo momento.
- **Sistemas de Grabación**
- **Sistemas de Seguridad**
- **Otros**

Puede ser esta subdivisión o cualquier otra. Incluso podríamos agrupar redes radio con satélite o sistemas de mensajería con los de información. Lo importante es la estructura TIC que permita sacar el **máximo rendimiento de nuestros medios y de nuestro personal**. Sin embargo queremos poner el acento en tres elementos que son fundamentales en una organización TIC para garantizar buenos resultados y que desde nuestro punto de vista deben estar siempre presentes. Son los siguientes:

HELP DESK

La HELPDESK, o Unidad de Atención al Usuario, es un conjunto de servicios que ofrecen la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral relacionados con las TIC.

Es un **elemento indispensable** para resolver en tiempo y lugar, la problemática que dentro de los Sistemas de Información y Telecomunicaciones, se presenta a los usuarios en el día a día, y que favorece el correcto funcionamiento del resto de la organización.

Es fundamental. No importa lo bueno que sea nuestro sistema. No importa el trabajo y las horas que le dediquemos. **Si el usuario no está contento con el sistema y si cuando tiene un problema no se lo resolvemos, todo nuestro esfuerzo habrá sido para nada.**

La Help Desk es el puente de unión de nuestro trabajo y la retroalimentación o feedback que nos dan los usuarios a los que servimos. La Help Desk se debe basar en un procedimiento que tiene que ser muy sencillo. Lo habitual es **basarse en un número de teléfono** al que puedan llamar los usuarios cuando tienen una necesidad o se encuentran con un problema relacionado con las TIC. El procedimiento de la Help Desk nunca debe provocar al usuario una problemática mayor que la que tenía inicialmente. **Debe ser atendido por gente con conocimientos técnicos, pero también por gente comprensiva y amable.** En el siguiente tema dedicado al usuario TIC entraremos en más detalles de cómo dar un buen servicio.

HELP DESK

TIC POC[77]

El TICPOC, o **Punto de Contacto TIC**, es un usuario dentro de cada división administrativa de nuestra organización de emergencias, que **será nuestro interlocutor para asuntos relativos a los Sistemas de Información y Telecomunicaciones** que afecten a sus unidades o dependencias. Aunque sería recomendable que el personal designado al efecto tuviera algún conocimiento previo sobre asuntos TIC, no es preciso que sea un especialista. Un requisito fundamental para su nombramiento debe de ser la permanencia en el puesto. Se debe asegurar en todo momento esta continuidad nombrando los

ATENCIÓN AL USUARIO TIC

Existen organizaciones en las que se han instaurado aplicaciones para el control de incidencias de los usuarios con las TIC.

En ocasiones son tan complejas que el usuario acaba desistiendo de resolver su problema ante la necesidad de rellenar múltiples y diferentes formularios, muchas veces incomprensibles para ellos.

Se han dado casos en las que a un usuario recién llegado a su organización se le exige que entre en la red de área local, que requiere un ordenador que no tiene, un usuario de red que tampoco tiene, y una password que por supuesto desconoce, para que pueda solicitar un ordenador y un teléfono con el que trabajar.

77. POC: *Point of Contact*, es decir Punto de Contacto.

titulares y suplentes necesarios, remitiendo dicha información a nuestra organización TIC. Él o ella recogerán las preocupaciones o las necesidades y nos las harán llegar de una manera organizada y controlada. El jefe de cada dependencia marcará criterios al TIC POC y dirimirá divergencias cuando los usuarios manifiesten peticiones incompatibles o incluso contrarias. Así nos evitaremos que los usuarios soliciten cosas dispares que nos quiten tiempo y que nos carguen excesivamente de trabajo.

CENTRO DE CONTROL DE LAS TIC

El Responsable TIC establecerá un **Centro de Control y Coordinación de los Sistemas de Telecomunicaciones e Información,** como **órgano responsable del control técnico del conjunto de los sistemas.** Desde dicho Centro se velará por el estado de las TIC.

En ocasiones este Centro, será una única persona, el propio Responsable TIC, quien tendrá en su cabeza lo que funciona, lo que ha dejado de hacerlo y priorizará las tareas a acometer. El problema se presenta cuando son múltiples los sistemas y múltiples las personas responsables de su control, resultando muy complicado tener en un momento dado la visión global del estado de los enlaces.

La existencia del Centro de Control TIC es la solución. Varía desde una sala repleta de complejos sistemas de supervisión de cada sistema, hasta una simple pizarra en la que cada responsable refleje la situación de su área de responsabilidad. El fin es tener conciencia del estado de los enlaces, para poder determinar las tareas de mantenimiento o administración necesarias.

FUNCIONES DEL RESPONSABLE TIC

Nuestro rol como equipo de coordinación TIC estará definido por las funciones y responsabilidades que debemos asumir según el uso y la integración de las TIC en las actividades diarias de la organización. Más si cabe en las intervenciones durante las emergencias declaradas.

Todo el mundo debe estar cualificado para operar sus herramientas TIC. Pero si hay alguien que debe controlar en detalle los sistemas y tener prevista las vías alternativas, ése es el responsable TIC de cada organismo. Este hombre o mujer deberá hacer todo el esfuerzo posible prestando asesoramiento y maniobrando con los recursos de telecomunicaciones para conseguir el enlace.

Indudablemente que nos podemos encontrar recién llegados a una organización que acabe de incorporar esta figura, por lo que se podrán encontrar algunas dificultades para definir estrictamente su papel, por eso debemos entender que el coordinador TIC deberá mostrar cierta flexibilidad e iniciativa personal atendiendo a las necesidades que la agencia requiera.

Las funciones del responsable de las Tecnologías de la Información y las Comunicaciones, son todas aquellas que el lector haya podido extraer de la lectura de este libro. No obstante, haremos una relación de las más importantes.

- Por descontado que su principal misión será la **supervisión y funcionamiento de todos los sistemas.** Serán tareas relacionadas con aspectos técnicos, instalación y configuración de los equipos y programas informáticos, mantenimiento y seguimiento periódico del correcto funcionamiento de los recursos, control de equipos y software, control de estándares de seguridad informática, etc.
- El Responsable TIC junto a su equipo, si lo hubiere, debe **integrarse** totalmente y en toda circunstancia en el funcionamiento de **la organización**.
- Una de las tareas clave en las primeras etapas de trabajo será **definir y divulgar nuestras funciones** específicas, allí donde no estén claras.
- También debe **coordinar y dinamizar la integración de las TIC en los procedimientos** de trabajo definidos por los responsables de área o departamentos de su agencia.
- Otra tarea será la de **prestar asesoramiento** a los directores de la organización en todo lo relativo a las TIC. No podemos dejar de ser un factor de innovación y añadir valor en los procesos de nuestra agencia.
- Se debe realizar de manera continua el **análisis de necesidades TIC de la organización** en su ámbito competencial.
- Es muy recomendable colaborar e **intercambiar información con otras estructuras TIC** de organizaciones similares a la nuestra para buscar el trasvase de experiencias que conlleven una mejora del rendimiento y eficacia de nuestros sistemas.
- Como señalaremos en el próximo capítulo se debe **atender debidamente a los usuarios** y acercar el uso de las TIC a todos ellos.
- Se debe asumir el **liderazgo de la formación de las TIC** en nuestra organización. Un eje central en todo proceso innovador en las organizaciones es la formación de sus miembros. Velar por ello no implica

únicamente la adquisición de competencias instrumentales básicas para el uso de equipos y programas; sino y sobre todo es necesario dar a conocer las posibilidades que ofrecen dichos medios. El liderazgo en la formación la aplicaremos en los tres ámbitos siguientes, adecuando a cada cual los temas a asimilar.

- Autoridades. Los jefes tienen que tener una idea general de los sistemas puestos a su disposición. Se les deben enseñar "**capacidades" y no "detalles".** Es decir un directivo no necesita saber cómo se sintoniza una frecuencia en un *walkie*, o cómo se hace una videoconferencia a través de una MCU. Ellos tienen que saber que tenemos sistemas radios y que hay capacidad para hacer videoconferencia. Si luego las circunstancias aconsejan que aprendan a usar algún sistema, se aplicará la norma indicada en el siguiente punto.
- Usuarios comunes. Es importante que los usuarios conozcan también las capacidades globales de las TIC de nuestra organización, pero es mucho más que cada cual sepa y controle el sistema TIC que la organización haya decidido poner en sus manos. **Se necesita una formación inicial y luego una formación periódica para mantener las capacidades,** sobre todo en aquellos sistemas que no se utilizan asiduamente, y sólo se utilizan durante la intervención en la emergencia. Se debe elaborar un itinerario formativo para que el usuario dé respuesta a las necesidades de cada puesto atendiendo a distintas modalidades formativas, cursos, seminarios, grupos de trabajo, etc. **Los ejercicios y simulacros** son la base para consolidar la formación.
- Técnicos TIC. Resulta básico mantener a nuestro personal TIC, o a nosotros mismos, actualizados. Hay que ser muy selectivo con el personal que se envía a recibir algún tipo de formación. Primero por lo costoso que resulta, y segundo porque el tiempo que pasan formándose no lo dedican a sus sistemas. Es sin duda una vulnerabilidad a no ser que haya personal adicional que cubra su baja. Además se debe velar porque el que haga algún tipo de curso lo devengue en la organización para rentabilizar la inversión.

  Igual de selectivo hay que ser a la hora de elegir el tipo de curso. El curso debe estar hecho a medida para cubrir nuestra necesidad.

- Una de nuestras preocupaciones será la **logística de personal y de materiales.**
  - Material: Para realizar nuestro trabajo debemos tener un entorno adecuado. Los **locales** dedicados a los sistemas TIC deben reunir los requisitos de seguridad adecuados y contar con unos **puestos de trabajo** acordes a las tareas a desempeñar. Resulta imprescindible contar con una estructura de **sostenimiento** (mantenimiento y abastecimiento) que se encargue de reponer o arreglar los equipos averiados.

    Los equipos de reserva, el control de su ubicación y la redundancia de materiales son un sueño para cualquier Responsable TIC. Por desgracia no suele ser tan idílico para los responsables financieros por los precios astronómicos de los sistemas con estas características, así que nos tendremos que conformar con tener algunos **repuestos** y tener **proveedores** que sean capaces de reponernos lo averiado.

Otra parte de nuestro trabajo será el **catalogar y organizar los propios recursos TIC** y elaborar bases de datos para la consulta, administración y uso del material catalogado. Otro aspecto importante será la toma de decisiones referidas a la compra y distribución de equipos.

- Personal: Ya hemos comentado lo vital del **proceso de selección** de nuestro personal TIC, pero lo es mucho más la organización y la definición de tareas de cada uno de los componentes. Si tenemos suficiente personal TIC a nuestro cargo podremos trabajar a turnos. Los **turnos** suelen dar un resultado aceptable, pero son caros de mantener y existe un constante riesgo de exceso de burocratización de los integrantes del mismo, que en muchas ocasiones acaban por desligarse emocionalmente de los objetivos y del espíritu de equipo de nuestra organización TIC. Se limitan a cumplir sus tareas en el mejor de los casos sin implicaciones adicionales.

- Debemos ser parte activa en la realización de **ejercicios y simulacros** en los que participen todos los estamentos de nuestra organización, autoridades, usuarios de medios TIC y nuestros propios técnicos. Ampliaremos este aspecto al final de este capítulo.

  También debemos ser proactivos a la hora de crear **procedimientos** dentro de la organización donde se tengan en cuenta nuestros sistemas TIC, y tampoco debemos olvidarnos de escribir procedimientos propios de cada sistema que nos facilite su administración.

- **La reserva TIC.** Un buen gestor de las TIC debe tener siempre un **as en la manga,** es decir sus reservas. Estas reservas pueden ser de diferentes tipos. Desde un par de radios para reponer otras averiadas, hasta un circuito reservado para derivar el tráfico cuando los principales están saturados. La reserva solo se debe empeñar cuando realmente sea necesaria, lo que se aprenderá con la experiencia y con la rápida evaluación de la situación en cada momento.

- Seguridad. Aunque en este libro no hemos querido hablar de la seguridad del enlace en emergencias por su excesiva complejidad para el aprendizaje en comparación con los réditos obtenidos, al menos vamos a dar unas pinceladas. Debemos velar a toda costa por la **seguridad** física de nuestros compañeros y también por la de los equipos. Los equipos de energía y los trabajos en altura son los que suelen aportar más peligro a nuestro entorno de trabajo. Debemos también aplicar medidas que intenten dar **seguridad a la información** propiamente dicha, es decir implementaremos **medidas INFOSEC[78].** Crearemos usuarios, roles y permisos en nuestros sistemas informáticos. Introduciremos procesos de autenticación y de auditoría, y habrá veces en las que incluso tendremos que cifrar las comunicaciones para protegerlas de escuchas indiscretas.

- En resumen lo más útil es elaborar un **Plan Director TIC de la organización**, en el que señalen los objetivos a alcanzar a corto, medio y largo plazo en su área de responsabilidad, así como velar por su cumplimiento. En este plan deben figurar todos los aspectos que acabamos de señalar y debe estar aprobado y sancionado por los directores o jefes de nuestra organización. Este documento será nuestra "**biblia laboral**".

- Y por supuesto un buen responsable TIC tiene que tener siempre una premisa. Si hay posibilidad de que algún sistema falle, éste lo hará en el peor

78. Se define INFOSEC, o seguridad de la información, como el conjunto de medidas técnicas que garantizan la seguridad de la información manejada por las TIC. Se compone de seguridad de los sistemas de telecomunicaciones (COMSEC), seguridad de los ordenadores o de los sistemas de información (COMPUSEC) y la seguridad de las emisiones no deseadas (EMSEC).

de los momentos. **Somos compañeros de viaje de "Murphy" y su ley nos acechará constantemente.** Nuestra solución será siempre la redundancia de equipos, la vías alternativas de enlace y una pequeña reserva de medios. Cualquier cosa para permitir cumplir la misión a nuestros compañeros.

LAS PRUEBAS TIC

Una **prueba** es una sesión de trabajo en la cual los técnicos TIC ponen en práctica acciones para mejorar el funcionamiento de los medios o servicios. Los ensayos o pruebas normalmente **sólo se hacen durante la preparación o la instrucción,** y rara vez los llevaremos a cabo durante una emergencia real.

Son una herramienta que empleamos los Responsables TIC para mejorar nuestras prestaciones y poder ofrecer un servicio de garantía a nuestros compañeros. Pueden ser muy simples o muy complejos. Desde probar el alcance de dos equipos radios hasta el funcionamiento de un sistema complejo desplegado sobre el terreno. **Lo importante es conocer de antemano, y previamente la emergencia, el comportamiento del sistema.**

Cualquier ensayo contribuye a **mejorar la coordinación interna** de los responsables TIC y por supuesto **la coordinación externa con el resto de la organización** y por tanto dentro del plan global que haya preparado nuestra agencia para afrontar una emergencia. Los ensayos, test o pruebas en nuestros sistemas nos servirán para imprimir una imagen mental de la secuencia de acciones claves que se producirán dentro de la emergencia. Las necesidades de enlace en cada fase, los medios a utilizar y las reservas que deberemos prever en nuestro planeamiento.

Hay que probarlo todo. Hasta la operación más simple debe estar testada. Nuestro campo de actuación está condicionado por agentes, a veces incontrolables, que se escapan de nuestra influencia y por tanto es necesario invertir unos minutos en realizar una prueba y constatar que el enlace se comporta tal y como esperábamos.

Ante la pregunta del usuario "¿esto funciona?"...la respuesta del TIC debe ser siempre "... hay que probarlo".

En el caso de simulacros en el que llevaremos al terreno de la realidad los planes teóricos, es primordial tener la seguridad de que la **columna vertebral de todo plan,** que es su sistema de telecomunicaciones y de información va a garantizar el cumplimiento de la misión. Esto implicará una carga de trabajo muy importante para nosotros y nuestro personal, pero incidirá directamente en el resultado. **Con la debida antelación,** para así tener tiempo de corrección de fallos, desplegaremos nuestros sistemas y además comprobaremos los servicios que sabemos positivamente van a ser utilizados en la emergencia.

El ensayo o **test ideal es el que se realiza con los propios usuarios** operando el sistema, algo que no siempre se podrá conseguir realizar.

SEGURIDAD DE LA INFORMACIÓN

¿QUÉ SE DEBE GARANTIZAR?

- **CONFIDENCIALIDAD**
  Se garantiza que la información es accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **INTEGRIDAD**
  Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **DISPONIBILIDAD**
  Se garantiza que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma siempre que lo requiera.

CAPÍTULO 11

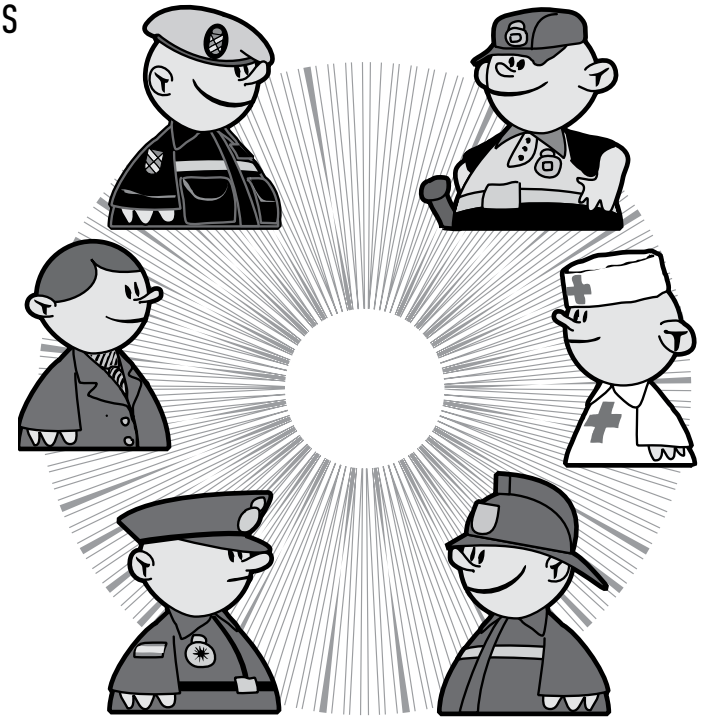
EL USUARIO TIC

Ya conocemos que los factores que influyen en el enlace son muy variados. Unos pueden ser de **origen técnico:** la potencia del transmisor, la sensibilidad del receptor, la adecuación de la antena... Otros los determinará el entorno: las condiciones atmosféricas, la presencia de obstáculos en el campo de transmisión, sean de tipo natural (orografía y vegetación) o artificial (presencia de líneas eléctricas, edificaciones o estructuras). Y por último los **inherentes a la naturaleza humana:** la capacitación del operador, la correcta configuración del equipo, la elección acertada del canal. Es decir, en el enlace, tal y como vimos en el capítulo 1, hay otros condicionantes que van a entrar en la ecuación de nuestro éxito o fracaso, y puede que uno de los más importantes sea el **usuario de las TIC.**

El conocimiento profundo y detallado del funcionamiento de los nuevos sistemas de telecomunicaciones e información no es imprescindible, aunque sí que puede resultar beneficioso. No debe ser un experto. Ya para eso está el Responsable TIC. **Pero toda persona que trabaje en Protección Civil** necesita tener nociones de la infraestructura del enlace que pueden emplearse con el fin de controlar todas las posibilidades y caminos secundarios que pudiera llegar a necesitar.

El **usuario** es esa persona que se debe beneficiar de nuestro planeamiento, de nuestro correcto diseño, de todas las eficaces precauciones y medidas que hemos tomado para que él pueda cumplir brillantemente su misión a través

DIVERSIDAD Y MULTITUD DE USUARIOS



TODOS NECESITAN ENLAZAR

Las telecomunicaciones son una herramienta imprescindible en cualquier organización, y dentro de ésta en todos los niveles de la jerarquía independientemente que se dediquen a la dirección o a la ejecución táctica.

Desde políticos tratando de recibir información en los primeros momentos de la catástrofe, pasando por elementos de búsqueda y rescate, cuerpos policiales o voluntarios de protección civil. Todos tienen en común la necesidad de dar y recibir instrucciones de lo que está aconteciendo.

de las TIC. En definitiva es ese hombre o esa mujer que nos mirará a la cara cuando todo haya pasado y con ojos vidriosos nos dirá: gracias por un trabajo bien hecho...Y luego, nos despertaremos.

Efectivamente estábamos en un sueño. El párrafo superior es una ilusión, es algo que seguramente, si alguna vez se produjo, no quedó constancia en los libros de historia.

Es nuestro sino. Y cuanto antes lo asumamos mejor nos irá a los responsables TIC de las organizaciones. Son otros los hechos y expresiones, bastante menos agradables, que nos van a acompañar a lo largo de nuestra vida profesional.

Lo mejor que nos puede pasar tras una emergencia es que nadie hable de nosotros. **La indiferencia del usuario de las TIC es el éxito del responsable del enlace.** Si nadie se acuerda de nosotros es porque todo ha funcionado relativamente bien, pero si hablan... seguramente será para ponernos a caer de un burro.

Existen **diferentes tipos de clasificaciones de usuarios** de medios de telecomunicaciones. Podríamos quedarnos en la clasificación básica realizada por Marc Prensky[79], y distinguir entre el "**nativo digital**" y el "**inmigrante digital**", es decir, entre aquellos nacidos y educados cuando ya existía la tecnología digital, y los nacidos antes de los años 80 que han tenido que adaptarse al proceso de cambio de la tecnología.

Sin embargo, aunque veremos que influye, esta clasificación se queda corta para explicar el fascinante mundo de los usuarios de medios de transmisiones en una emergencia.

Comencemos dando unas generalidades sobre ellos.

Todos ellos, los usuarios TIC, son unos incomprendidos por

79. Libro Inmigrantes Digitales

parte del personal TIC. Sí, no estamos errando. El incomprendido es el usuario porque el responsable de transmisiones en muchos casos no es capaz de ponerse en su piel. El usuario en las emergencias es una persona con un alto grado de estrés. Precisa transmitir y recibir mucha información en cortos plazo de tiempo, en un contexto de urgencia en el que muchas veces corren riesgo vidas humanas.

Expresiones habituales, como "**no funciona nada**", o "**esta radio es una mierda**", suelen ser mal interpretadas por el personal TIC, ya que realmente tienen otro significado del que a priori pudiera presuponerse. Encima, incomprensiblemente, el personal TIC tiende a tomárselas como un ataque personal hacia su trabajo.

Realmente tales apreciaciones quieren decir que aprecian profundamente el esfuerzo realizado por nosotros, el personal TIC, para conseguir materializar su sistema de mando y control, y que es una pena, que un sistema que ha funcionado perfectamente durante el 95% del día, haya ido a fallar precisamente en el momento que a esta persona le urgía hacer uso del medio de transmisión puesto a su disposición. Es el "momento" el que les hace poner, a veces, palabras inexactas en sus labios.

Lo cierto es que **los sistemas fallan, al igual que las personas**. Mucho más si se les somete a situaciones extremas. Por tanto está dentro de la normalidad que las transmisiones tengan cortes y se produzcan caídas del enlace.

Por increíble que pueda parecer... los propios usuarios a veces fallan. **Los responsables de las TIC nos enfadamos injustamente con los usuarios que cometen errores** en el uso de los sistemas y que por circunstancias acaban recayendo en nosotros. Esa radio con el canal erróneamente seleccionado, ese ordenador que no funciona porque el usuario ha olvidado la contraseña, o esa videoconferencia que no se oye, porque el usuario inocentemente ha pulsado el "*mute*".

Existe tendencia en los últimos años a **considerar al usuario como una parte del sistema de telecomunicación,** debido al importantísimo papel de interactividad que desarrolla. El usuario puede, y de hecho lo hace a menudo, condicionar el funcionamiento de un servicio a través de sus acciones, desencadenando comportamientos diversos del sistema de telecomunicaciones e información. Por ejemplo, la conexión de un llavero de memoria flash con un virus, en un ordenador de una red de área local, puede tirar abajo el más sofisticado de los sistemas. ¡Ojo! El responsable no sería el usuario sino nosotros mismos que no hemos tomado las medidas necesarias para evitar esa posibilidad.

Vamos a **dejar de lado esta redacción irónica** y vamos a analizar realmente a nuestro querido usuario.

El usuario según el Diccionario de la Real Academia Española de la Lengua dice que es quien usa ordinariamente algo, o bien es la persona que utiliza algún tipo de objeto o que es destinataria de un servicio. Es decir, podemos encontrarnos con dos tipos de usuario, **el que realmente usa de modo continuo los medios de enlace, y otro que no lo hace de manera cotidiana**.

Sin embargo hay asuntos que incluso podrían ser motivo de estudio psicológico. Nos estamos refiriendo al **alto grado de "torpeza tecnológica"** con el que nos podemos encontrar en algunos usuarios. No importa que el usuario utilice a diario un ordenador en el trabajo, que se pase el día con la PDA en la mano y que cuando llegue a casa se dedique a responder correos y a contestar a sus amigos de las redes sociales sentado cómodamente en un sillón con su último modelo de tablet. Aunque en una intervención se le dé un medio TIC similar al que usa en su vida diaria, si no lo ha usado antes o requiera una operación algo compleja, el fracaso está prácticamente asegurado.

Es evidente que nos hemos instalado en la demagogia. Por suerte no todos los usuarios son así, pero la experiencia dice que esta situación se da en un porcentaje muy alto. Probablemente esté justificado este hecho por las **circunstancias inusuales** en las que se produce, pero sin duda es un condicionante que deberá tener siempre presente el planificador TIC, y que se debe traducir en soluciones simples y flexibles y, sobre todo, mucha formación e instrucción en simulacros y ejercicios.

Hagamos una clasificación de las usuarias y usuarios con los que tendremos que trabajar.

TIPOS DE USUARIOS

Aunque es importante evitar ideas preconcebidas y crear estereotipos de los usuarios, hemos caído en la tentación de juzgarlos por algún rasgo reseñable, con la idea de advertir a los que se inician en este curioso mundo de los usuarios de las nuevas tecnologías. Vaya por delante que somos conscientes de que en realidad estamos proyectando nuestros propios sentimientos, o quizás vamos a valorar al usuario a partir de un único rasgo individual favorable o desfavorable.

CLASIFICACIÓN CIRCUNSTANCIAL DE LOS POSIBLES USUARIOS

- "Usuario por profesión"
- "Usuario por afición"
- "Usuario por accidente"

CLASIFICACIÓN CIRCUNSTANCIAL

Hemos introducido esta primera clasificación "circunstancial" porque la experiencia refleja que el **contexto en el que el usuario llega al manejo de los medios de enlace** marca de manera determinante el tipo de usuario global al que nos enfrentaremos. Es la siguiente.

En el mundo de las emergencias, encontraremos tres tipos diferentes. Existen por tanto usuarios de medios de enlace por profesión, por afición y otros por accidente.

- El "**usuario por profesión**", es evidente que es aquel profesional del mundo de las emergencias que dentro de su trabajo tiene, entre otras herramientas, uno o varios equipos para materializar el enlace.
- El "**usuario por afición**" es aquel que usa los medios de transmisiones como hobby. Los radioaficionados son la muestra más palpable.
- Los "**usuarios por accidente**", son ciudadanos corrientes que las circunstancias inherentes a una situación de emergencia les hacen incorporarse a la cadena del enlace, para transmitir algún tipo de información. Estamos hablando desde un ciudadano que informa de una emergencia ocurrida en la calle, hasta de un cargo político que de repente se encuentra en la tesitura de dirigir un operativo.

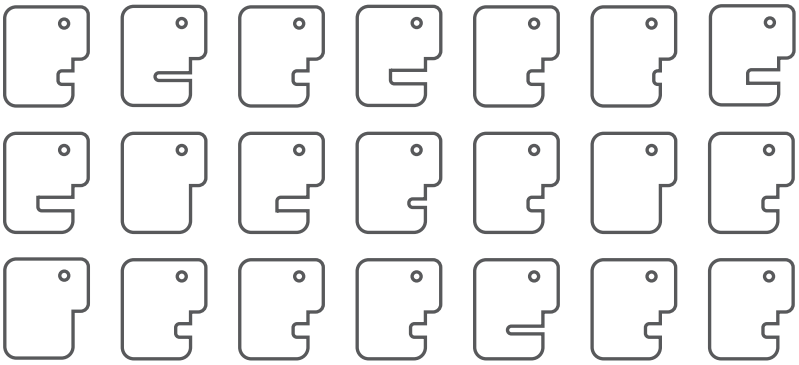
Los **secretos para ser un buen usuario de medios TIC** en una emergencia son: **estudio, práctica,** entrenamiento en busca de la **APTITUD**[80] y, fundamentalmente... **ACTITUD**[81].

Para los dos primeros tipos de usuarios señalados la aptitud se les presupone, y se les debe exigir la actitud necesaria para entender que, primero deben buscar superar permanentemente los conocimientos que se poseen, y segundo, aceptar los estándares de conducta y disciplina.

Por tanto, el problema lo encontraremos con los usuarios por accidente, los cuales rara vez tendrán la aptitud lo que puede provocarnos ciertos problemas. Pero si además no tienen la actitud, nuestro trabajo como Responsable TIC se nos complicará.

80. Aptitud: adquirir habilidad para operar medios TIC. Está relacionado con los atributos técnicos que consigue una persona con estudio y práctica.

81. Actitud: está relacionado con lo que se hace con lo que sabe. Relacionado con la concienciación de la importancia de las TIC y con la voluntad de mejorar una debilidad en un conjunto de habilidades relacionadas con el conocimiento y uso de los medios de enlace.



CLASIFICACIÓN GLOBAL DE USUARIOS TIC

- El usuario "concienciado"
- El usuario "inocuo"
- El usuario "maleducado"
  - Desconocedor de las TIC
  - Maleducado "per se"
- El usuario "comprensivo"
  - Conocedor de las TIC
- El usuario "inca"

CLASIFICACIÓN GLOBAL

Aparte de las circunstancias que llevan a una persona a convertirse en un usuario TIC, existen otras muchas que pueden condicionar su comportamiento. Es por ello por lo que nos atrevemos a hacer una **segunda clasificación** que denominaremos "global", y que trata de abarcar el mayor número de circunstancias personales y coyunturales de los potenciales usuarios.

Este es el catálogo que hemos definido.

- **El usuario "concienciado"**. Este hombre o mujer es una persona muy profesional que valora en su justa medida la importancia del enlace para acometer su trabajo en la mejor de las posiciones. Tiene su equipo TIC de dotación, al igual que el resto de sus herramientas, en las mejores condiciones de uso. Lo sabe usar a la perfección y conoce sus capacidades reales. Es plenamente consciente de las características del enlace en una emergencia, y por tanto conoce los medios y procedimientos alternativos que debería poner en práctica en el hipotético caso de que fallara su modo de enlace principal. Suele recurrir poco al responsable TIC de la organización, y cuando lo hace suele ser por alguna razón totalmente justificada (y aquí no estamos jugando con la ironía...). Además suele aportar posibles soluciones a los problemas detectados. Es mucho más normal encontrarlo al nivel interviniente que no en el nivel de dirección o gestión de la emergencia.
- **El usuario "inocuo"**. Es el más abundante que podemos enmarcar dentro de la normalidad. Conoce su trabajo y se ayuda de las TIC. Cuando no funcionan o tienen fallos lo comunican dentro de los procedimientos establecidos, no sin que ello signifique dejar de exigir su solución en el menor tiempo posible. Conoce las TIC en su justa medida como usuario y aunque no conoce las características de los sistemas de telecomunicaciones e información en emergencias es respetuoso con sus responsables. Lo podemos encontrar en cualquier nivel jerárquico.
- **El usuario "maleducado".** Es una persona exigente que se considera en posesión de la verdad. No suele conocer la importancia de las transmisiones y la de sus características en un contexto de emergencia. Emplea

expresiones ofensivas contra el sistema y sus responsables cuando las TIC fallan. Incluso cuando las quejas son justificadas, las formas empleadas le anulan profesionalmente. Se suelen dar en altos niveles de la cadena de mando o coordinación.

Existen dos variedades. El maleducado desconocedor de las TIC y el maleducado *per se*.

- ¤ El "maleducado desconocedor de las TIC" es alguien con escasa formación en la materia que suele ignorar el campo del enlace, por lo que no es de esperar ningún tipo de comprensión, sino todo lo contrario. Este usuario no es factible como usuario inocuo ya que posee una actitud negativa a verse involucrado con las tecnologías y resulta inútil volcarse en él. Tratará de ocultar su baja cualificación mostrando indignación ante las caídas del sistema, y si tiene necesidad no dudará en justificar sus errores con los fallos del enlace.
- ¤ El "maleducado *per se*" es alguien que reparte sus improperios por igual entre los que tiene a su alrededor, por lo que al tratarse de un profesional de la mala educación el Responsable TIC debe sentirse menos incómodo, al ser uno más dentro de los que le "aguantan".

- Llegamos al usuario "**comprensivo**". Este personaje es alguien que valora el trabajo de las TIC y que suele haberse informado de las características del enlace en emergencias. No suele conocer los medios ni las alternativas de enlace posibles como ocurría en el usuario concienciado, pero en cambio es curioso, pregunta y se deja asesorar. Existe una variedad.
  - ¤ El "comprensivo conocedor de las TIC", que es aquel que atesora algún conocimiento sobre nuevas tecnologías y que trata de demostrarlo. No suele ser muy insistente y con que se le dé la razón alguna vez y se le muestre un poco de "cariño", suele dejar trabajar. Suele darse en los niveles altos de la jerarquía.
- Dejamos para la última posición al **usuario "Inca"**. Se le denomina así porque es **incapaz** de realizar muchas de las tareas que exigen hoy día los sistemas de telecomunicaciones e información. Es el grupo de personas que se resignaron a utilizar la tecnología porque no les quedaba otra opción. Unas veces por **nerviosismo o prisas,** y otras veces por pura **torpeza**, suele ser una importante carga de trabajo para los responsables TIC de la organización, ya que como hemos explicado con anterioridad interactúa en exceso con los sistemas provocando, en el peor de los casos, importantes efectos dañinos. Se puede dar en cualquier nivel.

ENTONEMOS EL "*MEA CULPA*"

Igual de comprensible será que los Responsables TIC comentan, o mejor dicho, cometamos errores. No estamos hechos de otra pasta, ni estamos en posesión de la verdad absoluta. En ocasiones seremos los culpables de que el sistema falle, bien por errores propios, por fallos de la tecnología, por errores en el planeamiento del enlace, o simplemente porque hemos descuidado el adiestramiento de nuestros usuarios. Esto sin duda nos lleva de nuevo a recordar la clasificación de los Responsables TIC que acometimos, en justo castigo, en el capítulo anterior.

El rol que debe jugar el responsable TIC dentro de su organización de emergencias es fundamental, ya que debe cumplir la **función de guía o de maestro con sus usuarios,** es decir, de andamiaje; sobre todo en

contextos donde el uso de las TIC implique tareas complejas o innovadoras que obliguen al usuario a abandonar unos hábitos adquiridos.

Ya hemos aludido a lo largo de los primeros capítulos que **los fallos más comunes en nosotros los TIC** están concentrados en dos grandes bloques. No trataremos el hecho de que el enlace no se alcance o no se hagan las tareas necesarias para resolver la situación, porque en tal caso estaríamos hablando de un mal profesional y punto.

El primero de los fallos a que nos referíamos es el de **emplear constantemente un lenguaje excesivamente técnico** cuando hablamos con los usuarios. Ellos desconocen nuestra jerga y al dirigirnos a ellos con términos extraños tales como megabytes, ancho de banda, PIRE, dirección IP, etc., para explicar o excusar el comportamiento de un equipo o sistema, hace que **creen una repulsión natural hacia las TIC y en muchas ocasiones también hacia nosotros.**

Es el llamado "**TIC *proof***". El usuario crea una coraza de autoprotección y se blinda ante el personal TIC, porque no entiende lo que le estamos diciendo. Cuando el usuario encuentra alguna dificultad busca soluciones inmediatas. No quiere saber porqué no funcionan los equipos. Él, **lo único que quiere es que se lo arreglemos.** Ojo, que no estamos diciendo que no demos explicaciones si la situación lo requiere, pero si lo hacemos debemos cambiar el registro idiomático. Ejemplo.

¿Cuál de los dos mensajes siguientes es más apropiado para comunicar al director de una emergencia que tenemos dificultades para enlazar por radio con la base retrasada?

> ***Mensaje 1:*** *Director, hemos perdido el enlace HF con la base retrasada porque existe poca ionización en la ionosfera y la frecuencia utilizada atraviesa la atmósfera sin que se produzca la reflexión deseada de la onda electromagnética.*
>
> ***Mensaje 2:*** *Director, hemos perdido temporalmente la comunicación radio con la base retrasada. Hay que esperar a que amanezca.*

Es evidente que la información que necesita el director es la proporcionada en el segundo de los mensajes. Si nos decidimos a usar el primero de los mensajes, el Director de la Emergencia probablemente "desconecte" y tras la palabra "ionización" haya vuelto a pensar en su trabajo.

El segundo error más común en los Responsables TIC es el de tratar de imponer sistemas que el usuario no ha reclamado y que ni siquiera necesita. Este es un factor muy importante, y debería ser realmente el primero a tener en cuenta. Si un servicio no es necesario o tiene problemas de aceptación por parte de los usuarios, entonces no merece la pena dar un paso más en su explotación.

Este es un problema agudizado a causa de la rapidez de los avances tecnológicos. Existen diferentes teorías dentro de las empresas creadoras de nuevos servicios TIC. La llamada "***technology push***" apunta que se deben buscar usuarios para una determinada oferta tecnológica. En el lado opuesto encontramos la teoría del "***market pull***", la cual indica que se debe buscar la oferta tecnológica que satisfaga unos requisitos plantados de manera específica por el usuario.

Lo cierto es que si hubiéramos seguido los pasos indicados en los capítulos anteriores referidos al diseño de nuestro sistema de enlace en base al **concepto operativo** de los directores de las emergencias, por definición, habríamos acabado adoptando la **teoría del *market pull***.

Sin embargo siempre existe la posibilidad, y nosotros los TIC tendremos tentaciones de probar la ***techonology push***, pretendiendo incorporar alguna mejora al sistema. Si es así lo único que nos queda es recomendar la realización de una prueba o demostrador que "enganche" al usuario esperando una reacción positiva. Dicho demostrador se implantaría en un entorno aislado de preproducción, y una vez validado por la autoridad, se incorporaría al sistema y a los procedimientos.

Lo que desde luego no tendría ninguna lógica sería imponer algo innecesario o que no resulta cómodo su uso. Fácil de decir pero complejo de mantener. Sino que los lectores más experimentados echen la vista atrás y que confiesen sus pecados...

SENSIBILIZACIÓN Y CONSTRUCCIÓN DE UNA IMAGEN POSITIVA DE LAS TIC.

La **imagen de las TIC** para un usuario **varía considerablemente dependiendo del contexto en el que se produce su utilización.**

Si hiciéramos una encuesta a la población menor de 50 años, sobre lo que opinan del uso de las nuevas tecnologías en su **vida diaria**, no cabría duda de que la inmensa mayoría atestiguaría que las TIC son muy útiles y que han favorecido la calidad de vida y el acceso a la información. Sin embargo, si hacemos esa misma pregunta centrada en el uso en el **puesto de trabajo** de su organización, la imagen ya no es tan positiva.

Sin ánimo de entrar en disquisiciones psicológicas, no cabe duda de que el contexto profesional, más exigente y con responsabilidades añadidas, conlleva a un aprendizaje y a un uso de las TIC obligatorio que no existe en la vida privada, en la "no laboral".

Es decir, que en **nuestra casa,** y si nos apetece, hacemos el esfuerzo de aprender a usar una nueva herramienta tecnológica. Además no tenemos límites temporales más allá de los que nos queramos autoimponer. Si no tenemos éxito, o sencillamente no nos gusta, la abandonamos sin que por ello haya repercusión alguna. Por tanto los usuarios **se tienden a conformar** con lo que son capaces de obtener de las nuevas tecnologías en su vida particular.

Sin embargo en **nuestro trabajo** las circunstancias son diferentes. La herramienta TIC es una imposición por parte de la empresa para aumentar nuestro rendimiento, lo que ya en sí es percibido como algo menos amigable. Tenemos que aprender su uso en un periodo de tiempo limitado. Si el entorno en el que se lleva a cabo el aprendizaje es de estrés, como cabría esperar en una emergencia, el índice de rechazo puede ir claramente en aumento.

Podemos afirmar por tanto que las TIC no dan en general una imagen tan buena en el trabajo como fuera de éste por diversas razones. Sin embargo, a nuestro entender, **lo que realmente importa es el servicio que el usuario obtiene gracias a los medios de enlace** que se ponen a su servicio, y en cualquiera de los dos contextos es beneficioso. Nos estamos refiriendo al **acceso a la información.**

Este hecho incosteable en ocasiones pasa inadvertido. Existe una posibilidad poco practicada hasta la fecha en el campo del enlace en las emergencias y más concretamente en el de las nuevas tecnologías. Proponemos adentrarnos en el campo de las **técnicas de comunicación y marketing para favorecer por parte del usuario una mejor aceptación de las TIC** en su vida laboral en el día a día, pero sobre todo durante una emergencia.

Una **buena campaña de marketing** aumentaría exponencialmente las posibilidades de lograr que un producto sea exitoso. Si logramos acercar nuestro "producto TIC" a los usuarios habremos andado ya un gran camino. Debemos tratar por tanto que en nuestras organizaciones se utilicen las técnicas de comunicación para que estas herramientas tecnológicas se conviertan en algo cotidiano y amigable. Proponemos incluir aspectos relacionados con la **sensibilización y la construcción de una imagen positiva de las TIC.**

Veamos algunas sugerencias en esta dirección.

INCREMENTO DEL USO

En un primer momento se debe fomentar que el usuario se conciencie de la necesidad de **incrementar el uso de las nuevas tecnologías** en un **ambiente convencional de no emergencia.** Para que los usuarios sean conscientes de las ventajas de acceder permanentemente a la información gracias a las TIC, hace falta convencerles de la **necesidad de aprender a usarlas independientemente del entorno.** Debemos tratar de derribar esa barrera psicológica que les impide tratar a las nuevas tecnologías de manera similar en casa y en el trabajo.

CAMPAÑA DE MEJORA DE LA IMAGEN

Los responsables TIC debemos fomentar la sensibilización tanto hacia las nuevas tecnologías como hacia otras herramientas que sean de nuestra responsabilidad. Hay que **conseguir que se valore la importancia de su utilización y del acceso a la información que proporciona** su correcto uso.

Dentro de los distintos tipos de usuario que hemos definido encontramos algunos que no valoren la importancia de informarse, o lo que les puede enriquecer el uso cotidiano de las nuevas tecnologías. Otros desconfían de que puedan obtener la información que precisan en tiempo y forma adecuada. Algunos rechazarán de plano el uso de las TIC, por miedo a no superar la dificultad de su uso, e incluso los habrá que desconfíen de su eficacia. Seguro que habrá reticencia hacia nosotros, los expertos o responsables en las TIC. Resistencia al cambio de los hábitos adquiridos, rechazo o incomprensión de las normas y limitaciones que imponen los ordenadores, las radios, los teléfonos móviles, etc. En definitiva, miedo a preguntar, por temor a hacer el ridículo, o incapacidad de asumir que no se sabe algo.

Debemos empezar por **crear una imagen positiva** de las herramientas que ponemos a su disposición, que facilite y anime al uso. Esta imagen les predispone a aceptar las herramientas que les van a facilitar el enlace, sean tecnológicas o no.

Entre otros aspectos que podemos trabajar, la **imagen de las TIC depende de:**

- **De mensajes explícitos:** desde la acogida inicial que recibe el trabajador cuando llega a la organización, pasando por la imagen establecida de la propia agencia, hasta mensajes

gráficos como lemas, carteles, anagramas, logotipos, etc., que configuran la identidad visual del organismo. Si un organismo presume de estar a la vanguardia de la tecnología, será raro que un trabajador del mismo se niegue a aprender. Sin duda estos mensajes condicionan psicológicamente al usuario.

- **Del entorno físico:** la decoración, el edificio, el emplazamiento y la distribución del espacio. Un edificio moderno lo suele ser en todos los aspectos incluyendo, por descontado, los sistemas de telecomunicaciones, lo que va a predisponer al usuario de las TIC a un "mini reto" adicional.
- **De los servicios que se ofrecen en sí mismos:** Normalmente a mejores servicios, mejor imagen que percibe el usuario. Si por el contrario la organización impone algún tipo de restricción tecnológica[82] entonces la predisposición ya no es tan positiva. En tal caso conviene aclarar a los usuarios que son políticas de empresa, sin que el personal TIC tenga responsabilidad alguna mas allá, de la del cumplimiento e implantación de las instrucciones recibidas.
- **Del respaldo organizacional:** una entidad que fomente las TIC y que las exija es fundamental.
- **De la resolución de incidencias:** la velocidad de reacción, del éxito o fracaso en la resolución de problemas del usuario con sus herramientas TIC, marcarán de plano las futuras relaciones y la opinión de los "sufridores". Los servicios de HELP DESK son básicos en cualquier organización tal y como hemos comentado en el anterior capitulo.
- **De la imagen del personal responsable TIC:** Nuestra propia imagen influye. Sin entrar en aspectos físicos banales, el tipo de relación, trato y servicio que le demos al usuario será uno de los aspectos más relevantes.

MEJORA DE LA RELACIÓN USUARIO - HERRAMIENTA

A continuación apostaremos por **mejorar los modos de relación** que se dan entre los usuarios y las TIC, todavía en un **ambiente de no emergencia**. Trataremos de detectar las barreras a la relación, sus posibles soluciones y las actitudes que las favorecen.

Debemos ver, en primer lugar, qué obstáculos se interponen en esta relación, en esa comunicación, y después ver algunas actitudes y técnicas que favorecen su mejora.

Las barreras a la relación pueden deberse a:

- **Falta de formación:** el usuario no ha recibido la instrucción TIC necesaria para acometer sus obligaciones.
- **Características personales del usuario:** desconfianza hacia las nuevas tecnologías, desconocimiento de sus necesidades, indiferencia, prepotencia, intolerancia, falta de atención e interés...
- **Procedimientos erróneos:** la utilización de normas inapropiadas que exijan esfuerzos desproporcionados a los usuarios en comparación con los resultados obtenidos.
- **Semánticas:** uso de un lenguaje inadecuado a los conocimientos de los usuarios
- **Inaccesibilidad a los Responsables TIC:** bien porque se haga uso de barreras físicas como ventanillas, mostradores inadecuados, o sencillamente porque no responde al teléfono ante la aparición de una incidencia.

82. Por ejemplo la limitación a determinadas páginas web en horario laboral, filtrado de correo electrónico, prohibición de llamadas telefónicas a móviles, etc.

Deberemos por tanto tomar acción y cambiar las actitudes que favorezcan la relación entre el usuario con la herramienta; pero también las que faciliten la comunicación interpersonal entre usuario y Responsable TIC.

Las capacidades inmediatas de las TIC que el usuario medio puede identificar por sí mismo deben ser **complementadas a través de nuestro esfuerzo con otras menos obvias,** que amplifiquen las ventajas de su utilización.

Tenemos que hacer ver a nuestros usuarios que las TIC les van a acompañar a lo largo de toda su vida, y que ello entraña **aprender a manejar las herramientas que les dan acceso a la información** y los condicionantes. Ello requiere actuar sobre la **formación inicial** en los puestos de trabajo. Este aprendizaje debe ser realizado por los propios responsables del enlace o por profesores cualificados que deben apostar por la sencillez y la cercanía para llegar a la correcta interacción usuario máquina. Por muy sencillos que a priori puedan parecer se deben invertir unas horas en enseñar la utilización básica de la radio, ordenador, PDA, etc. Este contacto primerizo servirá además para que se conozcan Responsable TIC y usuario.

Se debe recurrir a **paneles informativos y hojas de ayuda** en las proximidades de los medios TIC. Hay que huir de repartir manuales soporíferos entre los usuarios. Es preferible hacer guías rápidas de uso a un manual de cientos de hojas en la búsqueda de una resolución puntual de un problema. Estas guías deben estar fijadas al propio equipo o en sus proximidades (pared, mesa, etc.). Si se deja "suelta" será archivada en cualquier cajón y no servirá para aquello para lo que se diseñó.

Y sobre todo práctica. **Mucha práctica** con los medios TIC en contexto de no emergencia de momento...pero que el usuario se familiarice, memorice y descubra los problemas que a ciencia cierta se le presentarán en una intervención real.

La **relación** podrá ser considerada **correcta entre usuario y las TIC cuando éste asuma su utilización, se valga de ellas para su trabajo, las entienda, las acepte, resuelva los problemas básicos cuando estos se presenten y nos retroalimenten** a nosotros como responsables de su correcto funcionamiento.

MEJORA DE LA RELACIÓN USUARIO - RESPONSABLE TIC.

Toda comunicación humana requiere, además de unas técnicas adecuadas, una serie de **actitudes hacia el interlocutor** que favorezcan la comprensión y aceptación de los mensajes. En la comunicación que mantengamos los responsables TIC con nuestros usuarios también debemos tenerlas presente. En este momento vamos a decir lo que debemos hacer nosotros, independientemente del tipo de usuario al que nos enfrentemos, y de las "formas" que éste utilice.

Nuestro comportamiento debe regir las siguientes pautas:

- **Consideración positiva incondicional:** aprecio, respeto, aceptación e interés por el otro. Para entablar contacto con el usuario debemos tener interés por su problema. Para él en ese preciso instante no hay nada más importante que el sentirse atendido. Incluso cuando no utilice los términos correctos. Esto permite un clima favorecedor de la comunicación y la cooperación. Incluso si el usuario nos falta al respeto, debemos ser capaces de identificar el problema tecnológico que tiene, independientemente que luego, si podemos..., le pongamos en su sitio. Si nosotros también partimos del menosprecio, o nos erigimos en árbitros de su capacidad, su necesidad, lo propio o impropio de su conducta, etc., no podremos hacer bien nuestro trabajo. Aunque tengamos la tentación de cortarle todos los enlaces y dejarle "aislado"... no debemos hacerlo. Hay que mantener un tono cordial y considerado. Dar la oportunidad de expresar su problemática, sin emitir juicios de valor. Expresar la voluntad de comprenderles y ayudarles. Si hay que contradecirles, o remitirlos a otro sitio, hacerlo con delicadeza, y con razones objetivas.
- **Dedicar el tiempo necesario al usuario:** Debemos organizarnos, nosotros y a nuestro personal, para que siempre haya alguien de servicio a disposición del usuario, dejándole y facilitándole que nos detalle el asunto en cuestión.
- **No demostrarle sus escasos conocimientos TIC:** a nadie le gusta que se le humille, y menos cuando además están envueltos en un problema. Se debe mostrar igualdad y nunca superioridad sobre el usuario.
- **Utilizar un lenguaje comprensible para él:** pecado habitual. Algunas recomendaciones para la mejor comprensión de nuestros mensajes son el expresarnos con brevedad y claridad, sin sobrecargar de datos accesorios, pues desviamos la atención de lo esencial. Es importante intuir el nivel de comprensión del interlocutor y adecuar nuestro lenguaje a él. Sencillez no implica menos

precisión. Por último es recomendable la ilustración. Dar ejemplos para reforzar la comprensión y la memoria de lo que queramos decir a los usuarios

- **No discutir jamás con un usuario:** debemos escuchar de forma activa, asentir y hacer eco de lo dicho. Señalar lo positivo de lo que han dicho, aceptar las objeciones y opiniones contrarias que enriquezcan. Hay que pedir que expliquen sus ideas o sugerencias y mostrar sinceridad, evitando suspicacias.
- **Mostrar autenticidad y empatía con el usuario:** esta actitud se refleja en una conducta espontánea, no encorsetada. Ponernos en el nivel y la perspectiva del otro, para crear una situación de diálogo fluido. Atender a lo no verbal, mirar al otro como señal de atención, cooperar físicamente con gestos afirmativos. Dar seguridad a quien nos habla y dejarles que terminen aunque sepamos lo que van a decir.
- **No dar más explicaciones de las necesarias:** además hay que huir de las explicaciones técnicas por las que se producen los fallos, y mucho menos los condicionantes tecnológicos que se tienen que producir para que el problema desaparezca.
- **No prometer cosas que no se han comprobado previamente:** Por muy fácil o sencillas que parezcan, el Responsable TIC debe comprobar el servicio antes de decir que funciona. No debemos olvidar que tenemos una doble dependencia: de la tecnología que no falle, y del usuario que haga uso del servicio correctamente.

APLICACIÓN EN LA EMERGENCIA

Una vez se ha logrado captar la atención sobre las TIC, se ha enseñado su uso, y hemos roto las barreras que impiden una relación fluida entre el usuario y nosotros, faltará trasladarlo a un ambiente hostil, un ambiente de emergencia.

Sin llegar al aforismo del docente y pedagogo argentino Faustino Sarmiento de "la letra con sangre entra", no cabe duda alguna de que es en estas situaciones extremas cuando se acabarán de dominar los equipos y procedimientos TIC, que debiéramos haber aprendido a utilizar antes de la emergencia.

Lo que decimos es muy complicado de realizar, ya que por suerte no estamos continuamente interviniendo en las emergencias. La solución pasa por ejercitar lo aprendido y asimilado en un contexto de no emergencia en ejercicios y simulacros.

CAPÍTULO 12

¿DIRECCIÓN, COORDINACIÓN O MANDO EN EMERGENCIAS?

En este capítulo vamos a tocar un tema curioso. En la gestión de las emergencias se ejercen distintos roles por parte del personal responsable de su resolución. Dependiendo de la procedencia o de la naturaleza del colectivo encontraremos **expresiones diferentes** que unos y otros emplean para dirigirse a un **mismo concepto**.

Este "concepto" no es otro que **la actividad que desarrollan los responsables en sus niveles correspondientes para planificar, dirigir, coordinar, decidir y controlar el empleo de los medios y las personas puestos a su disposición para resolver la emergencia en el menor plazo de tiempo posible.**

En cualquiera de los países anglosajones, y el mayor parte de los países europeos, nadie tendría dudas en decir que ese concepto no es otro que el de **Mando en Emergencias.** Pero una vez más en nuestro país somos dispares, si quieren incluso discrepantes.

Una parte muy importante de los responsables de la gestión de catástrofes en España se refieren a este concepto con expresiones tales como **Coordinación o Dirección de Emergencias.** ¿Existe diferencia entre los que ejercen el mando de los que realizan dirección o coordinación? ¿Son diferentes las misiones que desarrollan? A estas preguntas, y alguna otra, intentaremos dar respuesta en las siguientes páginas.

RELACIÓN DEL RESPONSABLE TIC CON ESTA DISYUNTIVA

Comenzaremos diciendo que esta diferencia en la **terminología no nos afecta** en absoluto como Responsables TIC ya que el enlace hay que materializarlo independientemente del nombre que se le dé. Sin embargo es cierto que si recordamos la definición de enlace vista en el capítulo 1, hablábamos de ciertas "acciones" que tendríamos que llevar a cabo que en ocasiones tendrían muy poco que ver con nuestras "misiones tipo" del Responsable TIC. Bien, pues **muchas de estas acciones están relacionadas con el Mando, la Dirección o la Coordinación** de las emergencias.

A nosotros como Responsables TIC, nos da igual el envoltorio. Nos interesa el contenido, o mejor dicho los componentes de los sistemas para el mando o la dirección que se hayan implantado. Por el momento diremos que para nosotros debe ser suficiente con saber que **somos una parte dentro de la globalidad del sistema de gestión de la emergencia**, y que habrá veces que tengamos que mover la "caja de ratones" para que todo el mundo aporte su parte.

Uno de los componentes esenciales de los sistemas de Mando, Dirección o Coordinación de las emergencias lo constituyen los **sistemas auxiliares que permiten obtener, tratar, almacenar, presentar y transmitir la información**, que como ya sabemos son los Sistemas de Telecomunicaciones e Información. Esta proximidad semántica y física, en ocasiones, lleva a malentendidos. Algunas organizaciones hacen responsable del Mando y Control de la organización a su experto TIC, cuando realmente lo que se quiere decir es que el "hombre TIC" de la organización es el responsable de los Sistemas de Información y Telecomunicaciones para el Mando o de la Dirección de la organización.

Lo irrefutable es que la función del **Mando, Dirección o Coordinación de una emergencia es sobre todo gestión de la información,** y aquí sí que los sistemas TIC[83] tienen mucho que aportar. No lo son todo, sin embargo nuestro asesoramiento, conocimiento de los sistemas y en ocasiones buenas dosis de trabajo subterfugio, ayudarán al buen desarrollo de la función.

DIRECCIÓN VS COORDINACIÓN VS MANDO

Aunque haya individuos que, por una u otra razón, distingan estos conceptos lo primero que nos proponemos es ver y analizar si existen realmente diferencias entre ellos.

DIRECCIÓN Y GERENCIA

Crisis es todo lo que altera el normal funcionamiento de una organización exigiendo decisiones rápidas para superarla. Según algunos tratadistas, nos encontramos en crisis permanente (caso de emergencias ordinarias). Decía Heráclito que "...todo fluye, nada permanece, ningún momento es igual al anterior y constantemente tenemos que tomar decisiones para resolver la situación del momento...". Pues bien, para superar una situación de emergencia o crisis es **indispensable disponer de un sistema de "gestión".** A veces este sistema se limita al pensamiento de una única persona. Este hombre o mujer puede contar con medios adicionales como personal auxiliar o herramientas TIC para agilizar su trabajo. Esta persona es la que ejerce la dirección.

Según el Diccionario de la Lengua Española (22ª edición), **Dirección** es "Consejo, enseñanza y preceptos con que se encamina a alguien", o "Encaminar la intención y las operaciones a determinado fin". También es "Acción y efecto de dirigir".

También nos dice el glosario que **Dirigir** es "Gobernar, dar reglas para el manejo de una empresa o pretensión"; "Aconsejar y gobernar la conciencia de alguien" u "Orientar, guiar, aconsejar a quien realiza un trabajo"

> *El ejemplo en España más evidente de entidad relacionada con las emergencias que conjuga el verbo dirigir en primera persona podría ser la Dirección General de Protección Civil y Emergencias del Ministerio de Interior, o cualesquiera de las Direcciones Generales de las Consejerías que lidian con estos asuntos en las Comunidades Autónomas (Dirección General de Seguridad y Emergencias del Gobierno de Canarias, Direcció General d'Interior, Emergències i Justícia de la CAIB, Dirección General de Seguridad Ciudadana y Emergencias de la Región de Murcia, Direcció General de Protecció Civil de Catalunya, etc).*

En el mundo empresarial y también en el de las emergencias aparece recurrentemente otro término relacionado con el de dirección, la "Gerencia". La **Gerencia** es "El arte de hacer que las cosas ocurran". Se entiende que es la dirección de más alto nivel dentro de una organización. El economista cubano, Dr. Alberto Krygier

83. Los sistemas de telecomunicaciones e información se pueden considerar como la dimensión física de la gestión de la información.

decía que la gerencia era el proceso que implica la coordinación de todos los recursos disponibles en una organización (humanos, físicos, tecnológicos, financieros), para que a través de los **procesos administrativos** se logren los objetivos previamente establecidos.

Los procesos administrativos[84] han sido estudiados durante muchísimos años para la mejora de resultados de las organizaciones. Uno de los referentes más importante es la aportación realizada por William Newman[85] con el llamado "**Proceso Administrativo de Newman"**. En él se identifican cuatro componentes:

1. Planificación: supone definir objetivos organizacionales y proponer medios para lograrlos. Los gerentes planean por tres razones: fijar un rumbo general de la organización, identificar y asignar los recursos para alcanzar sus metas y para decidir qué actividades son necesarias para lograr los objetivos.
2. Organizar: es el proceso para ordenar y distribuir el trabajo, de tal manera que estos puedan alcanzar las metas de la organización. Diferentes metas requieren diferentes estructuras para poder realizarlos.
3. Dirigir escalones inferiores: supone hacer que los demás realicen las tareas necesarias para lograr los objetivos de la organización. Según Fayol[86], "Una vez constituido el grupo social, se trata de hacerlo funcionar. Tal es la misión de la dirección, la que consiste para cada jefe en obtener los máximos resultados posibles de los elementos que componen su unidad, en interés de la organización".
4. Control: proceso mediante el cual una persona, un grupo o una organización vigila el desempeño y emprende acciones correctivas.

También encontraremos ejemplos de gerencias relacionadas con las emergencias. Valgan como modelos la Gerencia de Emergencias del 061 de Murcia o la Gerencia de Emergencias Sanitarias de Castilla y León.

Por lo tanto hasta aquí podemos concluir que gerencia y dirección desarrollan funciones idénticas, pero que institucionalmente se utilizan para diferenciar rango de la persona que realiza la actividad.

Pasemos, pues, al siguiente concepto.

COORDINACIÓN

El segundo término a analizar será el de **Coordinación**. Una vez más recurriremos al Diccionario. Éste nos dice que es la "Acción de concertar medios, esfuerzos, etc., para una acción común". También se pudiera entender como el acto de gestionar las interdependencias que existen entre diferentes actividades.

Pero es desde nuestro punto de vista la definición dada por el ya mencionado William Newman la más completa. "Significa la sincronización y unificación de las acciones de un grupo de personas. Hay trabajo coordinado cuando las actividades son armoniosas, ensambladas e integradas hacia un objetivo común".

Por tanto podemos decir que la coordinación en las emergencias es el proceso de reunir a las agencias y los individuos para garantizar una gestión eficiente y eficaz de las tareas y los recursos para lograr objetivos acordados. Es primordial destacar que la **coordinación se realiza a través de enlace.** La coordinación se refiere principalmente a los **recursos**.

Ejemplos de órganos "coordinadores" en las emergencias pueden ser los siguientes. Los Comités

84. Proceso administrativo: conjunto de acciones interrelacionadas e interdependientes necesarias para llevar a cabo una actividad. Involucra diferentes actividades tendientes a la consecución de un fin a través del uso óptimo de recursos humanos, materiales, financieros y tecnológicos.
85. William H. Newman nació en Estados Unidos. Fue profesor de empresariales y un autor en el campo de la administración de empresas muy influyente. Además fue el último sobreviviente de los fundadores de la Academy of Management. Murió el 31 de mayo de 2002 a los 92 años. El Dr. Newman fue el primer profesor de Empresas y Negocios en la Universidad de Columbia.
86. Henri Fayol es uno de los principales estudiosos del enfoque clásico de la administración. Turco de nacimiento y parisino de adopción es sobre todo conocido por sus aportaciones en el terreno del pensamiento administrativo. Expuso sus ideas en la obra Administración industrial y general, publicada en Francia en 1916.

PROCESO ADMINISTRATIVO DE NEWMAN

Estatales de Coordinación de cada Riesgo (CECO) que preside el Subsecretario del Ministerio de Interior, los Centros de Coordinación Operativa (CECOP[87]) o los Centros de Coordinación Operativo Integrado (CECOPI[88]) definidos en los diferentes Planes de Emergencias.

En este punto nos atrevemos a sacar una importante conclusión. La dirección se dedica a mandar, influir y motivar a los empleados para que realicen tareas esenciales; podemos ver rasgos de motivación y sobre todo de liderazgo. Sin embargo la Coordinación está un escalón por debajo de la Dirección, y son las acciones que sincronizan recursos y actividades en proporciones adecuadas y ajusta los medios a los fines facilitando el trabajo y los resultados. En la coordinación vemos rasgos de organización, de planeamiento, pero también algo de liderazgo aunque en menor cantidad que en la dirección.

Llegamos al último de los conceptos.

MANDO Y CONTROL

El **Mando** es un concepto muy extendido en el ambiente castrense y también en el mundo de las emergencias en algunos países, sobre todo nórdicos y anglosajones tal y como mencionamos al inicio del capítulo.

Hasta hace muy poco tiempo en las Fuerzas Armadas el término **Mando** iba siempre ligado al de **Control (Mando y Control**, o en inglés *Command & Control*, por lo que es extensamente nombrado como **C2**). En su naturaleza el mando incluye al control, aunque en la práctica la ejecución en detalle de este último se podría delegar en una persona diferente a la que ejerce el mando. Las últimas tendencias apuntan a hablar en exclusiva de Mando.

Podemos encontrar diferentes definiciones. Para OTAN el **Mando**

87. El CECOP es el centro neurálgico de la gestión de la emergencia, donde se integran los servicios que efectúan la planificación y la coordinación de las operaciones en situaciones de grave riesgo colectivo, catástrofe o calamidad pública y dónde se efectúa la toma de decisiones.

88. En caso necesario, el CECOP se constituirá en CECOPI, mediante la incorporación de los responsables de la Administración Estatal, en los casos en que se declare el interés suprautonómico.

y Control es "El ejercicio de la autoridad y dirección de una persona investida como "**Jefe**" sobre una fuerza asignada durante el cumplimiento de una misión".

La Doctrina actual de Empleo de Fuerzas Terrestres del Ejército de Tierra define el **Mando** como "La autoridad y consiguiente responsabilidad, conferidas a un jefe, para el planeamiento y la conducción de las acciones de una fuerza militar". La anterior versión de esta misma Doctrina, todavía mantenía unido el concepto C2, y definía el **Mando y Control**[89] como "El conjunto de actividades mediante las cuales se planea, dirige, coordina y controla el empleo de las fuerzas y los medios en las operaciones".

El saber mandar o el mando en sí **es un arte.** Se trata del ejercicio consciente y hábil de ejercer la autoridad para cumplir con sus responsabilidades a través de la **toma de decisiones y el liderazgo.**

La verdadera medida del ejercicio del mando no es si un jefe utiliza ciertas técnicas o procedimientos, **sino si las técnicas y usos de los procedimientos son apropiados a la situación.**

El **Mando está circunscrito a una organización**, y es ésta la que le confiere la capacidad "legal" de ejercer las funciones necesarias para alcanzar los objetivos, metas o misiones que se le asignen a dicha organización.

El correcto ejercicio del Mando se deriva de años de formación, del desarrollo personal y sobre todo de la experiencia adquirida.

Si nos referimos al **Control** podemos decir que es "El proceso mediante el cual una persona, un grupo o una organización vigilan el desempeño y emprenden acciones correctivas en caso de necesidad de las actividades combinadas de las agencias y individuos involucrados en el cumplimiento de un objetivo acordado".

Control opera horizontalmente en todos los organismos y personas involucradas. El control en contraste con el mando **es más una ciencia** que un arte, y se sirve de diferentes herramientas para poder ejercitarlo. Control se refiere principalmente **a las situaciones**.

Se realiza normalmente en su término más amplio en las organizaciones de emergencias que cuentan con planas mayores y con personal auxiliar que está atento al desarrollo de los acontecimientos. En los escalones más bajos, en los intervinientes por ejemplo, los jefes de equipo sólo pueden ejercer un control mínimo.

Los elementos primordiales para ejercer el control son:

- El establecimiento de normas de ejecución o desempeño de las tareas.
- Medición de los resultados presentes y compararlos con las normas establecidas.
- Gestión de la información, de la cual ya hemos hablado ampliamente en el capítulo 7, para llegar a la toma de decisiones que permitan tomar medidas

SIGLAS RELACIONADAS CON EL MANDO Y CONTROL

NATO
I
OTAN

- C2 (Command and Control)
- C3 (C2 + Communications)
- C3I (C3 + Intelligence)
- C4I (C3 + Computer)
- C4I2 (C3I + Interoperability)
- C2IS (+ énfasis Sistema)

89. Por otro lado la Doctrina de Mando y Control define por separado ambos términos. Así Mando es la "Autoridad conferida a un Jefe para planificar, dirigir, coordinar, decidir y controlar el empleo de fuerzas militares a él subordinadas". Control es entonces la "Actividad por la que el Jefe, asistido por su Estado Mayor o Plana Mayor, organiza, dirige y coordina las fuerzas y medios asignados para una misión".

correctivas cuando no se cumplan las normas de ejecución.

- Y por último los **medios de enlace** a su disposición que sirvan para establecer el flujo de información.

A tenor de lo expuesto podríamos decir que el **Mando y Control en una Emergencia** es "La autoridad legal conferida a una persona para planear, dirigir, coordinar y controlar los medios personales y materiales puestos a su disposición por la administración correspondiente, durante el tiempo en que dicha emergencia permanezca activa".

Es decir **mandar es mucho más que dar órdenes** y aplicar normas y procedimientos, es asumir responsabilidades constantemente en todas y cada una de las fases de la emergencia. Independientemente de la documentación que consultemos se indica que **el Jefe**, entendido como autoridad que ostenta el mando, nunca podrá ejercerlo en solitario excepto en los niveles más bajos de mando. Incluso en estos escalones más bajos necesitará disponer de un **Sistema para ejercer el C2.**

Ejemplos de órganos que "mandan" durante las emergencias en España encontramos los Puestos de Mando Avanzados que montan todas las CCAA y las grandes ciudades en la cercanía de las emergencias, los puestos de mando que puede llegar a montar la UME, o Jefaturas de Policía, que cambian la denominación de la función que realizan, por el de la persona que la ejerce.

COROLARIO FINAL

Pues tras examinar el significado de cada uno de los conceptos y ver la utilización que en nuestro país se hace de ellos para nominar a los diferentes organismos podemos concluir que los términos "**Dirección y Gerencia**" se aplican a los niveles más superiores de las organizaciones. Además suele estar ligado al conjunto de funciones y cometidos que se incluyen en la planificación, siendo empleado en muy pocas ocasiones para aquello que atañe a lo táctico u operativo. Suelen desempeñarlos cargos políticos.

La "**Coordinación**" es siempre un concepto subordinado o incluido en la dirección, que se aplica a niveles intermedios de las organizaciones. En emergencias, está ligado al conjunto de funciones para sincronizar participantes o intervinientes. Lo ejercen técnicos de muy alto nivel o políticos de menor rango que los anteriores con conocimientos operativos. La Coordinación opera verticalmente a través de una organización como una función de mando, y horizontalmente en todas las agencias en función del control.

El "**Mando**" o el "**Mando y Control**", es un concepto más ejecutivo-operativo, aplicable a niveles inferiores. En emergencias está ligado a las acciones directas para resolverlas, es decir a las actividades ligadas a la conducción y lo ejecutan técnicos.

Sin embargo una cosa es cómo se utilice en España y otra distinta lo que realmente se haga. La pregunta es sencilla. Cuando un **político** de cualquier organización llega a un Centro de Coordinación operativa o incluso se baja al barro y se sube a un camión de Puesto de Mando Avanzado, **¿está dirigiendo, coordinando o mandando?**

COMPARATIVA ENTRE C2 Y EL PROCESO ADMINISTRATIVO DE NEWMAN

MANDO & CONTROL ⬅·➡ PROCESO ADMINISTRATIVO NEWMAN

Mando y Control. Actividades mediante las cuales se:		Proceso Administrativo de Newman se compone de:
1. Planea	⟼	1. Planificar
2. Dirige	⟼	2. Dirigir inferiores
3. Coordina	⟼	3. Organizar
4. Controla	⟼	4. Control

Desde nuestro punto de vista mandan. Es mando porque toma decisiones que afectan a las organizaciones que tienen subordinadas. Es mando porque el político está investido de autoridad legal y el resto de miembros de la organización así lo reconocen. Es mando porque tiene capacidad para exigir que los demás le rindan cuentas de su trabajo. Y es mando porque participa en el planeamiento, la conducción y la coordinación de la emergencia.

Pero no son sólo los políticos. También los **técnicos en sus niveles respectivos ejercen el mando.** Dan órdenes y velan por su cumplimiento. Si somos bien pensados podríamos decir que estas personas se inclinan por verbos diferentes al de "mandar" porque, debido a condicionantes diversos, el uso de la expresión mandar, o **ejercer la autoridad en España sobre unos subordinados, tiene cierto carácter peyorativo hacia las personas que reciben las ordenes**. Si nos apartamos del "buenismo" y hacemos uso de nuestro pensamiento más suspicaz, podríamos llegar a la conclusión de que **quizás se emplean estos términos para huir de la responsabilidad si vienen mal dadas.** Como en casi todo, probablemente en el término medio encontremos la verdadera razón de este uso de expresiones diferentes para identificar una misma acción.

MANDO Y CONTROL EN LAS EMERGENCIAS

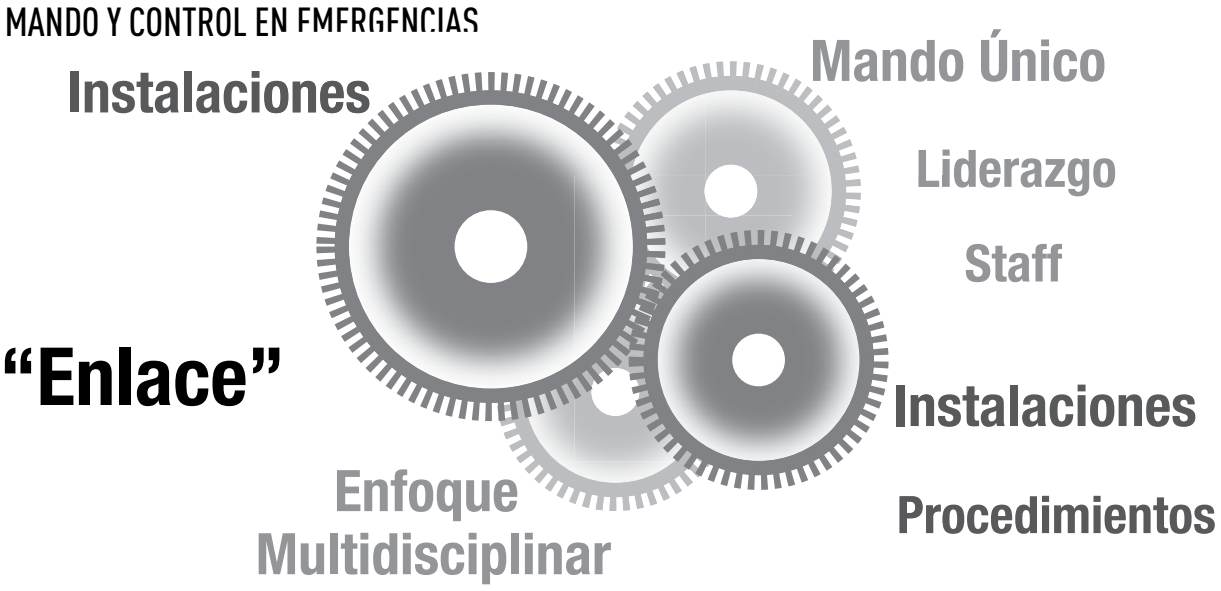
Las situaciones de emergencia se caracterizan por la irrupción brusca del desorden, la confusión, y el desconcierto en la vida cotidiana. **El estado de shock y la extensa destrucción** en la que se quedan las sociedades en las "situaciones de emergencia" es necesario contrarrestarla mediante la aplicación de medidas coordinadas por parte de todos los organismos participantes. La herramienta principal con la que se va lograr esta "hazaña" es implantando un **Mando y Control (C2) efectivo.**

El C2 en Emergencias se materializa mediante un "**Sistema de Mando y Control"** que contará al menos con los siguientes elementos:

- STAFF (estructura y personal)
- Medios e Instalaciones (incluyendo puestos de mando o centros de coordinación)
- Procedimientos
- Enfoque Multidisciplinar (*Comprehensive Approach*)
- **Enlace**
- Mando Único
- Liderazgo

STAFF (ESTRUCTURA DE MANDO Y PERSONAL)

Se debe contar con un **personal que se integre en una estructura de mando preestablecida,** aprobada y aceptada por todos. La necesidad se vuelve vital cuando se trata de grandes catástrofes. La implantación local de estructuras de mando, incluso en estado embrionario, constituye un impulso suplementario para la gestión de una crisis. El conocimiento de los interlocutores adecuados con anterioridad a las situaciones de crisis permite una ganancia notable en los tiempos y modos de llevar a cabo la reacción inmediata.



Por desgracia a veces incluso teniendo estas estructuras previstas no es suficiente. En las lecciones aprendidas difundidas por la Casa Blanca tras el Huracán Katrina, se destacó que la estructura prevista y asignada al Gobierno Federal de los EEUU, cuya misión hubiera sido la de coordinar los medios que diesen respuesta a las necesidades de Estados y ciudades, fue imposible de realizar ya que no se tuvieron en cuenta las circunstancias en las que se llevaría a cabo esta misión. A la falta de medios de enlace se unió la insuficiencia de personal, la desaparición del gobierno local y una dirección para establecer unas prioridades claras.

MEDIOS E INSTALACIONES (INCLUYENDO PUESTOS DE MANDO O CENTROS DE COORDINACIÓN)

El Mando y Control se debe basar en **instalaciones, fijas o desplegables,** y contar con las herramientas necesarias para llevar a cabo las tareas en las mejores condiciones. En el capítulo 9 ya hicimos mención a este respecto.

PROCEDIMIENTOS

Llevamos gran parte del libro destacando las grandes ventajas de tener las actividades **más esenciales procedimentadas** para poder realizarlas de modo automático independientemente del contexto en el que las llevemos a cabo. También se obtienen grandes ventajas en los procesos de transvase de conocimiento y en la gestión de la información.

ENFOQUE MULTIDISCIPLINAR *(COMPREHENSIVE APPROACH)*

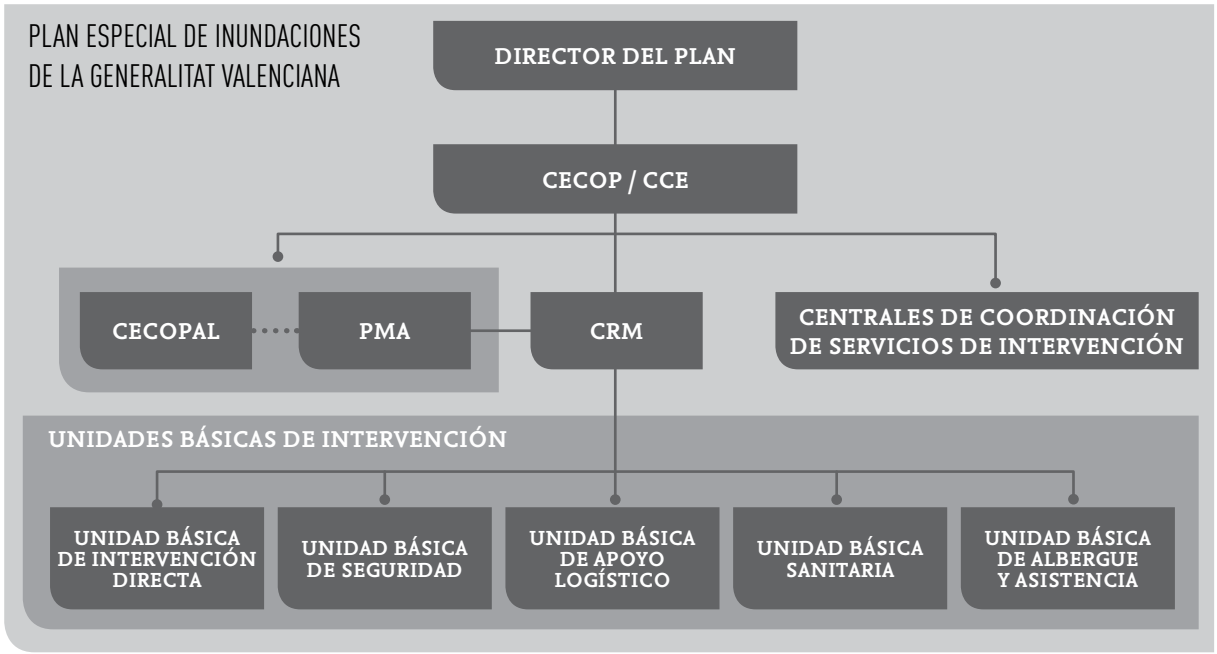
Salvo las pequeñas emergencias, o aquellas extremadamente especializadas, hoy día parece imposible imaginar un escenario en el que una única organización aborde en solitario la resolución de éstas.

De modo genérico podemos afirmar que el enfoque multidisciplinar se puede dar por dos causas:

- Se produce un **incidente complejo,** entendido como tal el que implica diferentes agencias capaces de gestionar en solitario emergencias propias de su ramo.
- Se producen **múltiples incidentes de distinta naturaleza** en una zona que deben ser coordinados por una misma autoridad

Sin embargo muchos incidentes que a priori se pueden gestionar con relativa facilidad, y que no precisarían un enfoque multidisciplinar, pueden complicarse derivando en un incidente complejo cuando se dan alguna o una combinación de las circunstancias siguientes:

- Se plantean problemas significativos de enlace.
- Se requiere una importante respuesta en términos de recursos.
- Existe un elevado número de heridos, muertos o damnificados.
- Se produce un gran daño a la propiedad o al medio ambiente.



- Se prolonga excesivamente en el tiempo.
- Se produce un alto grado de estrés o trauma en la sociedad.
- Genera un alto nivel de interés de los medios de información pública.
- Se involucra a agencias que no están acostumbradas habitualmente a participar en respuesta a incidentes.

La combinación de algunos o todos de estos factores requiere simplicidad en gestión, familiaridad con el enfoque y altos niveles de cooperación. Como cada agencia a menudo utiliza diferentes procedimientos y la terminología, un enfoque común facilitará su trabajo conjunto con el fin de gestionar los incidentes de la forma más rápida y eficaz posible. Organismos de Protección Civil, Sanitarios, Fuerzas Armadas o Cuerpos Policiales. La cooperación y la coordinación de todos ellos deben **alcanzar la sinergia** en las actuaciones.

ENLACE

Queremos una vez más llamar la atención del lector sobre el último componente del Sistema C2, el enlace. **Esto nos mete de lleno como responsables TIC en parte integrante del propio sistema de Mando y Control de la emergencia.** Si al principio del capítulo dijimos que éramos una parte dentro de la globalidad del sistema de gestión de la emergencia, tras este apartado nos atrevemos a decir que somos además una **parte esencial.**

Si tuviéramos que hacer frente a una gran catástrofe, el **sistema de Mando y Control** se convertiría en el **elemento impulsor de todas las acciones** que se deberían poner en liza para mitigar la situación. Si el **Sistema C2 es el cerebro** que organiza y manda las órdenes al resto de funciones, **el enlace es el sistema nervioso** que permite el flujo de información indispensable para controlar y evaluar la evolución de la situación.

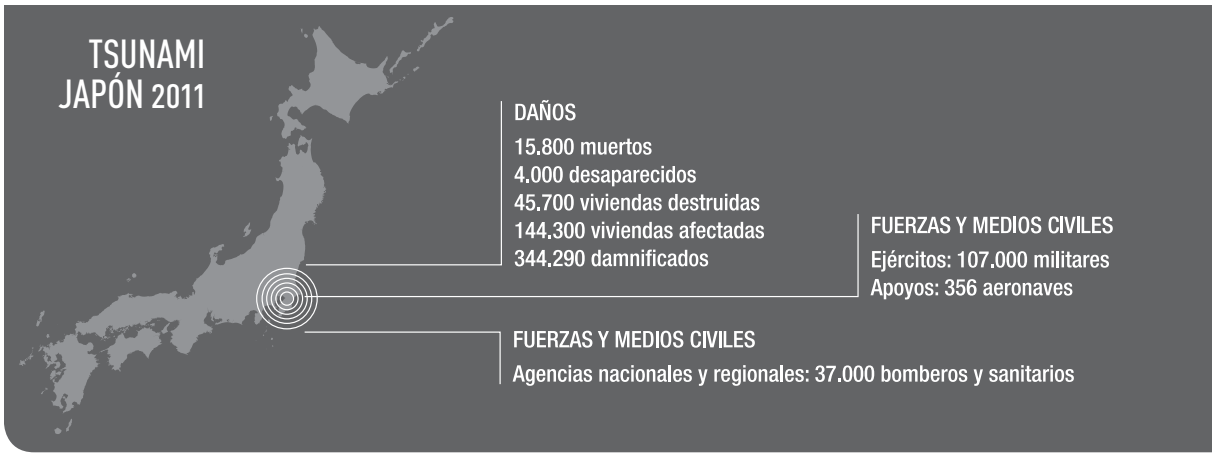
De acuerdo al informe de lecciones aprendidas elaborado por las Fuerzas Terrestres Japonesas, tras la crisis del **Tsunami del 2011** se detectaron una serie de problemas. A partir de marzo de 2011, y durante tres o cuatro días, **el gobierno japonés perdió totalmente la capacidad de dirección** de la emergencia. Pese a que con rapidez se **instauró una estructura de mando,** el colapso de las telecomunicaciones proporcionadas por los operadores civiles impidió el flujo de información, la estimación y análisis de la gravedad de la situación y por supuesto limitó la toma de decisiones. La situación no se resolvió hasta que fue capaz de aprovechar los recursos de **Mando y Control de las Fuerzas Armadas niponas,** y los **sistemas CIS de la Tercera Fuerza Expedicionaria de Marines de EE.UU.** que se puso al servicio del gobierno japonés.

De cara a una catástrofe natural que pudiera inducir una desorganización completa o parcial de los medios TIC de las autoridades civiles, las **Fuerzas Armadas normalmente estarán en disposición de tomar rápidamente el relevo.** Los ejércitos son una institución pensada para trabajar en el caos de una guerra, por lo que no les será difícil adaptarse al provocado por

LAS TIC EN EL TSUNAMI DE JAPÓN

Las TIC constituyen un factor esencial en el buen desarrollo de las operaciones de socorro. En el caso japonés se ha revelado la dificultad de llevar a cabo la evaluación y la coordinación debida a la destrucción de las infraestructuras de transmisiones gubernamentales.

En las respuestas a una catástrofe natural es decisivo restablecer rápidamente las redes de comunicaciones criticas, en unión con el apoyo de los operadores civiles y de las Fuerzas Armadas.



una emergencia. El CIS militar debe poder instalar los medios de mando necesarios que permitan a las autoridades legales continuar ejerciendo sus prerrogativas y en particular asegurar una coordinación eficaz de las operaciones de socorro.

MANDO ÚNICO EN LAS EMERGENCIAS

Los responsables de dirigir las emergencias precisan de un método eficaz que ayude a evaluar la situación, prever su evolución, decidir objetivos estratégicos a alcanzar, elegir tácticas adecuadas para conseguirlos, organizar los recursos y controlar de un modo continuo la intervención para readaptar el plan cuando sea necesario. Todo esto desde nuestro punto de vista **sólo se realizará si el mando es único en la gestión de la emergencia.**

El **Mando Único es sinónimo de "dirección coordinada"** y garantiza que todos los servicios y agencias participantes tengan una visión única de la situación y sepan con claridad cuáles son los objetivos a alcanzar y las estrategias a poner en marcha.

¡Ojo!, no es un invento exclusivo de militares. Muchas organizaciones civiles a lo largo y ancho del mundo utilizan esta filosofía que permite la **dosificación de esfuerzos, la aplicación correcta de los apoyos y permite sacar un mayor rendimiento de la información** obtenida porque es automáticamente compartida.

En este punto debemos hacer mención a un sistema de Mando que lleva en su propio nombre la característica principal del mismo. Nos referimos al ***Incident Command System* (ICS).** El Sistema de Mando de Incidentes se desarrolló originalmente en Estados Unidos en la década de los 70 y está siendo empleado en los últimos 20 años de un modo extensivo para dirigir y coordinar situaciones de emergencia de cualquier tipo. La principal característica de este sistema es que entre sus fundamentos claves[90], el ICS aboga por "el **Mando Único**" en la resolución de una emergencia. El Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos concluyó tras la tragedia del 11-S de 2001, que como solución a los problemas de interoperabilidad habidos se debía apostar por la implementación del Sistema de Mando de Incidentes (ICS), es decir, un mando único y puestos de mando avanzados con representantes de todos los departamentos que intervienen en la emergencia (enfoque multidisciplinar).

Por otro lado a nosotros **como responsables TIC, el mando único nos simplifica nuestros despliegue**s ya que suelen ser jerarquizados y por lo normal precisan menos medios que para atender grandes cúpulas de dirección que necesitan recibir la misma información y de manera simultánea.

El Mando Único es garantía de eficacia y las TIC deben estar en consonancia. Una obviedad como ésta no está reflejada en la realidad de las emergencias en España. De momento no existe una red única de gestión de emergencias a nivel nacional. El Secretario de "Homeland Security" de los EEUU incidió en su informe post Katrina en la necesidad de contar con un lugar donde poder compartir con todos los actores los sucesos y actividades que se estaban llevando a cabo, ya que él en ningún momento tuvo conciencia de lo que se estaba haciendo en otros niveles de la Administración. De ahí la importancia de la **Red Nacional de Emergencias (RENEM),** explicada en el Anexo 3.

El Mando Único será el responsable del control de la emergencia y asignará las tareas a los organismos participantes conforme a las necesidades de la situación. Es decir, especifica:

- Qué hay que hacer[91]
- Qué agencia debe llevarlo a cabo
- Dónde
- Y en qué momento

Las principales tareas a llevar a cabo por el Mando Único serían:

- La toma de control de la emergencia o catástrofe
- Evaluar la situación y asesorar a las autoridades competentes
- Establecimiento de prioridades y límites de tiempo
- Conformar el Puesto de Mando
- Elaboración del Plan
- Asignar misiones a las agencias participantes
- Coordinación de recursos y apoyo
- Solicitar recursos externos
- Informar de las acciones y actividades de los organismos y a las autoridades competentes
- Garantizar la seguridad de todo el personal participante en la emergencia
- El establecimiento de procedimientos de enlace

90. Fundamentos claves del ICS:
    - Jefe del Incidente
        - Desempeña la dirección global de toda la organización dispuesta para afrontar la emergencia
    - Establece los objetivos de la intervención.
    - Unidad Cadena de Mando
        - Cada individuo tiene designado un supervisor.
        - Estructura jerárquica con varios niveles y diferentes estructuras.
    - Integración de las Comunicaciones
        - Es necesario planificarlas.
        - Establecimiento de diferentes redes para propósitos operativos específicos: red de Mando, redes Tácticas, red de Apoyo y Banda Aérea.

91. Como es natural, el Mando determina quien hace las tareas, pero los organismos individuales son responsables de determinar la forma en que se va a hacer.

LIDERAZGO

Hemos visto que **el Mando** es aquella persona que está investida de autoridad legal y que además puede y debe exigir el cumplimiento de las órdenes que emanan de sus decisiones. Tiene capacidad para exigir que los demás le rindan cuentas de su trabajo.

Si a esa persona que además de tener las atribuciones propias del mando se le añaden cualidades positivas intelectuales y morales, y las adecuadas capacidades profesionales para ejercer sus funciones al frente de una organización o grupo, entonces tendremos **un Jefe**; en este caso un buen jefe. El Jefe debe ejercer el mando con plena responsabilidad, que no puede compartir con nadie y por tanto debe estar dispuesto a aceptar sus tinos, pero también sus equívocos. Su autoridad se debe enmarcar siempre en la legalidad vigente y en la garantía de la resolución de la emergencia.

Cuando al Jefe le arropan la autoridad como mando y la lealtad de sus subordinados, estaremos ante **un Líder,** que con su carisma y prestigio acortará los tiempos para la consecución de los objetivos. **El liderazgo en una emergencia es determinante.** Es el proceso de influir en las personas, proporcionando propósito, dirección y motivación para alcanzar los objetivos marcados y mitigar la emergencia en el menor tiempo posible.

El liderazgo es la capacidad de influir en las actividades de los demás a través de diferentes actividades para llegar a un objetivo común. No se debe confundir con la acción de Mando que incluye planificación, organización, dirección y control del personal y los recursos para alcanzar ese mismo fin común. Los líderes mandan personas, ejercen el control de la situación y coordinan los recursos a través de habilidades de liderazgo y gestión.

No vamos a caer en la tentación de analizar la eterna disyuntiva **"si los líderes nacen o se hacen".** Desde nuestro punto de vista en el modelo de gestión de emergencias **algunos aspectos del liderazgo deben ser inherentes a la persona y se acepta que la capacidad de liderazgo se puede desarrollar** o incrementar través de la educación y la formación. Si además se producen las circunstancias necesarias en un determinado contexto, la aparición de esta cualidad es posible.

A menudo se reconocen tres aspectos dentro del liderazgo: los fundamentos, las habilidades y las acciones que llevan a cabo los líderes.

FUNDAMENTOS DEL LIDERAZGO

La experiencia indica que se suelen repetir determinadas características en las personas que en una emergencia, o en otro contexto, llegan a alcanzar el calificativo de líder. Sin embargo también es cierto que estos fundamentos son sólo un comienzo. Tener estas cualidades no garantiza el éxito como líder, aunque sí que pueden servir para identificar **líderes potenciales**. Los atributos más deseados son:

1. Confianza en sí mismo
2. Valor
3. Empatía
4. Iniciativa
5. Integridad
6. Lealtad
7. Motivación
8. Autocrítica

HABILIDADES DEL LIDERAZGO

A los fundamentos del apartado anterior de los líderes potenciales, **les sumaremos habilidades a través de la formación y la educación** a fin de que alcancen:

1. Conocer su trabajo
2. Conocerse a sí mismos (auto-mejora)
3. Conocer a los miembros del equipo (habilidades interpersonales)
4. Saber escuchar y entender (habilidades de comunicación)
5. Saber lo que es correcto (ética)

ACCIONES DE LIDERAZGO

Poseer los fundamentos y conocer las habilidades necesarias todavía no es suficiente como para ser un líder eficaz. **Un líder debe actuar.** Las acciones deben ir encaminadas a:

1. Practicar el trabajo en equipo
2. Gestionar la tarea y los recursos
3. Aprender a asesorarse
4. Adaptar su estilo de liderazgo para adaptarse a la situación mediante la flexibilidad

Sin liderazgo el sistema de mando de la emergencia se resiente aunque las TIC funcionen y el enlace esté garantizado.

CAPÍTULO 13

PLANEAMIENTO DEL ENLACE EN EMERGENCIAS

Llegamos a este apartado con la sana intención de ayudar al lector a **planear el uso de "su sistema de enlace" en una operación de emergencia.** Vamos a repetir de nuevo la frase anterior por si no la hubiéramos leído con la suficiente atención. No es que no confiamos en el lector, que por supuesto lo hacemos (si ha llegado hasta aquí, sin duda es porque le interesa este asunto). Nos referimos al sistema de enlace de su agencia. Aquel que ha sido seleccionado por su organización para llevar a cabo el Mando y Control de la emergencia.

El Planeamiento es un proceso metódico diseñado para alcanzar un objetivo determinado. En nuestro caso la planificación **será un proceso de toma de decisiones sobre el empleo de nuestro sistema de telecomunicaciones e información para garantizar el enlace,** teniendo en cuenta todos los condicionantes como la situación actual, los factores internos o externos que pueden influir en el logro del objetivo.

Es decir estamos partiendo de una premisa: **ya tenemos un sistema** y unos procedimientos de uso que habremos diseñado correctamente si hemos seguido (más o menos) las instrucciones dadas en el capítulo 3 "*Soluciones a medida: diseño apropiado*".

El Planeamiento lo utilizaremos para adaptar el sistema de enlace de nuestra organización a las circunstancias precisas y exactas que tengamos que afrontar en una operación específica.

Veamos un ejemplo clarificador. En línea con el capítulo 3 supongamos que un Responsable TIC recibió de sus jefes un Concepto Operativo que utilizó para diseñar un sistema de enlace propio que facilitara el mando, control y coordinación de una organización sanitaria.

Tras haber trabajado concienzudamente en nuestras vistas operativas, de sistema y técnica, supongamos que en nuestro arquetipo el resultado del diseño del sistema de enlace de una recién creada organización sanitaria de una ciudad de 30.000 habitantes, es el que a continuación se relaciona:

- *Sistema de telefonía móvil, basado en una red privada virtual, suministrada por un operador de telecomunicaciones nacional que reserva un cierto número de canales en todo momento en las estaciones-base de telefonía móvil de nuestra ciudad.*
- *Todos nuestros médicos estarán dotados de terminales PDA o "Smart Phone" que aseguren su acceso a la red de datos permitiendo a su vez operar con el sistema llamado "SOCLAE" que hemos instalado en nuestro hospital y centros de salud, como herramienta de despacho (dispaching) de las intervenciones.*
- *Nuestros Enfermeros y Técnicos Sanitarios, estarán dotados con teléfonos con acceso únicamente a la red de voz. Por lo tanto no habrá instalaciones de telecomunicaciones vehiculares en nuestras ambulancias.*
- *Además hemos decidido preparar una furgoneta como Puesto de Mando Móvil, para atender las necesidades del pequeño hospital de campaña con el que se ha dotado el servicio. En la furgoneta hemos instalado un rack de comunicaciones, con capacidad de acceder al sistema "SOCLAE", ya que le hemos dotado de un router 3G y de un satélite Inmarsat BGAN, para asegurar el enlace en el caso de que la telefonía móvil se viniera abajo. La alimentación eléctrica la proporciona el mismo vehículo a través de su alternador y baterías.*
- *El enlace e integración con el 112 regional lo haremos mediante telefonía.*

Aunque es un ejemplo burdo y fuera de un contexto real, supondremos que hemos tenido en cuenta las famosas "**soluciones**" de los sistemas de enlace en emergencias (diversidad de medios, redundancia de vías y circuitos, particularización de los medios para determinados usuarios, y reducción de la dependencia de la infraestructura de telecomunicaciones terrestre).

Algún aventurado podría pensar que ya lo tiene todo y que ya no necesita planificar nada. Pongámoselo entonces un poco más complicado.

Hoy es 15 de abril y el alcalde de su ciudad ha decidido montar una romería en las afueras de su ciudad. El lugar elegido está a seis kilómetros, en un bonito lugar cerca del río y en las inmediaciones de un pequeño bosque de chopos. El día 15 de mayo, San Isidro, es la fecha prevista. La climatología no suele ser un problema en esta época, de hecho suele ser benigna, pero sí que existen antecedentes históricos de inundaciones alrededor de la ribera del río provocadas por tormentas puntuales.

Nosotros, como mujer u hombre TIC de nuestra organización, deberemos garantizar el enlace preparando el "dispositivo de transmisiones" que permita a su vez el trabajo del "dispositivo sanitario global" que nuestra organización vaya a establecer. Es decir, ***vamos a adaptar el sistema de enlace de nuestra organización sanitaria a las circunstancias específicas de la romería.***

Veamos cómo hacerlo.

CONSIDERACIONES BÁSICAS

La planificación es la gran herramienta para coordinar las actividades. Si no se coordina mediante el planeamiento, habrá de hacerlo por reacción ante los hechos, por lo tanto el Responsable TIC de la organización es una parte imprescindible de la misma, o debería serlo...

Ya hemos dicho con anterioridad que las comunicaciones son el sistema nervioso de la organización que participa en la emergencia. Es una **responsabilidad del jefe de la organización asegurar que el planeamiento de las operaciones a desarrollar tenga siempre en consideración los aspectos relativos al enlace,** otorgándoles la atención que su importancia exige.

Las transmisiones tienen que facilitar, y no impedir o limitar, la maniobra de los elementos participantes de nuestra organización. Éste es un punto que se repite recurrentemente en las organizaciones. En ocasiones el sistema de enlace establecido no sólo no facilita llevar a cabo la misión de los operativos sino que además dificulta otras tareas igualmente importantes.

JERARQUÍA EN EL PLANTEAMIENTO

Para que esto no ocurra el encargado del enlace tiene que **trabajar muy cerca y en perfecta sintonía con el elemento "planificador global"[92] de la organización.** Además, como veremos más tarde deberá formar parte del equipo asesor, dando su aportación técnica, a la solución global prevista.

El planificador TIC debe tener un **conocimiento exhaustivo** de la estructura de su **organización**, de los **miembros** que la componen, de los **procedimientos operativos** en general, y del **procedimiento operativo del uso del sistema de transmisiones** de la institución en particular. Se da por supuesto que debe ser el máximo conocedor de los medios propios TIC y de sus capacidades técnicas.

El planificador global por su parte debe tener un **conocimiento** lo más exacto posible **de los medios de enlace disponibles,** pero sobre todo de las **capacidades que esos medios le proporcionan**.

TIPOS DE PLANEAMIENTO Y SUS FASES

Existe una tendencia en los últimos años a utilizar el método de planeamiento táctico empleado por las Fuerzas Armadas en la planificación de operaciones de protección civil. Nosotros nos vamos a sumar a esta moda por las siguientes razones.

En primer lugar está contrastado sobradamente que es útil, sobre todo por lo sistemático que resulta. Con su aplicación es difícil que se nos escapen detalles y que dejemos campos importantes sin tratar. No deja de ser un "***checking list***" que una vez aprendido ayuda a realizar la preparación de las operaciones de manera automatizada.

Por lo tanto sin descartar otros métodos desarrollados *ex profeso* por las mismas organizaciones, u otros como el de "Incidente Único", nos inclinaremos por el llamado **planeamiento táctico militar,** aunque teniendo siempre presente las especificidades de las organizaciones del mundo de las emergencias.

92. En este punto conviene aclarar que nos referimos al planificador de más alto nivel que coordine e integre en el planeamiento global de la organización a los diferentes elementos que, a nivel inferior, exigen un planeamiento parcial más concreto y exhaustivo. Por ejemplo logística, intervención, transmisiones, etc.

Encontramos diferentes **tipos de planeamiento.** El tiempo y la cantidad de personas disponibles para realizar el planeamiento marcarán el detalle y profundidad de cada una de las fases. El planeamiento puede durar meses, o segundos. Lógicamente en los escalones más bajos, cuando no se dispone de tiempo o lo tiene que hacer una sola persona, a veces se reduce a un proceso mental. **Es el llamado planeamiento corto o expedito.**

En otras ocasiones como ocurrió en la ciudad de Madrid, los responsables emplearon más de un año en la definición del dispositivo que respaldó brillantemente las Jornadas Mundiales de la Juventud (JMJ) que tuvieron lugar en agosto de 2011 con motivo de la visita de su Santidad Benedicto XVI. En este caso se trató de un **planeamiento completo o formal.**

Por último haremos mención al llamado **planeamiento sobre la marcha**. Es el utilizado durante el transcurso de la emergencia para adaptar los planes y las órdenes previstas durante el planeamiento completo/formal o corto/expedito a la situación real.

El planeamiento táctico comprende las siguientes **etapas:**

- Análisis de la misión.
- Estudio de los factores de la situación.
- Consideración de las líneas de acción.
- Decisión y desarrollo de la misma.
- Preparación y distribución del Plan.
- Ejecución, Evaluación y Revisión del Plan.

ANÁLISIS DE LA MISIÓN

Oficialmente los **planeamientos parciales,** como el logístico o el TIC, comenzarán instantes después del **Planeamiento Global.** Éste **comienza formalmente con la recepción de una misión** si se trata de preparar con antelación un dispositivo para un evento concreto, **o en el mismo momento de recibir la alerta** si se acaba de producir la emergencia.

El Análisis de la Misión en el Planeamiento Global tendrá por objeto determinar el papel de la propia organización en el conjunto del dispositivo. **El Análisis de la Misión para el Responsable TIC** tiene por objeto ver como contribuirán los medios de transmisiones al cumplimento de la misión de nuestra organización.

Nuestro planeamiento del enlace se iniciará tan pronto como sea posible, en el marco del planeamiento general. El planeamiento del enlace es una herramienta sistemática que ayuda a tomar decisiones correctas y basadas en hechos e informaciones claras y objetivas. No debemos empeñarnos en obtener un documento a toda costa porque **no se trata de un fin en sí mismo.**

Con la recepción de la misión, **iniciaremos una serie de actividades que tendrán como fin la recopilación y actualización de datos,** para obtener una valoración adecuada de la situación. Esto lo haremos para los dos casos planteados, es decir, tanto si es para un dispositivo preventivo, como si es para una actuación inminente. La diferencia será el tiempo disponible, y por tanto estaremos pasando del planeamiento completo-formal a uno corto-expedito sin solución de continuidad.

Las actividades relacionadas con las TIC a desempeñar en este momento son las siguientes:

- Identificar claramente la **Autoridad de la Emergencia** (o del dispositivo) a la que debemos servir, que aunque normalmente será de nuestra organización, cuando se distribuyen unidades que pasan a trabajar para otra entidad, pudiera variar.
- Definir claramente la **misión para las TIC** que debemos cumplir de acuerdo con las instrucciones recibidas de la Autoridad de la Emergencia.
- Identificar completamente **nuestra cadena de mando**, desde el escalón más elevado hasta el último interviniente en los escalones más bajos, pues somos responsables de asegurar el enlace de todos ellos.
- Definir claramente los **órganos a enlazar ajenos a nuestra organización** en todos los niveles (actuantes, gestores de emergencia, etc.).
- Señalar e **identificar desviaciones posibles de nuestros procedimientos de enlace** preestablecidos.
- Identificar los **servicios TIC especiales.** Son aquellos no usuales que no están contemplados en nuestros procedimientos habituales de nuestra organización (videoconferencias, accesos a páginas web específicas, etc.).
- **Identificar las calidades** requeridas para esos servicios.
- Clarificar **responsabilidades de enlace** con respecto a otros organismos.
- Llevar a cabo y participar en cuantas **reuniones** sean necesarias realizar para obtener y clarificar todas las necesidades de enlace en la zona de la emergencia.

En nuestro ejemplo este apartado de Análisis de la Misión *se podría resolver como a continuación se señala. El lector debe ser consciente de que es solo una aproximación que para nada pretende ser exhaustiva.*

La "misión asignada a nuestra organización sanitaria" sería algo similar a "implantar el dispositivo sanitario de la romería de San Isidro que tendrá lugar el próximo día 15 de mayo, integrando dicho dispositivo en el despliegue global que dirigirá el concejal de festejos".

La "misión para nosotros como responsable del enlace" será algo así como "establecer, mantener y explotar el sistema de transmisiones de nuestra organización sanitaria durante el día 15 de mayo, apoyando la dirección y ejecución de las actuaciones sanitarias y adaptando su despliegue, si fuera necesario, a la evolución de las mismas".

La "autoridad de la emergencia", será el concejal de festejos, y por tanto deberemos asegurar el enlace de nuestro jefe de organización sanitaria con él. Es decir será la parte más elevada de la cadena de mando, pero ahora nos tocará identificar el resto de eslabones, colaterales y subordinados. Supongamos que en nuestro caso los colaterales serán la policía municipal, el parque de bomberos de la ciudad, la empresa pública de limpiezas, y por descontado el 112 de la comunidad autónoma. Como elementos subordinados tendremos el hospital, los centros de salud, todas las ambulancias propias de soporte vital básico, dos soporte vital avanzados que nos ha prestado la capital de la provincia, y el hospital de campaña junto a su Puesto de Mando Móvil.

Como "desviación de nuestro procedimiento" detectamos que los soportes vitales avanzados que nos vienen agregados no disponen de nuestro sistema de PDAs, por lo que deberemos estudiar cómo integrarles en el despliegue.

En relación con "los servicios TIC especiales" hemos visto que el concejal ha anunciado que la mañana de la romería querrá hacer una videoconferencia con los responsables de los servicios sanitarios, extinción de incendios, policía y servicio de limpieza. Esto nos implica decidir qué medio tendremos que utilizar, dependiendo de la ubicación que elija nuestro jefe de servicio. Es importante definir la calidad de imagen que el concejal va exigir en la videoconferencia, pues los medios a emplear y los requisitos de ancho de banda son radicalmente distintos.

Por último hemos conseguido que nuestro jefe solicite una "reunión de coordinación" en el ayuntamiento específica de telecomunicaciones, donde deberían acudir todos los Responsables TIC de los servicios con los que podríamos tener necesidad de enlazar en caso de necesidad y aclarar las responsabilidades del enlace de cada uno.

ESTUDIO DE LOS FACTORES DE LA SITUACIÓN

Cuando hablamos de estudiar los factores nos estamos refiriendo a conocer el contexto, el terreno, los medios y el tiempo disponibles. En resumen, aunque en el Planeamiento Global se realizará de un modo genérico, aquí desde el punto de vista del enlace lo que se trata es de repasar todos aquellos aspectos que de algún modo pudieran influenciar en nuestro trabajo.

CONTEXTO

Se trata de ver cuál es el ambiente en el que se van a desarrollar las actuaciones. Si es de día o de noche, la meteorología, si con mucha o poca gente, si habrá alcohol o si la seguridad ciudadana estará garantizada.

Es también muy importante detectar los apoyos que podamos requerir o prestar a otras organizaciones, que puedan implicar enlaces adicionales que tendremos que considerar. No podemos olvidar que en ocasiones agregaremos unidades nuestras a otras organizaciones o que podemos recibir refuerzos de otras organizaciones.

Igualmente útil resulta mirar el histórico de actuaciones con motivo del mismo acontecimiento u otro que se haya dado en esa zona. Y por supuesto repasar los planes de emergencia territoriales y municipales, estudiando cómo inciden en el evento.

TERRENO

Tendremos que realizar un estudio de la zona de terreno en donde se van a llevar a cabo las actuaciones. Orografía en general, vías de comunicación, cruces conflictivos, infraestructuras que podamos utilizar existentes, zonas de difícil acceso, etc.

MEDIOS

Partiremos por descontado del sistema de enlace propio de la organización. Sin embargo deberemos ver la posibilidad de contar con sistemas adicionales, que podemos alquilar, pedir prestados, o simplemente nos pueden venir agregados con alguna otra organización.

Deberemos hacer un estudio previo racionalizando los medios disponibles en cuanto a

las necesidades requeridas. Es imprescindible conocer todas las posibilidades y opciones de los mismos. Habrá que priorizarlos, balanceando sus características y circunstancias.

En las situaciones de emergencia ya hemos visto que suele ser uno de los elementos más dificultosos e importantes. En caso de participación de múltiples servicios tendremos normalmente medios heterogéneos y deberemos prever problemas de interoperabilidad. Si viene personal de otras organizaciones que se integran en la nuestra deberá explotar nuestro sistema y normalmente no conocerá ni el uso ni los procedimientos de empleo.

Cuando los medios no pertenezcan directamente a nuestra organización deberemos prever las comprobaciones pertinentes para asegurarse su funcionamiento y operatividad.

Los aspectos logísticos no son asunto sencillo. Habrá que realizar un estudio del material de repuesto y de posibles almacenes de medios de respaldo. Tampoco olvidaremos las formas de distribución a los diferentes escalones.

Tendremos prevista y habilitada una vía de reposición y reparación de materiales, organizando la cadena de mantenimiento de equipos y su sustitución considerando las adversas condiciones que puedan darse.

Por último hablaremos de la reserva. Siempre debemos guardarnos ese as en la manga. En forma de equipos, de servicios o de canales. Nos sacarán de situaciones comprometidas cuando la realidad se separe de lo planeado.

TIEMPO

Hay que estudiar el marco temporal en el que es previsible la actuación del servicio de comunicaciones a desplegar. Habrá servicios que se despliegen y estén operativos en cuestión de minutos, pero otros pueden requerirnos semanas.

Volvamos a nuestro ejemplo, y hagamos el análisis de la situación (ficticio).

CONTEXTO

La romería es tradicional y se desarrolla anualmente desde los años 60. La previsión meteorológica a un mes vista es de buen tiempo. Suele empezar la noche antes, cuando la gente se va a dormir para coger los mejores sitios. Dura hasta que anochece, momento en el que la gente se retira a sus casas. Suele haber excesos por comida y bebida, y la acumulación de personas origina riñas y peleas ocasionales.

Vamos a contar con dos UCIs móviles de la capital de provincia. Los planes de emergencia municipales definen a la zona de la romería como inundable para precipitaciones superiores a 30 litros de agua por metro cuadrado en menos de una hora. La última inundación coincidiendo con la romería se produjo en 1975.

TERRENO

La zona es llana y presenta una loma al sur de la zona, el Cerro La Horca, que domina el despliegue. Existe una carretera asfaltada en buenas condiciones y dos caminos de tierra paralelos a la carretera principal que llevan a la chopera desde la ciudad. Existe una casa, propiedad del ayuntamiento, con luz y agua que tradicionalmente se utiliza como zona de despliegue de los equipos municipales.

MEDIOS

Los planos de cobertura de telefonía móvil entregados por la operadora de telecomunicaciones nacional al ayuntamiento cuando se adquirió el dispositivo de PDA,s indican que la zona de la romería no tiene cobertura en datos (hablando de telefonía móvil). Sólo tiene capacidad de voz y los canales son muy limitados, sólo cuatro simultáneos. Esto es un gran hándicap.

El enlace con bomberos, policía municipal y servicio de limpieza lo haremos en el modo habitual, a través de telefonía móvil, ya que estos números están memorizados en todos los terminales de nuestro servicio.

El responsable TIC llevará dos PDA's y dos teléfonos móviles de repuesto y reserva para atender averías o necesidades sobrevenidas.

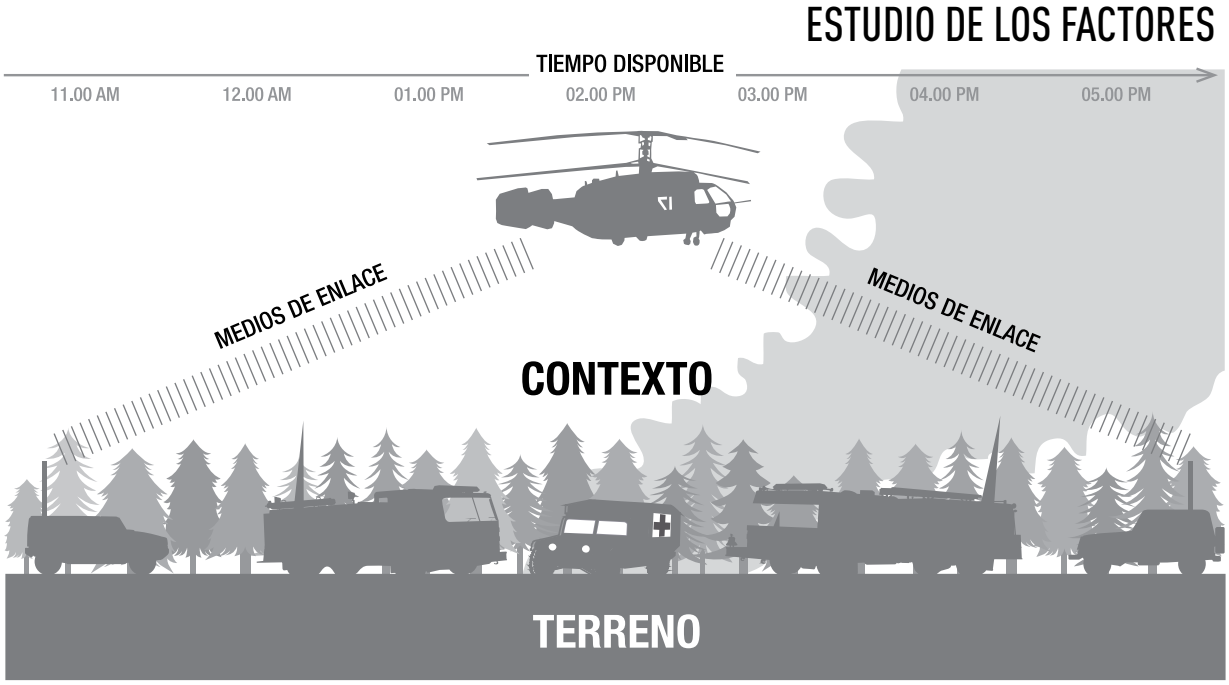
TIEMPO

Contamos con un mes, pero la solución que se adopte deberá estar operativa con una semana de antelación para poder hacer las pruebas de enlace pertinentes antes del evento.

POSIBLES LÍNEAS DE ACCIÓN

El estudio de líneas de acción no es otra cosa que **ver diferentes opciones de resolver un mismo problema.** Si formalmente podemos encontrar más de un modo de garantizar el enlace, lo que haremos será estudiar detalladamente las ventajas e inconvenientes de cada una de las posibles soluciones. Se lo explicaremos a nuestro jefe y le propondremos una de las soluciones como la más completa desde el punto de vista del Responsable TIC, es decir desde nuestro punto de vista.

En el dechado que arrastramos hemos visto que el sistema de nuestra organización sanitaria no funciona en la zona de la romería en modo datos, lo que



supone perder prácticamente la operatividad de la organización.

Vemos dos posibles opciones.

OPCIÓN 1: Vemos que el sistema habitual no puede ser utilizado si no realizamos algunas operaciones adicionales. En este caso podemos solicitar a la operadora de telefonía que despliegue dos estaciones base de telefonía móviles adicionales en la zona. Solicitaremos capacidad 3G para poder hacer uso de los datos por parte de nuestros facultativos y que aumente la capacidad de fonía a veinte conversaciones simultáneas.

OPCIÓN 2: Podemos pedir terminales radio a la policía local que sabemos positivamente funcionan en la zona, y distribuirlos entre nuestros operarios y facultativos.

La ventaja de la opción dos sobre la uno, es la economía. Sin dudas es una opción más barata, porque el despliegue de estaciones base adicionales habrá que pagarlo, o al menos negociarlo con la empresa de telefonía. Aun así propondremos a nuestro jefe la opción 1, ya que es el modo habitual de trabajo de nuestra organización, el que se adapta a nuestros procedimientos y como se asegura la mejor atención al paciente en caso de que algo ocurra.

DECISIÓN Y DESARROLLO DE LA MISMA

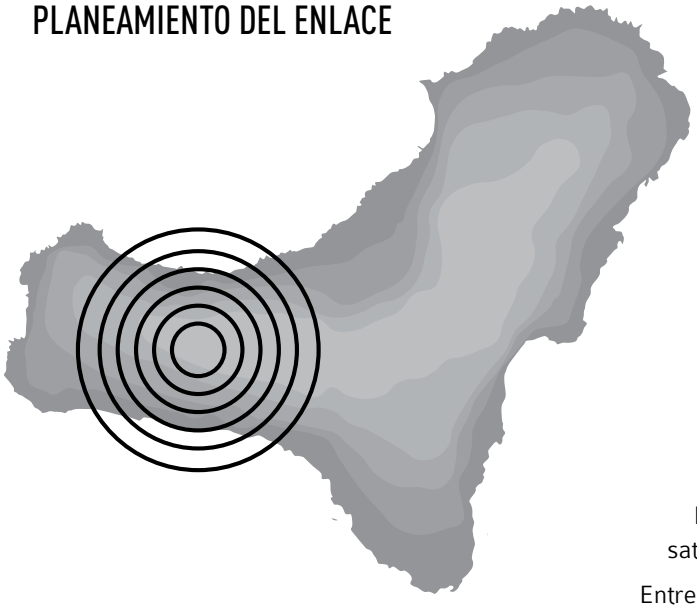
Es la última etapa. Es aquí **cuando el jefe decide globalmente lo que quiere hacer, y además elige la opción TIC que considera más conveniente para apoyar su trabajo.** Ahora nos queda materializar la decisión del jefe en una serie de acciones a desarrollar para concretar que todo se realiza tal y como el Jefe ha decidido.

PREPARACIÓN Y DISTRIBUCIÓN DEL PLAN

Lo habitual será redactar un documento que recoja el **plan global u orden de operaciones**[93], al que nosotros como Responsables

93. La diferencia entre un plan y una orden de operaciones es que en el plan no se incluye un calendario de ejecución de las acciones que se contemplan en el plan. Todo el resto es igual.

PLANEAMIENTO DEL ENLACE



TIC contribuiremos con las ideas más importantes. Es muy **conveniente redactar un anexo específico de transmisiones** al plan global u orden de operaciones de cada operación. En este documento se resumen las actuaciones TIC a realizar, y se pormenorizan aquellas acciones que se salen de lo "normal". También es muy importante difundir este documento entre todos los participantes, pero sobre todo entre los responsables TIC de cada escalón.

Suele ser un elemento muy útil porque resume los órganos a enlazar, los medios a emplear y las instrucciones de coordinación que hay que llevar a cabo para obtener un resultado satisfactorio.

Entre otros muchos temas este "**anexo de transmisiones**" documento puede contener los siguientes temas:

- Redacción de la misión exacta de las TIC para cada fase de la emergencia.
- Agregación y segregación de medios y personal TIC.
- Definir los despliegues de los medios en el lugar y tiempo requerido.
- Analizar las vías y circuitos de telecomunicaciones, así como los medios disponibles para ese despliegue.
- Cometidos específicos TIC a las unidades subordinadas y colaterales.
- Punto de contacto con los diferentes actores TIC que intervienen en la acción.
- Matriz de servicios TIC, esquemas de cada órgano a enlazar con indicación de los medios asignados.
- Arquitectura de las diferentes redes a establecer.
- Apoyos a recibir en la zona como corriente eléctrica, alimentación para nuestro personal, repostaje de vehículos, etc.
- Puntos logísticos propios. Prioridades en la prestación de servicios TIC, regímenes de empleo y prescripciones particulares para la utilización de determinados medios, etc. Medidas particulares para la gestión del espectro electromagnético.
- Apoyo a la gestión de la información y del conocimiento.
- Conseguir los permisos de instalación de los diferentes medios o centros de comunicaciones coordinándolo con las autoridades o propietarios.
- Medios en Reserva y su ubicación en el despliegue.

Una vez adoptadas las medidas, redactado y distribuido el Plan u Orden de Operaciones sólo resta reunir a los participantes, clarificar dudas y ensayar el despliegue. Este **ensayo puede ser global o específico de transmisiones.** Los mejores resultados se obtienen cuando los usuarios reales de los medios TIC hacen uso de ellos, aunque muchas veces es difícil que se realicen por restricciones económicas o por carga de trabajo.

CRISIS VOLCÁNICA DE EL HIERRO

Con motivo de la crisis volcánica en la isla de El Hierro del año 2011, en el archipiélago canario, se pusieron en marcha diversos planes de contingencia para asegurar el funcionamiento de las TIC:

- Activación de un interlocutor de Telefónica en el CECOES Tenerife y en el CECOI de El Hierro.
- Instalando sistemas de transporte de señal vía radio con rutas alternativas por La Palma y La Gomera en caso de corte del cable submarino El Hierro-La Gomera .
- Aseguramiento suministro eléctrico mediante grupos electrógenos transportables y baterías.
- Aumento de la capacidad de comunicación de la telefonía.
- Incremento de las dotaciones de repuestos de todas las tecnologías.
- Traslado a la isla de elementos de comunicaciones de emergencia: Unidad transportable de Móviles para 140/280 comunicaciones simultáneas en 2G y 3G vía satélite o radio respectivamente, 2 Radioenlaces transportables, 9 unidades INMARSAT, 6 Unidades IPSAT, y 2 Unidades Minilink.

Si no se hace el global debemos tratar por todos los medios de hacer el nuestro en el que podamos comprobar los medios de transmisiones y el correcto funcionamiento de los servicios.

En nuestro ejemplo, el jefe se decide por la opción de los repetidores adicionales de telefonía móvil. Nos reuniremos con la empresa, decidiremos el lugar y fechas del despliegue de las estaciones base. Probaremos todo la semana antes.

Además solicitaremos un grupo electrógeno remolcado al servicio de limpieza del ayuntamiento y le pediremos que lo despliegue en la casa de la zona de la romería, en previsión de posibles cortes de luz.

La videoconferencia que quiere hacer el concejal con nuestro jefe de servicio, la haremos desde el mismo hospital de campaña, ya que hemos probado el enlace con el satélite BGAN del Puesto de Mando Móvil y funciona bien (la calidad de la imagen es aceptable). Además cuando estén los repetidores de telefonía móvil adicionales tendremos la opción de tener una solución de respaldo o back up, gracias a la telefonía móvil 3G.

EJECUCIÓN, EVALUACIÓN Y REVISIÓN DEL PLAN

A partir de este instante sólo nos queda estar atentos y adaptarnos a las circunstancias, porque el lector debe ser consciente que **el planeamiento no garantiza el buen resultado.** Una vez que se inicie el simulacro o se desencadene la emergencia real tendremos que adaptar nuestro Plan a la realidad. Por desgracia el dicho de "que no hay planeamiento que dure más de cinco minutos, después de que se desencadene la emergencia", suele ser una realidad. Sin embargo sí que **el haber planeado nos ayudará a conocer las circunstancias y facilitará la rápida respuesta para contrarrestar los hechos acaecidos.**

Finalmente evaluaremos el desarrollo del planeamiento, sacaremos **lecciones aprendidas** y aplicaremos las enseñanzas obtenidas en planes y emergencias futuras.


FIRE

CAPÍTULO 14

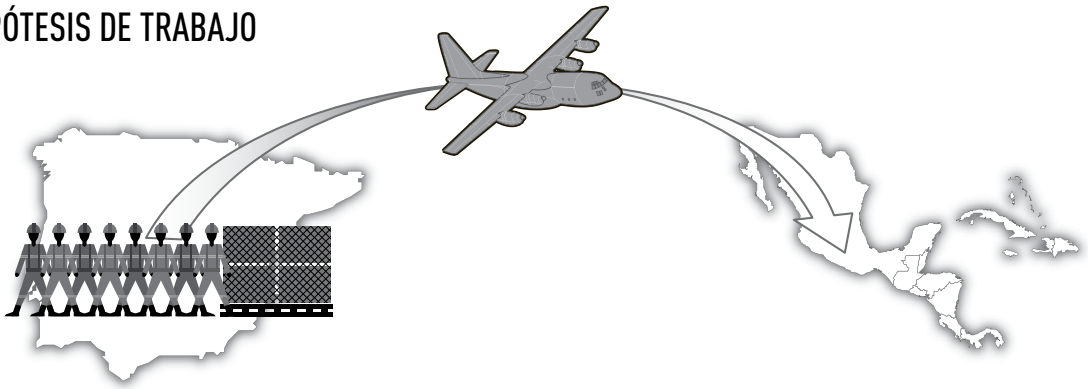
MISIÓN: GARANTIZAR EL ENLACE EN UNA OPERACIÓN EXTERIOR

Al igual que las ONG, las organizaciones de emergencias nacionales de muchos países realizan operaciones de socorro en el extranjero. Ejemplo de ello son las unidades francesas **UIISC** (*Unité d'Instruction et d'Intervention de la Sécurité Civile*), la **THW** (*Technisches Hilfswerk*) de Alemania, la **DEMA** (*Danish Emergency Management Agency*) de Dinamarca, o la **SRSA** sueca (Agencias de Servicios de Rescate). A menudo, prestan servicio de asistencia en el marco de acuerdos bilaterales concertados con el país beneficiario, como miembros de Naciones Unidas o el marco del Mecanismo de Protección Civil de la Unión Europea.

Los organismos nacionales que prestan asistencia internacional suelen contar con sistemas de enlace para sus propias necesidades y en ocasiones ayudan también a otras organizaciones, ONG y los servicios locales.

En este capítulo vamos a intentar hacer un **guía burros,** de los diferentes preparativos que tendremos que realizar como Responsables TIC, suponiendo que nos tenemos que preparar para salir en misión más allá de nuestras fronteras. Como lo más complejo desde nuestro punto de vista de las transmisiones sería un despliegue lejos de nuestra Base o de nuestro

HIPÓTESIS DE TRABAJO



- Nos prepararemos para afrontar una misión internacional
- Centroamérica
- Partiremos de un sistema de enlace propio adquirido por nuestra agencia, y mediante un detallado proceso de planeamiento adaptaremos su uso a la especificidad de la misión
- Equipo de entre 8 y 12 personas
- Situación muy desfavorable: sistemas de telecomunicación del país fuera de servicio

Centro de Coordinación habitual de pertenencia, supongamos que vamos a ser proyectados al exterior, es decir **nos prepararemos para afrontar una misión internacional.**

Tal y como hemos señalado en el capítulo anterior, lo normal es que como componentes de una organización **partiremos de un sistema de enlace propio** adquirido por nuestra agencia, que mediante un detallado **proceso de planeamiento** adaptaremos su uso a las especificidades de la misión.

Para no repetirnos supondremos que ya **hemos completado todas las fases del planeamiento formal** ((análisis de la misión, estudio de los factores, desarrollo de líneas de acción posibles, decisión y preparación del plan u orden de operaciones). En nuestro caso vamos a suponer el despliegue de un equipo de entre 8 y 12 personas.

Evidentemente, en un despliegue internacional no se puede llevar una cantidad ingente de medios, por lo que resulta imperativo **seleccionar un mínimo de sistemas que permitan cumplimentar la misión.** Es imprescindible hacer un estudio sin partir de supuestos "demasiado ventajosos". Es decir, imaginaremos una situación desfavorable en las que los sistemas de telecomunicación del país de destino están inservibles y fuera de uso debido a los daños causados por la catástrofe. Si luego resulta que cuando lleguemos no es tan mala la situación desde la perspectiva del enlace, pues tanto mejor; podremos replantearnos el uso de determinados medios, sobre todo de los que cuestan más dinero.

NECESIDADES DE ENLACE A CUBRIR

- De la "base de operaciones" desplegada en la zona con nuestra "base retrasada o homo base" en territorio nacional
- Enlace entre los miembros de la expedición dentro de la zona de operaciones
- Facilitar enlace con otros grupos operativos en la zona de emergencia
- Condiciones óptimas de trabajo en la base de operaciones, incluyendo electricidad e iluminación
- Dotaciones mínimas de material que permitan trabajar de forma ininterrumpida
- Prever un mínimo de sistemas redundantes por si se producen averías de material
- Contar con una reserva de medios

Diseñar nuestro sistema de "enlace" significará elegir y descartar medios. Deberemos analizar ventajas e inconvenientes de cada uno de los procedimientos de enlace que queramos, o podamos, implementar.

Supongamos que tras el análisis de la misión decidimos que nuestro diseño final deberá cubrir las siguientes necesidades según cuadro adjunto:

- Posibilitar la comunicación de la "Base de Operaciones" desplegada en la zona con nuestra "Base Retrasada o Home Base" en Territorio Nacional.
- Asegurar el enlace entre los miembros de la expedición en la propia zona de operaciones.
- Facilitar la comunicación con otros grupos operativos que puedan intervenir en la zona de la emergencia.
- Garantizar unas buenas condiciones de trabajo dentro de la "Base de Operaciones", incluyendo alimentación eléctrica de los equipos e iluminación.
- Contar con unas dotaciones mínimas de material que permitan trabajar de forma ininterrumpida.
- Prever un mínimo de sistemas redundantes por si se producen averías en el material.
- Contar con una reserva de medios.

ENLACE CON TERRITORIO NACIONAL

Este enlace cubrirá dos necesidades muy importantes. Por un lado la de establecer el **flujo de información con la organización** que nos ha destacado, y por otro lado el de mantener alta la moral del personal desplegado (***Moral, Welfare and Recreation***) manteniendo el enlace con sus familias.

Lo tradicional hasta la explosión de Internet y de los medios satélite portátiles hubiera sido recurrir a los enlaces **radio HF a larga distancia.** Hoy día resulta más ágil y sencillo recurrir a una solución basada en un **sistema de enlace satélite comercial.**

Como ya sabemos existen varias opciones. El sistema satélite más común y extendido es sin duda el INMARSAT, con sus diferentes modelos y capacidades. Existen otros operadores como GlobalStar, Thuraya o IRIDIUM que pueden también cubrir nuestras necesidades. Deberemos tener la certeza de que el sistema adquirido tiene cobertura en la zona destino. Esto se suele ver en las páginas web de los diferentes operadores, donde se exponen las huellas satelitales en diferentes partes del mundo. ¡Ojo! Son empresas que buscan obtener beneficio... y en ocasiones **sus planos de cobertura son demasiados "optimistas".** Esto se debe traducir en precaución a la hora de aceptar como buena la información de cobertura en determinadas zonas del globo, sobre todo aquellas que están en los extremos de la huella.

Estos terminales satélites guardan una **buena relación entre servicio ofertado, precio de adquisición y facilidad de operación.** Además casi todos son ya duales con la telefonía móvil, permitiéndonos la **transmisión y recepción tanto de voz como de datos.**

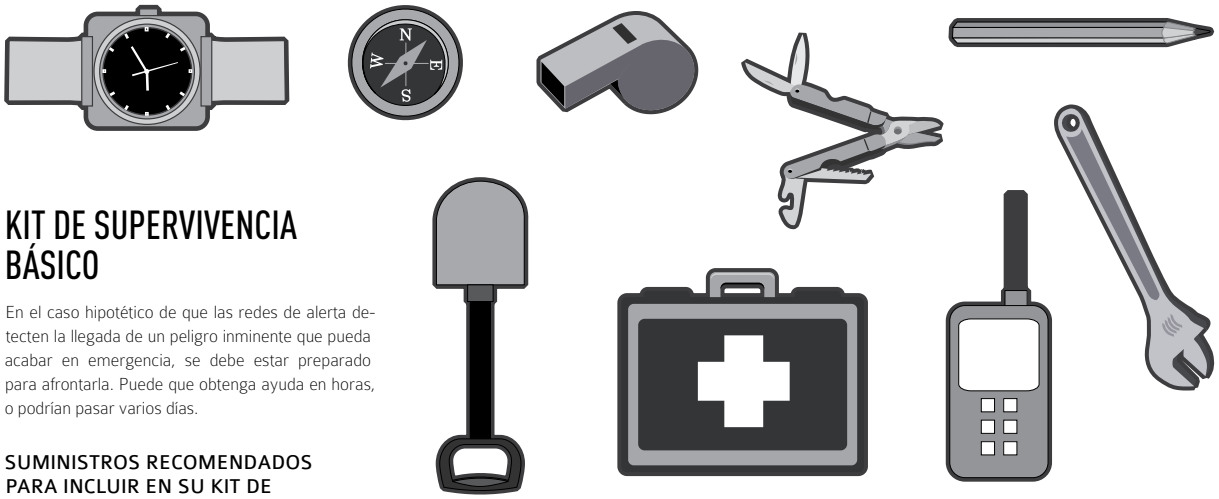
Si el presupuesto lo permite llevaremos **más de un terminal satélite,** que nos servirá como reserva o para cubrir picos de esfuerzo que se puedan dar en algunos momentos de la misión. Por ejemplo cuando tengamos que desdoblar en algún momento nuestra Base de Operaciones o para asegurar el enlace con nuestro personal si no hay telefonía móvil en la zona.

Existen **otras soluciones satélite** más completas, pero menos conocidas. Dependiendo de la zona del mundo donde vayamos a desplegar se puede hacer un estudio de satélites que dispongan de canales a disposición de usuarios temporales. Suele tratarse de satélites de empresas de telecomunicaciones, satélites militares, o incluso de cadenas de televisión que ponen en alquiler determinados servicios.

La solución pasa por desplegar terminales **satélites semiestáticos**[94]. Se suele componer de una antena con amplificador (adaptada a la banda de trabajo), un módem y un equipamiento de banda base. Se requiere alquilar una portadora con un ancho de banda reservado en un satélite con cobertura en la zona de la emergencia. Un ejemplo típico de empresa suministrada de este tipo de servicios es el proporcionado por los satélites de la constelación de EUTELSAT o los VSAT.

Tanto el terminal como la tarificación son mucho más caros que para los terminales inicialmente expuestos. Suelen dar altos rendimientos al contar **anchos de banda reservados** para el usuario y no entrar en competencia con nadie más. Un claro ejemplo que ratifica la problemática de competencia entre usuarios para adquirir un mismo servicio se dio en el terremoto de Haití del año 2010. La gran cantidad de equipos de diferentes países

94. Los terminales satélite semiestáticos, se diferencian de los portátiles en que no son transportables por una sola persona, como lo puede ser un teléfono móvil. Tampoco son terminales fijos, que están completamente anclados al terreno constituyendo las denominadas estaciones de anclaje satélite. Podemos afirmar que son una solución intermedia, más cercana al terminal fijo, por volumen y capacidad de servicios que al terminal portátil. Se pueden transportar normalmente en cajas o cofres diseñados *ad hoc*.



KIT DE SUPERVIVENCIA BÁSICO

En el caso hipotético de que las redes de alerta detecten la llegada de un peligro inminente que pueda acabar en emergencia, se debe estar preparado para afrontarla. Puede que obtenga ayuda en horas, o podrían pasar varios días.

SUMINISTROS RECOMENDADOS PARA INCLUIR EN SU KIT DE SUPERVIVENCIA BÁSICO

- Agua, un litro de agua por persona al día, para al menos tres jornadas.
- Comida, provisiones por lo menos para tres días de alimentos no perecederos.
- Linterna y baterías de repuesto.
- Botiquín de primeros auxilios y medicamentos indispensables.
- Silbato o bengalas para alertar y pedir ayuda.
- Toallitas húmedas y bolsas de basura.
- Navaja multiuso o alicates tipo leatherman.
- Llave inglesa y bridas de diferentes tamaños.
- Abrelatas para la comida (si el equipo contiene alimentos enlatados)
- Mapas locales.
- GPS.
- Teléfono móvil con cargador y/o baterías auxiliares.
- Documentación importante. DNI, pasaportes, pólizas de seguros...
- Dinero en efectivo.
- Saco de dormir
- Bolsa de ropa estanquizada.
- Prenda de abrigo.
- Pastillas depuradoras de agua.
- Fósforos en un recipiente a prueba de agua.
- Artículos femeninos y para la higiene personal.
- Juegos de utensilios desechables tipo *camping*, vasos desechables, platos de cartón y cubiertos de plástico, toallas de papel.
- Papel y lápiz.
- Rollo de alambre, cuerda y cinta aislante.

desplegados en la zona, que usaban el mismo tipo de sistemas (en aquel caso, terminales BGAN Inmarsat), hizo al sistema Inmarsat en aquella zona del globo bastante inestable, debido a la saturación. Cientos de equipos tratando de acceder al mismo satélite de forma simultánea, hizo constatar un vez más que la saturación y poca fiabilidad de los medios de comunicaciones son hechos constatados en las primeras fases de la emergencia.

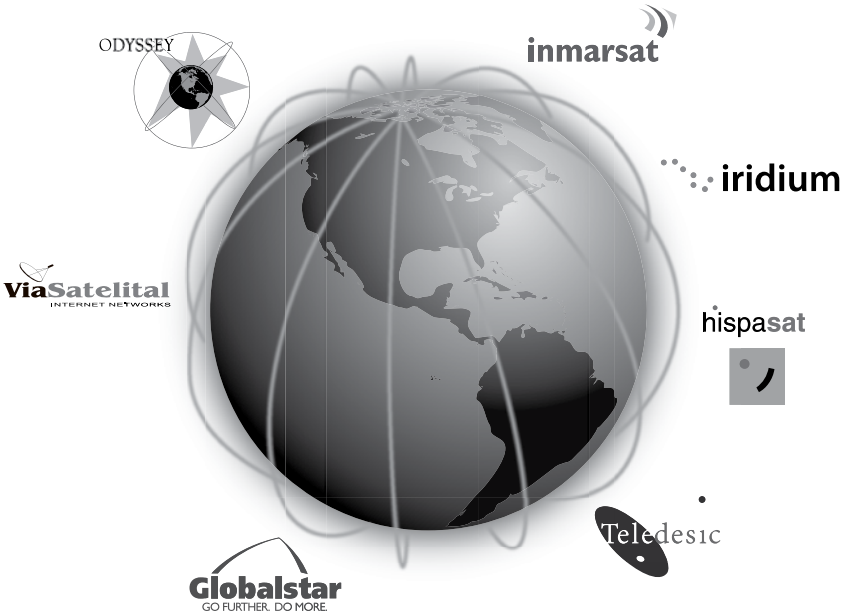
Esta solución suele emplearse para misiones de larga duración, pero sobre todo cuando se requieren servicios demandantes de mucho ancho de banda (videoconferencia, acceso a internet, etc.). En estos satélites se obtiene un **enlace en fonía** (voz) que permitirá evidentemente comunicaciones telefónicas y de fax con cualquier parte del mundo. Y **enlace de datos** garantizando la conexión a Internet, con lo que nos permitiría el acceso a servicios básicos como es el correo electrónico, acceso a páginas web, videoconferencia IP o aplicaciones on-line (por ejemplo de GIS o cartografía en general).

Igualmente nos permitiría, en caso de que alguna otra organización disponga de un material satélite igual o compatible con el nuestro, hacer **enlaces de datos punto a punto** para hacer otro tipo de uso, como podría ser el de videoconferencia punto a punto, compartición de bases de datos, etc.

En este apartado de enlace con Territorio Nacional deberemos tener siempre presente la posibilidad de **contratar telefonía fija local o adquirir telefonía móvil autóctona de la zona de despliegue,** si se comprueba su fiabilidad, teniendo presente los momentos y las misiones cuando se podrían utilizar.

Aunque ya hemos mencionado la complejidad de uso de los **enlaces HF**, no debemos obviarlo, y si tenemos espacio suficiente para transportar radios de HF en los aviones designados para el transporte, meteremos al menos una emisora, y un grupo de diferentes antenas. Utilizaremos este sistema como respaldo (*back up*) para garantizar el enlace en caso de fallo o avería del sistema satélite principal que hemos propuesto. Las antenas que llevaremos serán como mínimo una de varilla y un dipolo de banda ancha, con los soportes necesarios para su elevación. La primera nos permitirá usar el HF para enlazar con zonas cercanas a la ubicación del equipo, mientras que el dipolo

CONSTELACIONES DE SATÉLITES COMERCIALES



de banda ancha nos permitirá cambiar de frecuencia de trabajo sin que tengamos que estar reduciendo o ampliando la longitud de los brazos. Este tipo de enlace nos permitiría enlace voz y una capacidad muy reducida de transmisión de datos.

COMUNICACIÓN ENTRE MIEMBROS DEL EQUIPO

Aunque lo ideal es reducir el número de equipos y que el mismo sistema elegido nos sirva para mantener el enlace con Territorio Nacional, con otros organismos colaterales desplegados en la zona, y con los propios miembros de nuestro equipo cuando salen de la Base de Operaciones, la verdad es que no siempre lo conseguiremos.

En el estudio de los factores habremos abordado la orografía de la zona por la que nos vamos a mover y que sin duda va a condicionar nuestra misión. No tiene nada que ver enlazar en una llanura, en una zona montañosa, en un bosque o en el centro de una ciudad. A estas alturas del libro éste es un concepto que seguro ya tenemos claro.

Al **terreno** habrá que unir otros factores, como es por ejemplo el estado de la infraestructura de telecomunicaciones en la zona donde vamos a desplegar. Idea también ya consolidada o al menos eso esperamos.

La primera elección se basaría en **elegir entre teléfono, terminal satélite portátil y radio.** No teman. No vamos a repetir todas las ventajas e inconvenientes de cada uno de estos medios de transmisiones. Solo unos breves apuntes.

TELÉFONO

El caso es que el **uso del teléfono perteneciente** a las antiguamente denominadas operadoras públicas PTT (Portes, Telégraphes, Téléphones), no acarrea ninguna trascendencia desde el punto de vista del Responsable TIC. Funcionará o no, pero estaremos en mano de las operadoras de telefonía fija y móvil de la zona.

SATÉLITE

La alternativa al teléfono PTT es recurrir a los **terminales portátiles satélite** tipo IRIDIUM o Global STAR, que pueden ser incluso los mismos que hemos señalado en el apartado anterior.

Una vez confirmada con los planos la cobertura de estos satélites deberemos decidir si apostar por **instalaciones vehiculares** o limitarnos a satélites **manpack o portátiles.** Estos terminales no son muy caros, aunque sí y mucho el tráfico que generan. Por tanto se planteará un punto de decisión entre decantarnos por una de las tres opciones, y sin duda a la hora de elegir se verá condicionado por el presupuesto y por el periodo de permanencia en la zona. Si el periodo es de más de seis meses empiezas a ganar valor la radio y la telefonía autóctona. Si es inferior es preferible el satélite.

El **número de terminales** satélite deberá ser el suficiente para cubrir las misiones de los componentes del equipo que salgan de la base de operaciones de manera simultánea quedándonos con al menos uno de reserva. De esta manera garantizaremos el movimiento de nuestros equipos por la zona pudiendo siempre dejar una capacidad residual mínima en la Base de Operaciones para garantizar el enlace en situaciones sobrevenidas.

La **ubicación** de los terminales satélite variará con el propósito del mismo. Los dedicados a la Base de Operaciones y emplazamientos fijos se instalarán normalmente en la zona de trabajo. Los equipos irán montados sobre vehículos y tendremos que tener en cuenta si tienen capacidad de enlace en movimiento SOTM (*sat on the move*) o si son estáticos, lo que nos obligaría a parar el vehículo, y a apuntar la antena antes de operarlos. Los terminales manpack, son muy ligeros y muy similares a los teléfonos móviles.

RADIO

Cosa muy distinta es si hemos apostado por usar **enlace radio** para hablar con nuestros compañeros de grupo cuando están fuera o lejos de la Base de Operaciones o Puesto de Mando. Debemos contemplar tres opciones:

- OPCIÓN 1:
  Radios VHF/UHF. Aunque se precisaría un **reconocimiento radioeléctrico**[95] previo para confirmar las zonas de sombra con respecto a los sistemas que vayamos a utilizar, a priori y teniendo en cuenta que las comunicaciones radio VHF y UHF exigen prácticamente línea de visión directa, para cubrir una zona de acción extensa (estamos hablando de distancias superior a tres kilómetros aproximadamente) debemos tener prevista la ubicación de **repetidores**. Estos regeneradores de señal se podrán ubicar en distintos emplazamientos, todos ellos elevados, y podrán ser atendidos o no.

  Un repetidor atendido es aquel que dispone de personal para operarlo y que además cuenta con electricidad para recargar las baterías o alimentar las fuentes de alimentación. Son difíciles de encontrar porque tampoco estaremos en condiciones de repartir nuestro personal. Se suele intentar que organizaciones o instituciones con las que colaboremos nos permitan ubicar estos equipos en sus asentamientos.

  Para la solución basada en repetidores inatendidos (sin personal) lo ideal es que al menos cuente con alimentación eléctrica. Si no es así suponen una carga logística importante ya que obliga a ir prácticamente a diario a cambiar las baterías que alimentan los equipos.

  La mayor ventaja de este tipo de radios es que las instalaciones radio vehiculares y los terminales portátiles son simples y ligeros, muy sencillos de usar y el tráfico no genera ningún gasto adicional. El inconveniente es el corto alcance y la dependencia de las baterías.

- OPCIÓN 2:
  Radios trunking. Ya se explicó la filosofía de funcionamiento de este tipo de redes en los primeros capítulos. Aunque no será normal que se desplieguen en misiones internacionales conectadas a su "red madre" (enlazadas a una red trunking nacional o regional), sí que existe la posibilidad de ser desplegadas con una estación base móvil, que permita el trabajo en modo local, es decir, sólo en la zona de la emergencia. Estas estaciones base móviles crean una "burbuja" de cobertura que varía entre 8 y 20 kilómetros de radio, y cualquier equipo portátil que se mueva bajo esta cobertura le permitirá las mismas funciones que tendría en caso de estar trabajando en Territorio Nacional dentro de su propia red.

95. Estudio detallado de cobertura radio de una zona determinada. Se realiza dejando una radio fija en un punto característico (normalmente el Puesto de Mando o Base de Operaciones), mientras que una persona con otra radio se va desplazando por la zona de la emergencia haciendo llamadas. Usando un plano este último va comprobando diferentes puntos (normalmente a caballo de las líneas de comunicación), anotando si el enlace es afirmativo o nulo (zona de sombra). Al finalizar el recorrido por la zona se obtiene el llamado mapa de coberturas.

La principal ventaja de utilizar este tipo de radios es que si el usuario está ya instruido en el uso de estas radios no nota ningún cambio en las condiciones de uso aunque esté a miles de kilómetros de su ciudad de origen. El tráfico no genera ningún gasto adicional y las capacidades son mucho mayores que la de los *walkies* descritos en el apartado anterior.

El inconveniente es tener la capacidad técnica para montar la estación base y sobre todo instruir a la gente que no haya utilizado nunca este sistema, ya que no es tan intuitivo como las radios anteriores.

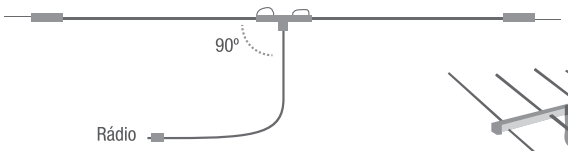
- OPCIÓN 3:

Radios HF. En determinadas circunstancias, para cubrir una zona de acción orográficamente complicada, como pudiera ser una zona montañosa, debemos tener prevista la instalación de radios de HF en los vehículos e instalaciones fijas.

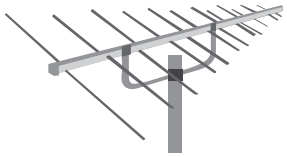
La ventaja del uso de este tipo de radios es que la falta de fiabilidad y la orografía son fácilmente salvables con un correcto cálculo de frecuencias y buscando una manera de propagación radio adecuada. En algunas ocasiones nos veremos obligados a combinar la onda de tierra con la reflexión ionosférica, en concreto usando enlace NVIS para garantizar una reflexión casi vertical y evitar así las zonas de sombra.

Los enlaces radios llevan implícita la ubicación de los llamados **campos de antenas**. En el caso de VHF y UHF es suficiente con un mástil en el tejado o un mástil elevadizo telescópico. También sirve para las radio trunking tipo TETRA o TETRAPOL. Sin embargo para el HF debemos disponer de una zona de terreno amplia para ubicar las antenas. Las antenas podrían ser una varilla y un dipolo cruzado de banda ancha, para no tener que cambiar la longitud de

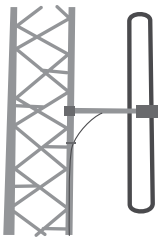
ANTENAS MÁS COMUNES



Dipolo simple

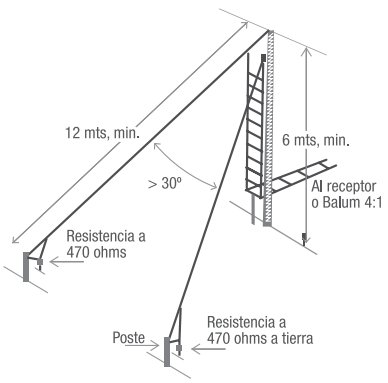


Logoperiódica



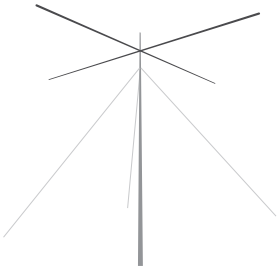
Dipolo doblado

Para el calculo de la longitud del dipolo se utilizará siguiente fórmula:
142.5 / f = Longitud del dipolo en metros, donde f es la frecuencia deseada para el dipolo en megaciclos.
Ejemplo: Deseamos construir una antena para la frecuencia 28.500.
142.5 / 28.5 = 5 metros.



Dipolo en V invertida

Monopolo Vertical Varilla



Dipolo Spider Beam

antena con cada cambio de frecuencia ni vernos obligados a cambiar la dirección de apuntamiento del dipolo dependiendo de la dirección por dónde nos llegue la señal del emisor. Otra opción pudiera ser una antena logaritmo periódica que permitirá un apuntamiento más sencillo.

La ubicación de los terminales radio variará con el propósito de los mismos. Los dedicados a la base de operaciones y emplazamientos fijos se instalaran normalmente en la zona de trabajo. Tendremos que tener en cuenta el ruido que hacen los equipos radio, sobre todo los de HF.

ENLACE CON OTROS EQUIPOS DESPLEGADOS

Todos los medios expresados en los dos apartados anteriores permitirán facilitar la comunicación con otros grupos operativos que puedan intervenir en nuestro área, ya que son equipos de uso extendido entre las organizaciones del mundo de las emergencias.

Si el recurso económico lo permite se podría recurrir a **integradores de comunicaciones[96] de voz,** que aparte de hacer compatibles las comunicaciones entre radios que trabajan en distintas frecuencias también funcionarían como pasarelas entre redes radio y redes telefónicas o satelitales. Estas soluciones a parte de complejas son costosas en esfuerzo y dinero.

MATERIAL DE IMPRENTA, MATERIAL AUXILIAR TELEFÓNICO E INFORMÁTICO PARA LA BASE DE OPERACIONES

En mitad de la selva...o del desierto no venden ni cartuchos de tinta ni folios. Es interesante por tanto llevarse una cantidad importante de estos pertrechos en reserva. Lo habitual será tener lista una caja estanca con un **mínimo de material de imprenta.** Cuadernos, libretas de campo, bolígrafos, rotuladores indelebles, chinchetas, celo, cinta americana, etc.

Hablemos del **material auxiliar telefónico.** Si partimos de la base de que dispondremos de algún enlace telefónico (sea telefonía fija, móvil o satelital), lo complementamos con un **equipo multifunción (FAX, SCANER, IMPRESORA)** que nos permitirá asegurar las funciones básicas de un pequeño Staff o Plana Mayor de Mando.

Ya hemos dicho que podemos complementar nuestro sistema tanto como queramos, lo que en muchas ocasiones también significa complicarlo. Es en este momento que podemos plantearnos el uso de una pequeña **central telefónica para el puesto de mando.** Todo dependerá del número de potenciales usuarios y del tiempo que vaya a durar el despliegue. En ocasiones nos bastará con complementar nuestro enlace telefónico con un **pack de telefonía inalámbrica DETC**, tipo dúo o trío, que nos permitirá ampliar el número de personas de nuestro equipo que pueden tener acceso al teléfono. Incluso se puede configurar para poder realizar llamadas telefónicas entre terminales telefónicos inalámbricos. Si buscamos una solución más profesional deberemos decantarnos por una **central telefónica portátil** o quizás por una solución que nos valga para la conmutación tanto de voz como de datos. Nos referimos a los routers. **El uso de un router como central telefónica** es cada vez más habitual, y al usar la voz sobre tecnología IP, se favorece la interoperabilidad con otros usuarios. Esto llevará de manera inexcusable el uso de terminales telefónicos específicos para este tipo de tecnología.

96. La Guardia Nacional estadounidense y la Unidad Militar de Emergencias española cuentan en dotación con este tipo de aparatos de los modelos ACU 1000 y 2000.

Pasemos al **material Informático.** Para un grupo de 10 personas, lo ideal será complementar los terminales telefónicos con al menos **dos ordenadores portátiles** con todo el software necesario (no olvidar el antivirus).

En este punto cabe la posibilidad de analizar la **eterna disyuntiva entre ordenadores rugerizados o los "convencionales".** La fiabilidad que dan estos ordenadores preparados para trabajar en condiciones extremas, es muy alta. El problema es el precio. Las Fuerzas Armadas de todo el mundo han decidido dejar de apostar por terminales informáticos rugerizados por el alto coste que supone su adquisición, y por el poco tiempo que transcurre hasta que se quedan obsoletos debido a la rapidez con que la tecnología avanza.

La **recomendación** es la siguiente. Si tenemos la opción de preparar el equipo de enlace con meses o años de antelación, debemos decantarnos por material comercial normal y corriente. Esto nos permitirá sacarle provecho independientemente de que seamos o no desplegados. Si el tiempo pasa y el ordenador se queda viejo, lo podremos cambiar por otro más moderno, y además le habremos sacado todo el "jugo" al primero.

Por el contrario si el presupuesto nos lo permite y tenemos que comprar un ordenador para desplegar, como quien dice... pasado mañana, debemos decantarnos por el rugerizado. El precio puede ser hasta tres veces más que el ordenador comercial, pero en cambio la fiabilidad del rugerizado será diez veces superior. El uso inminente o que esté casi garantizado, debe influir en la elección hacia el ordenador protegido.

Otro aspecto importante es llevarnos algún **soporte informático** (memorias USB, DVD,s, Discos Duros Externos, etc.) con todo el **software necesario para poder reinstalar los ordenadores** en caso de que se desconfiguren y se tengan que volver a formatear. Recuerden que Murphy estará siempre preparado para hacerse notar...

Igualmente contaremos con un número suficiente de **memorias USB** de diferentes capacidades para poder distribuir la información con otros elementos desplegados y como herramienta de trabajo.

Es imprescindible llevar un **Disco Duro Externo para "*BACK UP*",** en el que al final de cada jornada, hacer una salvaguarda de los datos más importantes del día, para que en el caso de que algún ordenador quede inutilizado, se tenga un soporte alternativo del que recuperar la información.

Hasta este momento no nos habíamos planteado montar una **Red de Área Local (LAN).** Normalmente en este tipo de misiones no se plantean redes basadas en cable y se suelen decantar por **redes inalámbricas,** por su bajo coste y sobre todo por su fácil y rápida implementación. Para materializarlas deberemos llevar un router Wifi. El número a partir del cual es útil montar esta red es el de cuatro ordenadores. Por debajo de este número se pueden implantar otro tipo de soluciones que no necesitan de la existencia del router.

El Kit informático lo completaremos con **una videocámara** para recoger imágenes fotográficas y/o video para tener la posibilidad de tratarla en nuestro sistema de información.

Para acabar este apartado haremos mención a los **equipos de videoconferencia**. Existe en el mercado una extensa variedad de equipos de videoconferencia (VTC). Estos equipos suelen ser aparte de caros, muy exigentes en lo relativo a anchos de banda. Lo normal en nuestra misión será conformarnos con la solución proporcionada con los propios ordenadores portátiles con camera web incorporada.

LA "CHULETA"

Aunque nosotros los Responsables TIC pensemos que tenemos buena memoria, y que sabemos de sobra los datos que nos son imprescindibles para hacer nuestro trabajo, es importante llevar a mano un pequeño documento, convenientemente protegido de las inclemencias del tiempo (plastificado, enfundado, etc.). En este documento reflejaremos aquellos datos que sean difíciles de recordar o sencillamente que nos sirvan para no confundirnos en momentos de estrés o alta tensión.

No existe formato estándar, o mejor dicho existen miles de modelos porque cada cual se organiza el suyo propio. Un documento con los teléfonos más importantes de nuestros corresponsales o con los de la gente de nuestro equipo. Los indicativos radio, las direcciones IP de nuestros servidores, etc. A este documento en argot militar se le denomina "**extracto de IBT**[97]" o "IBT" a secas.

Si este documento puede llegar a ser útil para nosotros los responsables TIC, imagínese el lector lo que puede ser para algunos de los "tipos" de usuarios TIC que hemos visto en capítulos anteriores el poder

97. IBT: Instrucción Básica de Transmisiones. En la actualidad se está perdiendo esta denominación a favor de IBCIS, instrucción Básica de los Sistemas de Telecomunicaciones e Información.

disponer de estos datos a mano en un momento dado. Por lo tanto deberemos ser nosotros los que preparemos este documento para ellos.

Tiene que ser un documento sencillo, pequeño que no ocupe mucho más que una tarjeta de crédito y que se pueda portar por ejemplo dentro de la cartera o en el interior del pasaporte que cada miembro del equipo lleve encima.

También es útil pegar a las mesas o en tablones cercano a los medios de enlace que se estén utilizando, teniendo muy presente que la información que se refleje en estas "chuletas" no debe ser sensible o que ponga en peligro la seguridad de la operación en su conjunto o la de las personas en particular.

SISTEMA DE ALIMENTACIÓN ELÉCTRICA E ILUMINACIÓN

Para finalizar deberemos tener presente todo el **componente eléctrico**. En Estados Unidos durante el año 2004, se produjeron unas fuertes tormentas de nieve y el servicio telefónico se interrumpió porque se cayeron los tendidos eléctricos y además se agotó el combustible de los Grupos Electrógenos de respaldo. Aunque trataremos de conectar nuestro sistema de comunicaciones a la Red Eléctrica General del país damnificado, debemos prever llevar desde Territorio Nacional alimentación mediante **Grupos Electrógenos (GE) portátiles.**

Se precisarán al menos dos (2). De esta manera tendremos asegurada la alternancia entre ellos para descanso y repostaje. La elección entre grupos de gasolina o diesel dependerá de la zona de despliegue. Por ejemplo en el continente americano, preferiremos los de Gasolina (más fácil de conseguir) en lugar de los de Gasoil. Los GE de gasolina son más baratos y menos pesados, lo que los hace muy aptos para el aerotransporte.

La potencia de los Grupos dependerá del cálculo de consumo de los equipos que vayamos a poner en funcionamiento. Los GE portátiles suelen estar **entre 3 y 5 KWA de potencia.** Al subir de potencia, aumentan de tamaño lógicamente. En el mercado existen soluciones sobre remolque de grupos de potencias superiores que siguen cabiendo en una aeronave de transporte para su traslado hasta la zona de operaciones.

Puede ser muy útiles o imprescindibles si se va a una zona sin corriente eléctrica, el dotarse de **medios auxiliares para recarga de baterías** de los equipos. Nos estamos refiriendo a **mantas solares y a generadores de mano tipo dinamos** (conocidos como "molinillos", por su semejanza con los antiguos molinillos de café). En este caso es esencial comprobar que los conectores de salida de las mantas o de las dinamos manuales son compatibles con los conectores de las baterías. Si no lo son es imprescindible fabricar **regletas de adaptación** en algún taller de electrónica.

Otra precaución a tener en cuenta si decidimos conectarnos a la red general eléctrica del lugar de la emergencia es la **tensión o voltaje y la frecuencia.** En Europa las fuentes de alimentación de los equipos electrónicos están preparadas para trabajar a 50 hertzios (Hz), mientras que en América lo hacen a 60 Hz. En cualquier buscador de internet se pueden obtener los amperajes y voltajes de todos los países del mundo.

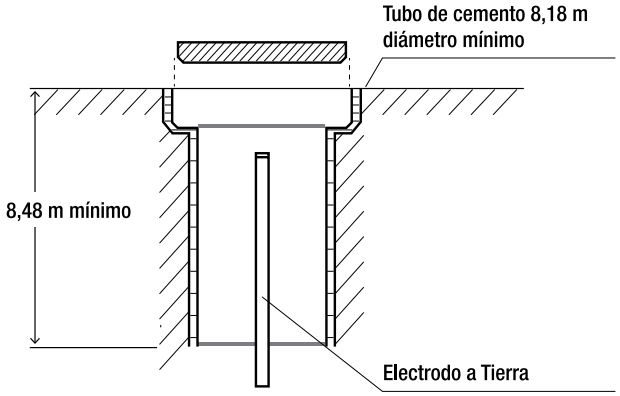
Para resolver en parte esa situación, últimamente muchos fabricantes de equipos portátiles incluyen un adaptador o transformador universal de corriente, que acepta un amplio rango de tensiones o voltajes y frecuencias de entrada de corriente alterna. Esos dispositivos tienen la ventaja que se pueden utilizar tanto en casa como cuando viajamos a otros países donde la corriente alterna tiene características diferentes a la de nuestro país, para que así no tengamos que preocuparnos por ese tema. Para conocer si un **adaptador es "universal"** o no, lo único que tenemos que hacer es leer la chapa o pegatina de datos que normalmente muestran en un lugar visible esos dispositivos.

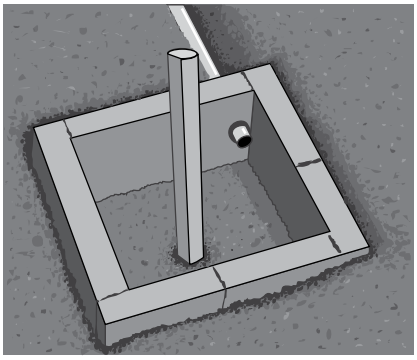
En la ilustración de la derecha se puede observar la chapa informativa de un adaptador de corriente eléctrica, en la que se puede leer que acepta una AC (corriente alterna) de entrada (IN) que puede ir de ~ 100 hasta 240 V (volts) y entre 50 y 60 Hz de frecuencia.

Debemos llevar elementos que puedan proteger nuestros equipos de variaciones en la tensión de las fuentes de suministro eléctrico. Bien sea suministro general, bien grupos electrógenos se pueden producir subidas que pueden, literalmente fundir, nuestros equipos si no están protegidos convenientemente.

A este efecto debemos prever llevando algún **Sistema de Alimentación Ininterrumpida (SAI) / Estabilizador de Corriente** con capacidad suficiente para conectar todos los equipos mencionados. Si la potencia de la SAI no es suficiente para conectar todos los medios, entonces elegiremos los más sensibles a las fluctuaciones, pero sobre todo los más vitales para cumplimentar nuestra misión. De esta manera además aseguraremos la supervivencia ante los picos de tensión y tendremos tiempo suficiente para apagar los equipos

FALLOS EN LA TOMA DE TIERRA





cuando se vaya la luz. No olvidaremos tampoco **alargaderas y regletas de conexión** para asegurar los tendidos.

Por último nos queda abordar la **iluminación del lugar de trabajo**. Si llegamos a un edificio, es de imaginar que éste cuente con la suya propia. No obstante si estamos en disposición de preverlo, se debe preparar un arcón o caja de transporte con un **juego de luminarias estancas** que garantice una correcta iluminación del área de trabajo. Estos juegos de luminarias suelen ser bastante caros, por lo que dependiendo de nuestro presupuesto, la instalación de la luz en nuestro puesto de mando se puede limitar a llevar 30 metros de cable, 8 casquillos y otras tantas bombillas que nos puedan sacar del apuro. Se debe tratar de que estas bombillas sean de bajo consumo para no sobrecargar a los grupos electrógenos.

Es primordial comprobar la **toma de tierra** de la instalación que vayamos a ocupar si se trata de un edificio. Incluso si tuviéramos duda del estado deberíamos hacer una para evitar accidentes. Los grupos electrógenos van dotados de su propia toma.

Una toma de tierra básicamente consiste en un conductor que entra en contacto con el suelo. Existen diversas formas de hacerlo. El cable de masa partirá del cuadro eléctrico de la instalación fija o de la entrada de corriente de la Base de Operaciones.

Como conexión a tierra podemos usar una barra metálica, conocida como **jabalina**, de unos dos metros de longitud completamente clavada en el suelo. La barra puede ser de cobre con un diámetro superior a los 15 milímetros, o de acero con un diámetro mayor de 25 milímetros. También podemos utilizar un cable pelado como conexión a tierra. En este caso podemos colocarlo siguiendo dos disposiciones: a lo largo de una zanja que de la vuelta completamente al perímetro de la casa o de la tienda del Puesto de Mando (anillo perimetral) a un metro de las paredes, o a lo largo de una zanja recta que se aleje unos cuantos metros de la zona de trabajo. En cualquier caso tendremos un buen número de metros de cable pelado enterrado en una zanja.

Hay que tener en cuenta que cuanto menor sea la resistencia que ofrezca la toma de tierra, mejor actuará como tal. Así que el cable o el poste que utilicemos deberán ser de un grosor considerable y deberemos mantener la zona húmeda regándola regularmente.

ACCIDENTES POR MALA TOMA DE TIERRA

El contacto con una corriente eléctrica puede tener peores consecuencias que el típico calambrazo que todos hemos sufrido en alguna ocasión: desde graves quemaduras hasta una parada respiratoria o cardiaca. Las consecuencias van a depender de la intensidad de la corriente y del tiempo de exposición a la misma.

Reconocer una quemadura eléctrica es relativamente sencillo ya que tiene unas características particulares: la lesión de entrada está bien definida, es pequeña, indolora, de un color blanco grisáceo y con apariencia de piel endurecida. La lesión de salida es más grande, más oscura, hundida en el centro.

Su buen aspecto y tamaño es engañoso: la verdadera lesión se produce debajo de la piel, afecta a músculos y huesos y es tan potente que puede llegar a destruir toda la musculatura de una extremidad.


M31
M31

CAPÍTULO 15

ENLACES ESPECIALES

Este capítulo pretende ser un apartado totalmente complementario. Incorpora por un lado una ampliación sobre algunos de los medios de enlace ya comentados, y trata por primera vez otros de los cuales no habíamos hablado hasta este instante. Además se van a acometer las particularidades de los medios de enlace a emplear en emergencias que se producen en determinadas ubicaciones.

MEDIOS DE ENLACE ÓPTICOS

Es difícil que estos medios se empleen en una emergencia, pero no imposible. Así que demos una breve reseña. Los medios visuales u ópticos son aquellos que emplean un código de señales visuales para la transmisión y recepción de mensajes.

Hay muchas formas de comunicaciones ópticas **que no están basadas en la tecnología.** Empezando por el lenguaje de sordomudos, o un aviso que realice una persona desde la tierra al paso de un helicóptero reclamando su atención. Otro ejemplo lo podemos encontrar en las maniobras ejecutadas por una aeronave, que tienen significados particulares. Así cuando un avión quiere avisar a una embarcación en peligro, puede describir un círculo alrededor de la embarcación, por lo menos una vez; volar a baja altura cruzando el rumbo de la embarcación, y alabeando las alas; o abriendo y cerrando el mando de gases.

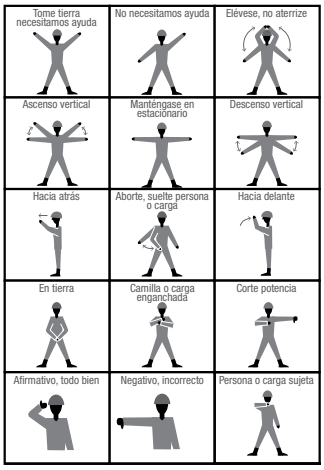
EJEMPLOS DE SEÑALES ÓPTICAS

Paineles Tierra-aire

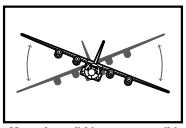
No	MENSAJE	SÍMBOLO
1	NECESITAMOS MÉDICO HERIDOS GRAVES	I
2	NECESITAMOS MEDICAMENTOS	II
3	NO PODEMOS PROSEGUIR VIAJE	X
4	NECESITAMOS ALIMENTOS Y AGUA	F
5	NECESITAMOS ARMAS DE FUEGO Y MUNICIONES	VV
6	NECESITAMOS MAPA Y BRÚJULA	□
7	NECESITAMOS LÁMPARA DE SEÑALES, RADIO Y BATERÍAS	I
8	INDIQUEN LA DIRECCIÓN A SEGUIR	K
9	ESTAMOS AVANZANDO EN ESTA DIRECCIÓN	↑

No	MENSAJE	SÍMBOLO
10	INTENTAREMOS DESPEGAR	I>
11	AERONAVE CON GRANDES AVERÍAS	LL
12	PROBABLEMENTE SE PUEDA ATERRIZAR AQUI CON SEGURIDAD	△
13	NECESITAMOS COMBUSTIBLE Y ACEITE	L
14	SIN NOVEDAD	LL
15	NO	N
16	SI	Y
17	NO COMPRENDEMOS	⅄L
18	NECESITAMOS MÉDICO	W

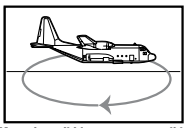
Visuales con Helicopteros



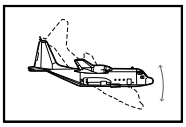
Visuales Aire-tierra



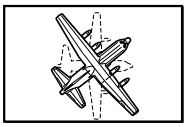
Mensaje recibido y comprendido (Alabeando)



Mensaje recibido y no comprendido (Describiendo un círculo)



Afirmativo (Cabeceando el morro)



Negativo (Guiñando a izqda y dcha)

Se pueden hacer diferentes clasificaciones dependiendo el equipo que se utilice. Así podemos mencionar:

- Paneles: también utilizada la palabra "**painel**". Son señales realizadas mediante un código convenido que se materializa con paneles, o similares (telas, maderas...).
- Equipos generadores de señales ópticas: se pueden usar de diferentes tipos. Entre los más utilizados están las persianas de Morse, luces de navegación, los heliógrafos y las banderolas de señales. No nos olvidamos tampoco de los destellos de un espejo.
- Artificios luminosos o de humos: bengalas, hogueras, botes de humo o candelas.
- Equipos de señales ópticas no visibles: persianas de infrarrojos.
- Otros: gesticulación de personas, maniobras concertadas de aeronaves, etc.

En ocasiones, y relacionadas con este tipo de señales ópticas, aparecen mencionadas las almenaras[98], torres, torretas, globos aerostáticos o globos cautivos[99]. Cualquiera de estos elementos resulta ser una ayuda adicional al enlace óptico mediante el cual se gana altura del elemento transmisor utilizado (luces, fogatas, heliógrafos, etc.), y por tanto se aumenta el alcance de la señal en distancia.

MEDIOS DE ENLACE ACÚSTICOS

Una pistola u otro medio detonante/explosivo disparado a intervalos de un minuto, una señal sonora interrumpida con cualquier aparato para indicar la presencia por ejemplo en la niebla, son claros ejemplos.

Las **bocinas, silbatos o cualquier elemento que haga ruido** sirven para el envío de mensajes breves, a distancias relativamente cortas, y con arreglo a códigos

98. Almenara: procede del árabe al-manāra. Fogata que se hacía por la noche en las cumbres de los montes o en atalayas, que con un lenguaje simple preestablecido, servía para comunicar mensajes básicos. Por ejemplo las harkas rifeñas que combatían contra España en las Guerras de África a finales del XIX y principios del XX, las usaban asiduamente para convocar alguna reunión urgente, pedir auxilio o llamar a los muyahidines a la Yihad.

99. La diferencia entre globos aerostáticos y los cautivos radica en que los primeros tienen capacidad de trasladarse y dirigirse por sus propios medios, y con la ayuda de un piloto, a un destino concreto, mientras que los segundos sólo se elevan en la misma posición en la que se encuentran permaneciendo unidos mediante una o varias cuerdas al suelo para que no se desplacen horizontalmente.

previamente establecidos. Son inexactos pero pueden facilitar por ejemplo la localización de los supervivientes, aunque también pueden inducir a error en la interpretación de los códigos cuando el personal que los maneja no está suficientemente instruido.

OFICIALES DE ENLACE (OFEN)

Ya sabemos que son aquellas personas de una organización cuya misión es mantener el contacto o la comunicación entre su agencia origen y otra a la que ha sido destacado para asegurar el mutuo entendimiento y unidad de propósito y acción durante el trascurso de una emergencia. Antaño fue uno de los procedimientos más empleados para mantener el enlace entre organizaciones. Un OFEN (en inglés "Liaison Officer" (LNO) u oficial de enlace **es como una pequeña "sucursal" de nuestra organización insertada dentro de otra. Representa a su Jefe o al Staff de su organización** y sirve para transmitir de primera mano que está haciendo su agencia y para recabar información que pueda ser de interés para la organización propia desde dentro de la agencia ajena.

Las misiones más comunes de los Oficiales de Enlace son:

- Mantener su agencia informada de la situación
- Mantener el organismo apoyado informado de la situación de su propia agencia
- Asesoramiento sobre los recursos disponibles de su agencia
- Proporcionar asesoramiento técnico sobre las capacidades de la agencia
- Ayudar en el desarrollo de los planes coordinados entre las agencias
- Retransmisión y asignación de tareas a su agencia en nombre de la agencia apoyada

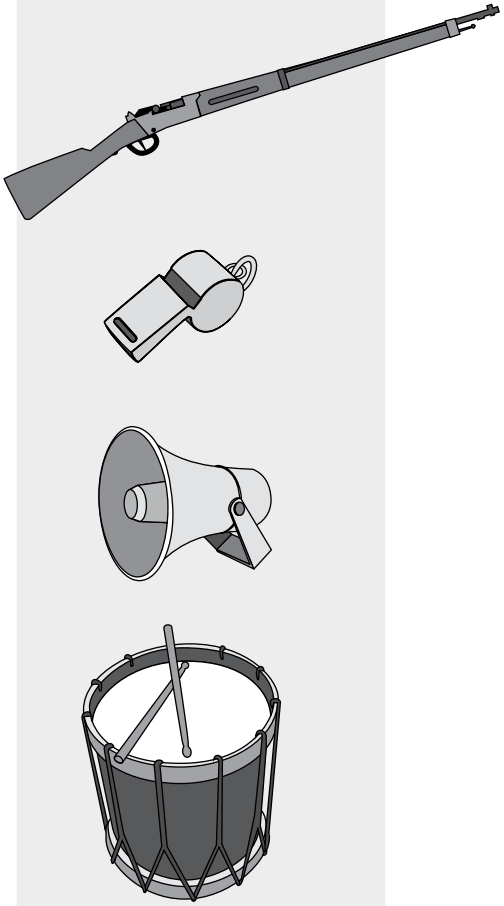
Son especialmente útiles para sincronizar acciones y focalizar el interés en aspectos que de no estar presente podrían no llegar a visualizarse en la agencia de origen. Además evitan posibles fricciones o malos entendidos ya que estos son testigos presenciales de las operaciones que cada cual desarrolla. Se suelen usar para transmitir mensajes directos entre directivos, obviando escalones intermedios con lo que se consigue claridad y agilidad.

La formación y el puesto en la jerarquía dentro de la organización son aspectos a considerar antes de destacar nuestro OFEN a otra agencia. El entrenamiento, la competencia y la confianza que en él se depositen son fundamentales.

Cuando destaquemos un oficial de enlace propio a otra organización **debemos enviarle con los medios de enlace necesarios para asegurar el flujo de información con nosotros.** Es decir llevará su propia radio, ordenador y cualquier otro enser que pueda necesitar para cumplir sus cometidos. Sin embargo será la **organización que lo acepta** la que le proporcionará y **cubrirá sus necesidades logísticas básicas,** comida, alojamiento, etc. En caso de que se le dote con un pequeño staff auxiliar (administrativos, coche con conductor, etc.) pasaríamos a denominarle "**destacamento de enlace".**

Sirva como ejemplo que en cualquier intervención que realiza la Unidad Militar de Emergencias a petición de las Comunidades Autónomas, por procedimiento automáticamente destaca oficiales de enlace a los CECOP y a los PMA de las CCAA que entren en funcionamiento.

PROCEDIMIENTOS Y MEDIOS ACÚSTICOS



TAMBOR DEL BRUCH

Entre los siglos XVI y XIX, los contendientes de los campos de batalla europeos, luchaban al ritmo marcado por las cornetas y tambores. El Tambor del Bruch (en catalán *el timbaler del Bruc*, "el tamborilero del Bruch" o también conocido popularmente como El Niño del Tambor) es el nombre de una leyenda formada a partir de hechos ocurridos en 1808 durante la Guerra de la Independencia Española. Cuenta la tradición que al transmitir las ordenes de combate a traves de los redobles, la reverberación del sonido del tambor al chocar con las paredes de Montserrat hizo creer al invasor francés que el número de soldados españoles era muy superior al que realmente había.

LOS MENSAJEROS

Las personas que ejercían esta misión recibían antiguamente la denominación de "**correo**", precisamente por portar este material entre dos lugares diferentes. Es evidente que los motoristas actuales de las empresas de mensajería guardan todavía cierta relación con aquellos que a caballo o a pie recorrían grandes distancias, apoyándose en estafetas y postas[100].

Los **mensajeros profesionales (pertenecientes a empresas de mensajería)** son personal instruido que utilizando diferentes tipos de transporte realizan el **envío de documentos y mensajes.** La principal ventaja es que permiten transportar tanto documentos normales como otros de gran volumen. También son de mucha utilidad para aquellos con un formato difícil de enviar por medios convencionales.

Aunque las empresas de mensajería podrían tener su papel en las emergencias, en este apartado pondremos el acento en otro tipo de mensajero que en lugar de estar asociado a una empresa lo va a estar a un **recorrido "*ad hoc*"** que muy probablemente haya marcado el Responsable TIC **para satisfacer un enlace entre dos puntos** durante el transcurso de una emergencia.

Se trata por lo tanto de **nominar una o más personas, que en unión a un medio de transporte, se desplazará por la zona de la emergencia para llevar información entre diferentes ubicaciones.**

En las emergencias son muy útiles cuando existen situaciones inestables en las que los puestos de mando no tienen un emplazamiento fijo, o cuando otros medios de enlace han dejado de funcionar. Además en cualquier momento se puede utilizar un transporte que vaya a pasar por el lugar donde esté la persona que tiene que recibir la información, para hacerle llegar el documento.

El principal inconveniente es la lentitud, o mejor dicho **la no inmediatez,** marcada por el medio de transporte empleado, que a su vez se ve influenciado por las condiciones meteorológicas y el terreno.

Aunque cada organización puede determinar la existencia de uno o más mensajeros sin sujeción a un horario concreto, se pueden establecer previo planeamiento, las denominadas **redes de mensajeros.** Estas redes están definidas por el momento y el modo en cómo se hacen los recorridos entre los lugares que se determine que hay que enlazar mediante este servicio. Así podremos tener los siguientes procedimientos:

- Rotación: los mensajeros recorren un itinerario fijado con arreglo a un horario establecido.
- Intercambio: los mensajeros van a horas determinadas a un lugar donde se intercambian los mensajes entre ellos.
- Radial: desde una ubicación concreta se envían varios mensajeros a múltiples destinos. A su vez dentro de este sistema se puede implementar la rotación o el intercambio.

SERVICIOS POSTALES

Este formato será poco utilizado en las emergencias. Las nuevas tecnologías le han quitado protagonismo a la carta postal debido que esta última no reúne las condiciones de rapidez que las comunicaciones en emergencias exigen.

Tiene un antecedente común en el apartado que acabamos de dedicar a los Mensajeros. En nuestro país es Felipe V el que durante la Guerra de Sucesión, decidió

100. Las **postas** eran casas situadas en los caminos, separadas unas de otras entre dos y tres leguas (aproximadamente 4,4 km), donde había caballos de refresco. **La estafeta** o cartería era el lugar donde se recibían y depositaban las cartas.

recuperar para el Estado las concesiones y arriendos que hasta la fecha tenía cedidas a empresas privadas encargadas de la correspondencia en la península y en el vasto imperio español que en aquella época se extendía por cuatro continentes.

En la actualidad en España sigue existiendo el Grupo Correos[101] (en pleno proceso de adaptación al Siglo XXI), que es el operador responsable de prestar el **servicio postal universal en España**, de acuerdo a unos requisitos de calidad, regularidad, accesibilidad y asequibilidad que hacen efectivo el derecho de todos los ciudadanos a las comunicaciones postales.

El servicio ofrecido se articula para **satisfacer las necesidades de correo y paquetería ordinarias entre sedes conocidas y fijas.** Es decir, aunque se pueda encontrar algún tipo de similitud (de hecho la hay) con los mensajeros de Empresas de Mensajería, la mayor diferencia con los servicios de mensajeros "ad hoc" de emergencias se encuentra en que estos últimos recorren la zona de la catástrofe enlazando puestos de mando o personas físicas allí desplegadas, algo que sin duda quedaría fuera de las funciones de Correos o de una empresa de paquetería convencional.

ANIMALES ADIESTRADOS

No es común en nuestros días, pero históricamente han dado muy buenos resultados. No dejan de ser un medio complementario de envío de información en circunstancias muy especiales. La paloma sobresale sobre otros animales.

La **Colombofilia** es el arte de criar y entrenar palomas mensajeras. Hoy día su finalidad es deportiva, pero se utilizan también en caso de catástrofes y operaciones de salvamento. Incluso han sido utilizadas para intercambio de muestras entre hospitales. Sin embargo tampoco es sencillo su trabajo y no es fácil ni segura la llegada a su destino, que por cierto es su casa. Son muchas las dificultades que encuentra: la orografía, las condiciones meteorológicas reinantes del territorio donde tiene que volar, las aves de rapiña, o los cazadores.

COMUNICACIONES RADIO DENTRO DE EDIFICIOS

Nos estamos refiriendo a los diferentes equipos radio portátiles que pueden llevar los intervinientes de las organizaciones de socorro y emergencia cuando tratan de realizar su labor dentro de edificios. Hemos visto que estas radios suelen ser equipos que trabajan en unas bandas concretas, **VHF y UHF**, las cuales tienen dificultad de penetrar a través de paredes de mampostería o de hormigón armado. Sin embargo atraviesan ventanas, pasillos, huecos de escalera y tabiques interiores próximos con relativa facilidad. Además se puede producir la llamada **difracción**, explicada en la figura siguiente.

El empleo de radios de **UHF/SHF facilita la penetración de las ondas de radio en las viviendas** en comparación con las de la banda de **VHF, que tiene peores condiciones de propagación** dentro de los edificios. Sin embargo ninguna de las dos es la panacea, por lo que debemos buscar algunas soluciones que favorezcan asegurar el enlace.

Una solución es **cambiar de ubicación** buscando el menor número de obstáculos, en nuestro caso paredes, y facilitar el enlace. **Dentro de la misma planta**

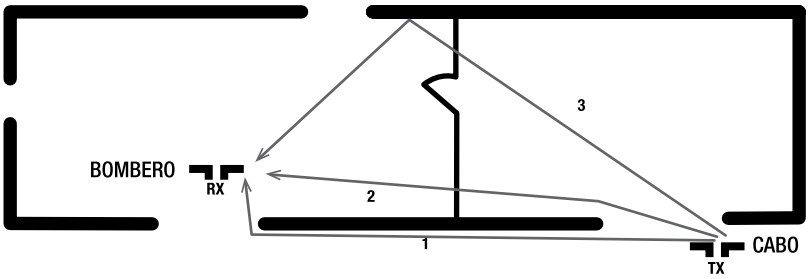
EL ENEMIGO DE LAS PALOMAS MENSAJERAS

Durante las Guerras Mundiales tuvo lugar el nacimiento de la llamada Guerra Electrónica (EW, del inglés *Electronic Warfare*) entendida como la actividad tendente a determinar, explotar, reducir o impedir el uso de los medios de enlace del adversario.

Los alemanes siempre confiaron en el sistema de las palomas mensajeras y fue ampliamente utilizado en todos los frentes y en especial por los espías alemanes situados en Gran Bretaña. La base de las palomas alemanas estaba situada en Freilassing en el centro de Alemania.

Los alemanes entrenaron halcones peregrinos para la caza de las palomas utilizadas por los aliados, ya que se trata del enemigo natural de estas aves. Establecieron una completa red de defensa en Francia, Bélgica y Holanda compuesta por halcones y francotiradores para interceptar a las mensajeras aladas de los aliados.

101. El Grupo Correos, conocido comúnmente como Correos, es una empresa de capital cien por cien público cuyo propietario es el Estado español, a través de la Sociedad Estatal de Participaciones Industriales (SEPI).



LA DIFRACCIÓN

Un Cabo de bomberos en el exterior de un edificio con una PMR trata de hablar con su compañero situado en el interior. En este caso, existen tres trayectorias desde el transmisor del Cabo al receptor del Bombero, y ninguna de ellas es directa.

La trayectoria 1 pasa a través de la ventana más cercana al lugar en el que se encuentra ubicado el Bombero y es difractada alrededor del borde saliente del marco de la ventana hacia el receptor.

La trayectoria 2 pierde el camino directo hacia el receptor del Bombero. Es difractada ligeramente por el marco de la ventana más cercana al transmisor y luego atraviesa una pared interna en el camino hacia el receptor.

La trayectoria 3 pasa a través de una ventana y de una pared interna antes de chocar contra una pared externa del edificio y luego reflejarse nuevamente hacia el receptor.

Cada una de estas trayectorias tiene una distancia diferente y, por consiguiente, puede producir distorsión por trayectoria múltiple. Con frecuencia, el mover el receptor unos pocos centímetros en cualquier dirección evitará una o más de las trayectorias disponibles, mejorándose enormemente la recepción de la señal.

los intervinientes deben buscar los espacios libres como los pasillos con el fin de que las ondas lleguen "rebotando" hasta el receptor destino. Si la comunicación es entre **interior y exterior** del edificio se deberán buscar las ventanas por parte de los actuantes que deambulan por el edificio; mientras que **el personal que está en el exterior,** si están tratando de enlazar con personal que se encuentran en plantas superiores, deberán separarse del edificio para buscar la línea de visión directa entre radios.

Cuando el enlace es **entre intervinientes** que se encuentran **dentro del edificio** en diferentes plantas, se deben buscar huecos de ascensor o de escaleras, con la misma filosofía expuesta en el párrafo anterior, es decir, buscar el menor número de obstáculos posibles.

Otro modo de facilitar el enlace dentro de edificios es hacer uso de **repetidores de radio.** Los repetidores se pueden colocar tanto en planta como en altura del edificio. En ambos casos hay que guardar el procedimiento de buscar zonas libres de obstáculos. Dentro de la misma planta se ubicarán en pasillos y esquinas, mientras que si lo que queremos es ganar enlace entre plantas, los ubicaremos en los huecos de escalera principalmente.

Los repetidores también se pueden colocar **en edificios que estén enfrente del edificio siniestrado,** en cuyo caso los intervinientes que trabajen en el interior en plantas altas, buscarán las ventanas exteriores (preferiblemente las más próximas al repetidor). También se podría ubicar el **repetidor en un helicóptero, o en globo estático,** si no hay edificios alrededor. En este caso el piloto debe volar en círculos alrededor del edificio que tenga la emergencia, pero nunca encima.

Por último y como no podía ser de otra forma la tecnología actual ha encontrado el modo de facilitar el enlace. En la actualidad existen **equipos radio IP** con la llamada **tecnología MESH.** Por un lado han aumentado la frecuencia con respecto a los equipos convencionales PMR usados en emergencias, ganando así penetrabilidad. Pero además cada radio se convierte en un repetidor potencial. Los operarios pueden comunicarse entre sí. Todo nodo perteneciente a una red MESH permite el paso de la información a través de él hacia otros nodos. Cuando un usuario quiere hablar con un tercero con el que no tienen enlace, pero existe un segundo interviniente que tiene enlace con ambos dos, la radio, sin intervención del segundo operador, se encarga de retransmitir la información hasta que le llega al destinatario.

COMUNICACIONES SUBMARINAS / ACUÁTICAS

Debemos conocer como Responsables TIC que posibilidades tenemos para comunicarnos con intervinientes que se encuentren, por ejemplo en operaciones de búsqueda y rescate dentro del agua.

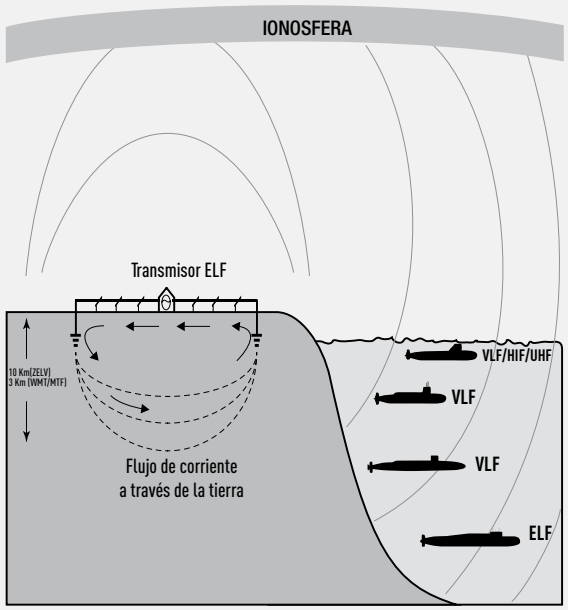
Las **comunicaciones por radio** dentro del agua sólo son posibles en frecuencias muy bajas, por debajo de 10 KHz, con muy poco ancho de banda y una gran atenuación. En comparación con los sistemas de enlace que trabajan con señales propagadas por el aire, en el medio submarino están severamente limitados debido a que el agua es esencialmente opaca a la radiación electromagnética, con excepción de la banda de la luz visible, aunque ésta penetra sólo unos pocos cientos de metros en las aguas más cristalinas, y a una menor profundidad en las cargadas de sedimentos o altamente pobladas.

Las **comunicaciones ópticas** submarinas se usan hasta unos 100 metros de profundidad, con luz verde y azul, que penetran mucho más que el rojo. El ancho de banda es muy alto, ya que la información viaja incrustada sobre la portadora óptica luminosa. Esto posibilita el despliegue inalámbrico de sistemas de vídeo, control en tiempo real o de sensores con necesidad de gran ancho de banda, sin las limitaciones de movilidad del cable submarino.

En consecuencia, se han desarrollado **técnicas acústicas** que son ahora el modo de comunicación submarina predominante entre barcos y vehículos robóticos o submarinistas bajo el agua. Sin embargo, los sistemas acústicos, aunque permiten la comunicación a larga distancia, transmiten datos a velocidades limitadas y la transferencia se realiza además con retardo debido a la velocidad relativamente lenta del sonido en el agua.

En ocasiones cuando la profundidad es poca como ocurre por ejemplo cuando los buzos realizan trabajos con escafandra, se aprovecha la conducción por la que se suministra el oxígeno para meter sistemas de comunicación telefónicos o incluso de video para proyectar en la superficie lo que se hace en las profundidades del mar, pantanos o ríos.

ENLACE CON SUBMARINOS



LA TIERRA COMO ANTENA

El uso de ondas de muy baja frecuencia (VLF), permite la comunicación con submarinos que estén a menos de 20 m. de la superficie. La OTAN tiene una red de decenas de emisoras VLF en todo el mundo.

Para enlazar con submarinos que estén lejos de la superficie, hay que hacer uso de ondas electromagnéticas de extremada baja frecuencia (SLF/ELF). A priori se necesitarían antenas de miles de kilómetros.

Como esto no es viable, se optó por usar parte de la tierra como antena. Esta fue la solución que adoptaron tanto la URSS como Estados Unidos durante la Guerra Fría. La URSS construyó el sistema ZEVS; su emisora de 82 Hz en la península de Kola mientras que EEUU emitía a 76 Hz desde el estado de Michigan con su WMT/MTF.

Ambos sistemas son cables de más de 50 km. cuyos extremos están enterrados cientos de metros en el suelo.

COMUNICACIONES SUBTERRÁNEAS EN GENERAL

Pasamos a continuación a tratar en éste, y en los tres apartados siguientes, lo que podríamos denominar "**TIC subterráneas**" que se caracteriza por una **problemática particular**.

Si quisiéramos recurrir a la solución radio rápidamente nos daríamos cuenta de que las telecomunicaciones aquí están muy condicionadas por el terreno. La señal radio se ve obligada a atravesar rocas con conductividades muy variables. Se produce una gran absorción de la señal en los muros de las galerías subterráneas. Se trata por tanto de un **medio muy hostil** caracterizado por la humedad y el agua; el barro y el polvo; donde resulta muy difícil la progresión y con frecuencia se producen derrumbes y explosiones.

Podríamos hacer una **clasificación inicial** sobre las tecnologías disponibles en comunicaciones subterráneas:

- Comunicaciones inalámbricas con infraestructura previa existente. Éste puede ser el caso de un túnel o una mina.
  - Tendido previo de cable radiante.
  - Inalámbricas con antenas distribuidas.
  - Inalámbricas con estaciones base.
- Comunicaciones inalámbricas sin instalación de infraestructura previa, como ocurre por ejemplo en una cueva:
  - Propagación por conductores metálicos existentes (LF/MF).
  - Redes Ad-Hoc (UHF).
  - Propagación natural por túneles (UHF).
  - Propagación a través de la roca (Through The Earth, TTE) (VLF).
- Comunicación por cable o fibra.
  - Sistemas geneofónicos.
  - Despliegue *in situ* de cable telefónico.

RESCATE EN MINAS

La actividad minera se ha alineado desde siempre a la evolución tecnológica, principalmente por la necesidad de mejorar sus niveles de seguridad de las personas y la eficiencia en la explotación de los proyectos mineros. Del mundo de las **telecomunicaciones** se ha valido este sector **para mejorar los flujos de información** en los distintos procesos de la minería gracias a la digitalización, los equipos de enlace móviles y la irrupción de ciertos protocolos como el IP.

Cuando se producen accidentes en este entorno **no queda otra opción que tratar de aprovechar los**

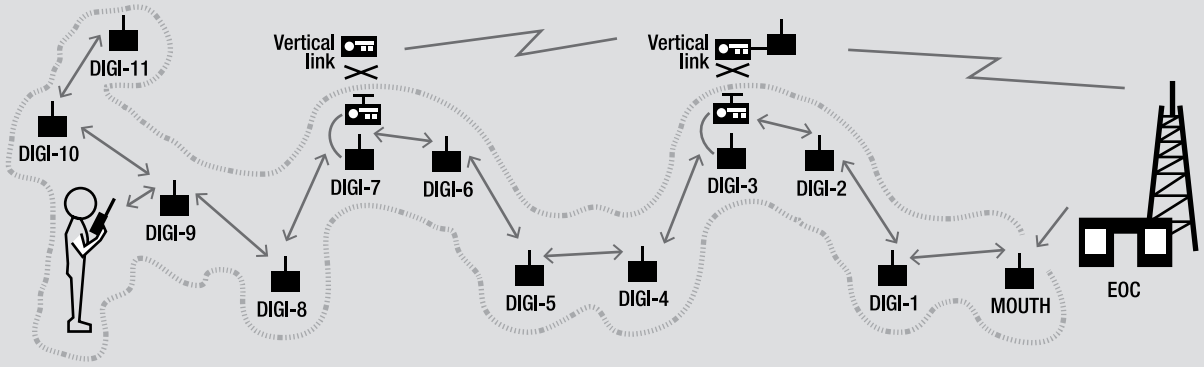
TELECOMUNICACIONES INALÁMBRICAS SUBTERRÁNEAS 1

Propagación por conductores metálicos existentes:

- Usa la infraestructura de explotación de la mina o túnel: cables de alimentación, rieles de transportes, cintas transportadoras, etc. En frecuencias: LF-MF.
- No se puede garantizar a priori el alcance de comunicación.

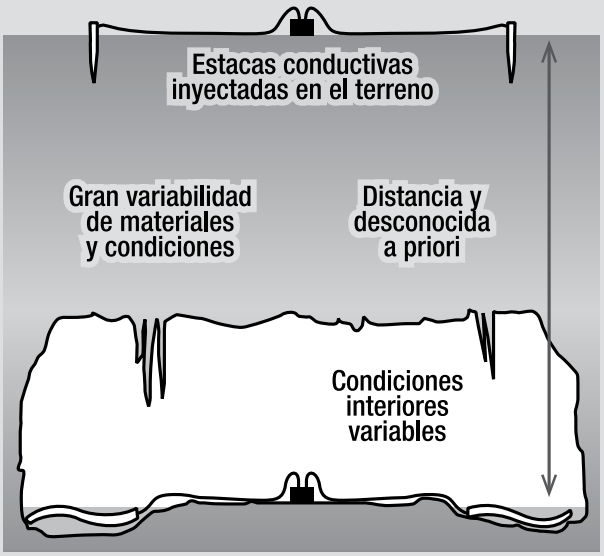
Redes Ad-Hoc:

- Autoconfiguración de red. Cada nodo es punto de acceso y enrutador.
- Frecuencias poco aptas para entornos subterráneos. (802.11, Zigbee, MESH).
- Necesidad de despliegue de muchos nodos intermedios en un medio muy hostil.



Propagación natural por túneles:

- Para túneles homogéneos de condiciones conocidas. (microondas > 1GHz).
- No apta para cuevas subterráneas (cambios de dirección, obstáculos…).



TELECOMUNICACIONES INALÁMBRICAS SUBTERRÁNEAS 2

- *Through-the-Earth* (a través de la tierra o la roca, TTE)
- Frecuencias menores (VLF-LF): mayor penetrabilidad
- Muy afectadas por infraestructuras metálicas
- Afectados por interferencias radio en equipos exterior
- Iluminación LED provoca interferencias en equipos interior
- Mínimo tiempo de instalación
- Técnica de Acoplamiento inductivo:
  - Alcances menores de 300 metros
  - Más seguro pero menos ancho de banda
- Técnica de Inyección de corriente:
  - Alcances en torno a 1000 metros
  - Más ancho de banda
  - Alcance muy dependientes del terreno
- No existe tecnología comercial
  - Prototipos precomerciales
  - Tecnología amateur y experimental

sistemas de telecomunicaciones supervivientes a la catástrofe. En las minas existen sistemas de comunicaciones de muy diversos tipos. **Alámbricos o filares,** incluyendo cables convencionales y fibra óptica. **Sistemas inalámbricos,** microondas, Wimax o Wifi. Y por supuesto equipos radio que van desde simples PMR UHF/VHF hasta las ya mencionadas radios Mesh. Todos ellos para asegurar el funcionamiento de una gama amplísima de sistemas de información de control de las plantas, controles de acceso, sistemas de telefonía, videovigilancia, videoconferencia y o incluso telepresencia[102]. Las soluciones de enlace para la minería están diseñadas para trabajar en condiciones extremas, porque en una mina existen altas concentraciones de polvo en suspensión, vibraciones producto de las explosiones y humedad, junto con la complejidad adicional de que, a gran profundidad, disminuye el oxígeno, y baja la temperatura considerablemente.

En las emergencias en minas destacan los **abrigos o refugios** a los que pueden acudir los mineros en caso de accidentes. Estos habitáculos están especialmente dotados de sistemas TIC para emergencias de los que poder valerse los supervivientes para contactar con la superficie y viceversa. Aparte de los sistemas depuradores de CO^2, suelen tener sistemas de telefonía o genéfonos[103] que están enlazados con los centros de supervisión de la mina. Incluso en ocasiones tienen hasta pequeñas **torres de ventilación** que pueden ser usados para la transmisión de mensajes, o como ocurrió en el derrumbe de la mina San José de Chile ocurrido en agosto de 2010, para el intercambio de testigos que llevaban en su interior mensajes escritos. También son muy conocidos los ya

102. La Telepresencia es una solución de videoconferencia con altas prestaciones de audio e imagen y que se presenta en unos entornos muy singulares de iluminación, mobiliario y domótica que permiten un fácil manejo intuitivo de los equipos así como favorecer un mejor contacto visual.

103. Los genéfonos para minería son un sistema telefónico que no necesita ni baterías ni alimentación eléctrica. Gracias a un micrófono y altavoz de altas prestaciones los genéfonos son capaces de establecer la comunicación sin necesidad de alimentación externa. La señal de llamada se genera a partir de una rueda dinamo situada en la parte inferior. El alcance se sitúa en torno a los 10 km.

mencionados ***Through-the-Earth* (a través de la tierra o la roca, TTE)** que son un tipo de radio que utiliza ondas de baja frecuencia que son capaces de atravesar la roca. La antena ocupa toda la superficie de la mina.

RESCATE EN CUEVAS

Hemos visto en el punto anterior que las comunicaciones son de gran importancia en cualquier actividad subterránea, y más si cabe en la minería. Cuando en la mina ocurre un accidente podremos usar lo que quede en funcionamiento del sistema de enlace previamente instalado. Sin embargo esto no ocurre en los salvamentos en cuevas, ya que previamente no había nada. Esto significa que si los espeleólogos que hay que sacar no tuvieron la idea de crear una "**línea de vida de telecomunicaciones**" para estar enlazados con el exterior, los rescatadores son los que tendrán que implementarla para llevar a cabo el rescate.

Aunque el uso de la radio es posible y existen equipos como los tratados en el apartado anterior que son capaces de atravesar la roca a muy baja frecuencia. Son los llamados **sistemas de campo inducido[104],** equipos radio que emplean el principio de campo inducido, en lugar de radiado, con lo que se evita la necesidad de incluir grandes antenas en el equipo. Esto quiere decir que **se utiliza el propio terreno que hay alrededor del equipo como antena,** donde se genera un campo electromagnético. La propagación de ondas a través de la roca depende de las propias características de la emisión. La penetración de la señal depende de la longitud de onda de la radiación, y suele ser una distancia equivalente a ésta. La frecuencia con la que trabajan los equipos de **87 KHz** implica una longitud de onda de 3.5 km en el aire. Debido a la reducción de velocidad de la señal dentro de un medio rocoso, la longitud de onda se reduce hasta una fracción de la original, que dependiendo del medio será mayor o menor, lo que da una penetración máxima en torno **a los 1000 metros** pudiendose alcanzar mayores distancias en condiciones ideales.

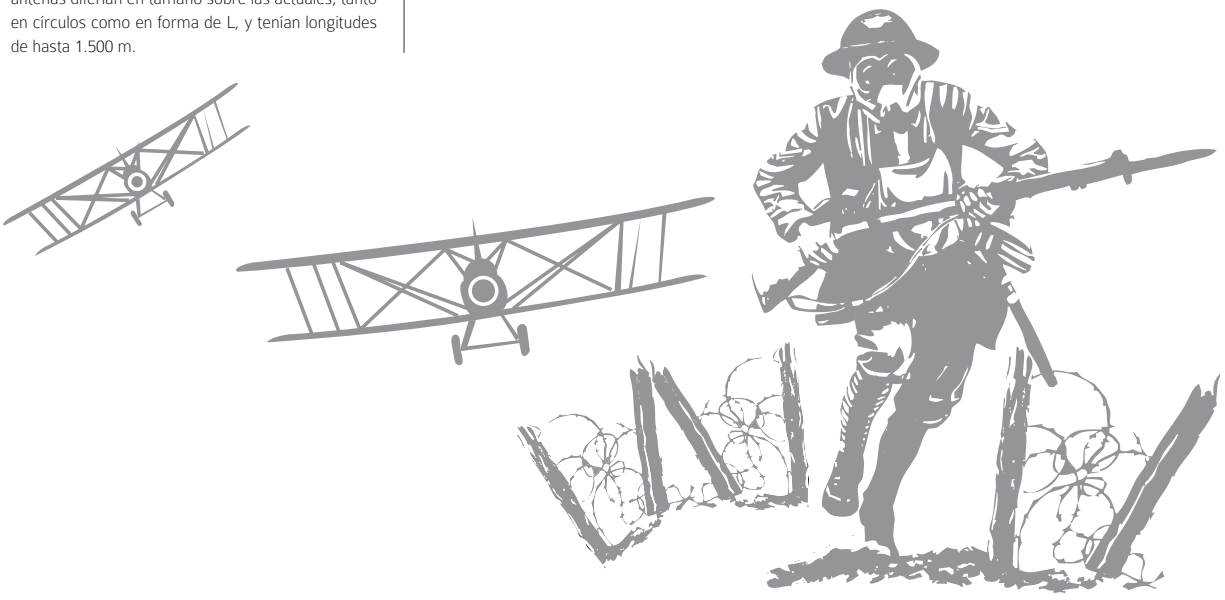
104. Tedra, Heyphone, Canary Link y Nicola son los sistemas más usados en la actualidad.

RADIOS DE CAMPO INDUCIDO

PRIMERA GUERRA MUNDIAL

La transmisión por radio a través de formaciones rocosas se utilizó por primera vez a principio del Siglo XX, durante la Primera Guerra Mundial. El sargento Ernest H. Hinrichs, americano de origen alemán destinado al frente francés en 1917, desarrolló el sistema y estuvo a cargo de las comunicaciones entre trincheras.

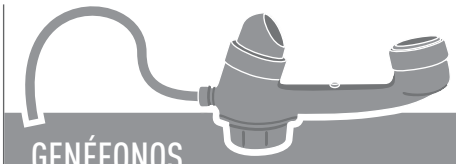
La transmisión se realizaba en el rango de frecuencias de 300 a 1.200 Hz., alcanzándose enlaces de hasta 3 km. a través de formación rocosa. Las antenas diferían en tamaño sobre las actuales, tanto en círculos como en forma de L, y tenían longitudes de hasta 1.500 m.



Lo más normal es hacer **uso del cable** para asegurar el enlace con el exterior. Esto es un trabajo sumamente costoso ya que implica ir tendiendo cable durante todo o gran parte del recorrido del equipo que ha entrado en la cavidad. Se puede emplear **telefonía convencional de dos hilos, telefonía de un hilo con retorno por tierra y genéfonos.** Los equipos de rescate pueden usar radio portátiles para enlace dentro del equipo que entra en la cueva, aunque no para hablar con el exterior.

En el caso de usar **tendidos genefónicos**[105] se establecerá una base radio en la boca de la cueva y se tenderá la línea, tratando que este tendido no coincida con las zonas de paso. El uso frecuente de retenciones será clave para la supervivencia de la línea. El corresponsal en la entrada de la cueva será el encargado de retransmitir vía radio normalmente la información desde el interior a los responsables que se encuentren en el puesto de mando.

Al igual que ocurre con las comunicaciones en edificios y en minas se empieza a utilizar la **tecnología MESH** dentro de las galerías para enlazar rescatadores con el puesto de mando del rescate que se monta a la entrada de la cueva.



GENÉFONOS

El genéfono está pensado para su conexión fija a un cable de comunicación de dos hilos o bien mediante conexiones rápidas móviles que pueden ser de dos tipos:

- Por pinza, donde la conexión se realiza de forma instantánea y en cualquier punto del cable de comunicación mediante una pinza y un cable de comunicación especial plano de dos hilos.
- Por conector, donde la conexión se realiza de forma instantánea mediante un conector a unas bases fijas situadas a lo largo del cable de comunicación.

RESCATE EN TÚNELES

Aunque en España la Ley 2/1985 sobre Protección Civil define, en sus artículos 5 y 6, aspectos importantes a la hora de abordar los planes de emergencia en túneles, no fue hasta el accidente del túnel de Mont-Blanc[106], ocurrido el 24 de marzo de 1999 con un resultado de 39 personas fallecidas cuando las autoridades nacionales empezaron a tomar conciencia de la importancia de estas emergencias. La normativa vigente obliga a las empresas constructoras a implementar diferentes tipos de **sistemas de enlace que garanticen la seguridad de las personas** que transiten por el túnel.

En las emergencias que tienen lugar en túneles las telecomunicaciones juegan un papel crítico y fundamental, por lo que son muchos los sistemas que podemos encontrar en su interior. Prácticamente todos los sistemas de enlace utilizados se basan en las TIC, que deben reunir unos requisitos concretos para que dichos sistemas sigan funcionando cuando se produzca un accidente en su interior.

Cualquier incidente menor puede derivar en incendio. Los túneles, al ser cavidades muy aisladas del exterior, presentan el problema de la dificultad de eliminación del **calor, el humo y las sobrepresiones,** que se pueden llegar a generar durante un incendio dando lugar a los efectos llamados "**horno**[107]" y "**cañón**[108]". Una vez más la información se vuelve clave y la comunicación entre intervinientes y **Centro de Control del túnel** tiene que estar garantizada, por lo que se deben cumplir de manera taxativa unas características en las comunicaciones implantadas:

- Protección: Los sistemas instalados si no reúnen por si mismos las funcionalidades de trabajo en situaciones extrema, se les debe proteger para que sí lo hagan. Es decir los sistemas de interfonía, videovigilancia, control de luces y paneles informativos, equipos radio de emergencias, etc, estarán dotados de envolventes anti-deflagrantes, los cables estarán dotados de cubiertas ignífugas, con baja emisión de humos y cero halógenos. Los postes de emergencia por ejemplo contarán con sistemas de alimentación ininterrumpida (SAI).

105. Se prefiere el uso del genéfono al teléfono por la influencia que las condiciones interiores de la cavidad tiene sobre las baterías.

106. A raíz del accidente se creó una comisión que elaboró un amplio informe sobre las circunstancias del accidente dando 41 recomendaciones. De estas hay dos referidas a las TIC:

- Recomendación n° 10. La explotación del túnel debe ser dirigida desde un centro único de control, equipado con sistemas informáticos y de comunicaciones, necesarios a las circunstancias de la infraestructura.
- Recomendación n° 12. Los elementos de medida y sistemas de alerta disponibles deberán reportar una idea de la situación real, en cada momento, en la gestión del túnel y mantener un sistema eficaz de comunicación que permita la fluidez del tráfico en el interior del túnel.

107. Efecto horno. Consiste en la acumulación progresiva del calor, que se traduce en un aumento continuado de la temperatura. Se le denomina efecto horno, porque la situación es muy parecida a lo que ocurre con el horno de una cocina (pero siendo los usuarios, en el caso del túnel, los que pueden llegar a terminar asados).

108. Efecto cañón. Éste se presentará, cuando se produzcan explosiones. La sobrepresión generada por la explosión en el interior del túnel, sólo puede liberarse hacia ambos lados a partir del punto de origen de dicha explosión. No es difícil imaginar, que existiendo sólo una cavidad lineal, ésta, se comportará como si fuera el cañón de una escopeta.

- Redundancia: tal y como ya hemos dicho en otros capítulos del libro, hablando de telecomunicaciones la redundancia es necesaria para garantizar el servicio en las peores circunstancias. El coste es elevado pero a la postre es rentable. Se puede optar por sistemas alternativos muy fiables y de bajo precio. Un ejemplo puede ser el de la Telefonía de bomberos en túneles de Metro de Valencia (FGV), en la que se optó por un sistema de back up sobre cable de cobre, sencillo de manejo en situaciones de pánico, y donde además se hizo el tendido del cableado por una ruta alternativa a la del propio túnel.

Aunque el confinamiento hace guardar alguna característica común con los accidentes en cuevas y minas, la linealidad de la cavidad facilita en cierto modo las comunicaciones de los intervinientes en las emergencias. El papel estrella es desempeñado por los **Centros de Control,** que en los túneles más modernos se desdoblan en primario y secundario en bocas diferentes. Además los túneles ya están dotados de **sistemas de comunicaciones pensados específicamente para coordinar las situaciones de emergencia**, enlazados permanentemente con los Centros de Control. Estos son los de megafonía de emergencia (diferenciado por cada zona del túnel), sistemas de interfonía SOS[109], paneles[110] indicadores para señalización de salidas seguras, cables radiantes[111] y circuitos cerrados de televisión con todo tipo de cámaras (estándar, infrarrojas, intensificadores de luz, etc.).

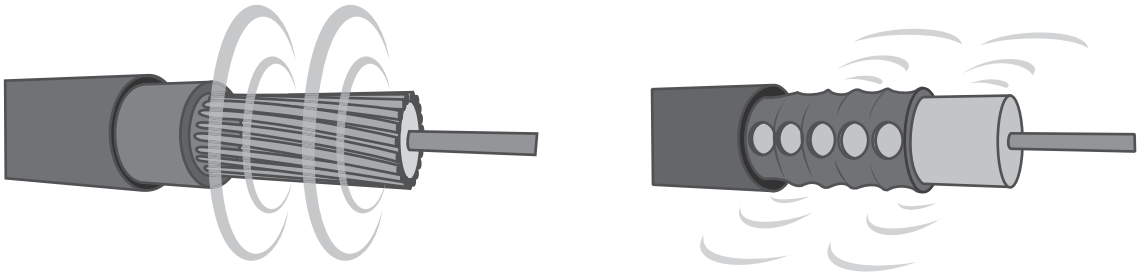
Hoy día incluso los usuarios pueden llamar al 112 desde su teléfono móvil. Los túneles están provistos de miles de metros de cable de fibra óptica, además de sistemas de retransmisión de señales de radio, que permiten escuchar en el interior las principales emisoras comerciales. En caso de emergencia, éstas serán interrumpidas para la emisión de instrucciones desde el centro de control. También existen repetidores de los sistemas radio trunking TETRA/TETRAPOL que los equipos de emergencia de esa zona utilicen.

Y por supuesto que los equipos de intervención con sus Responsables TIC a la cabeza deberán agudizar el ingenio para mejorar las comunicaciones radio o establecer tendidos de cable ad hoc que garanticen la seguridad de los intervinientes y el flujo de información hasta el Centro de Control o el Puesto de Mando que se establezca provisionalmente a la entrada del túnel.

Entre los "trucos radio", que por supuesto podemos aplicar indistintamente en minas, cuevas o túneles, podemos encontrar los siguientes:

- Inclinar la antena de la radio hasta poner la antena paralela al suelo para ganar alcance dentro el túnel.
- Aumentar potencia de transmisión.
- Cambiar antenas dentro del túnel por otras de mayor sensibilidad.
- Utilización de integradores **radio-hilo**[112].
- Instalación de repetidores para asegura el enlace desde la zona de la intervención hasta la boca del túnel.

COMUNICACIONES EN TÚNELES



109. Además de los postes unidos por teléfono vía cable a los Centros de Control, existen en el mercado radios fijas, situadas en postes que trabajan en la banda de 2,4 GHz, que se pueden usar en situaciones extremas en las que un siniestro puede inutilizar todas las redes de cable (principales y redundantes). Funcionan con una batería local por poste en caso de caída de la red eléctrica, ofreciendo una autonomía entre 2 y 5 horas. El problema suele ser la no existencia de un terminal en el punto crítico del siniestro.

110. Estos paneles llevan una doble conexión, vía cable y vía Wifi con el Centro de Control.

111. El cable radiante se asemeja a un cable coaxial con pequeños orificios para radiar en forma transversal las señales de radiofrecuencia a lo largo del cable que se extiende por toda la longitud del túnel como si este fuera una antena muy larga. Estos sistemas se utilizan principalmente para radiocomunicación VHF y UHF. El cable radiante VHF radia las ondas de radiofrecuencia de manera omnidireccional, es decir, 360 grados alrededor del cable pero tiene el inconveniente de que debido a su poco blindaje, se induce más ruido, se requieren más repetidores y sólo puede manejar frecuencias hasta los 200 MHz. En cambio el cable radiante UHF, radia las ondas de radiofrecuencia por los costados, dando como resultado un mayor blindaje, hay menor ruido en la señal y soporta señales de mayor frecuencia hasta 1.000 MHz, estas cualidades lo hace el medio de comunicación ideal para transmitir señales de radio de mayor frecuencia, de menor longitud de onda y que tienen un mayor poder de penetración haciéndolo entre 100 y 200 veces más eficiente que el cable radiante VHF.

112. La integración radio hilo permite asegurar el enlace entre intervinientes que usan radio fuera del túnel y los que ya dentro del túnel trabajando en la zona del incidente que usarán teléfono o genéfono vía cable. Se debe realizar un tendido de cable entre entrada del túnel y el incidente. En la boca del túnel se colocaría el integrador radio.

CABLES RADIANTES

El Sistema de Cable radiante en VHF y UHF puede retransmitir dentro del túnel de una mina o una autopista o en general cualquier túnel, los canales VHF/UHF de radiocomunicación de algunos servicios de emergencia de protección civil, la Cruz Roja o bomberos.

Se instalan amplificadores que se conectan en serie a lo largo del túnel para amplificar cada 350 metros, hasta un máximo de 3 ó 4 km. A partir de aquí se instala una nueva fuente para volver a amplificar la señal hasta un límite cercano a los 200 km.

EMPLEO DE INTERNET Y REDES SOCIALES

Internet es útil para casi todo. Bueno, por qué no decirlo, es útil siempre, y sobre todo en situaciones de emergencia. La combinación de cualquier medio de enlace y la web es una herramienta potente que debidamente gestionada nos permitirá agilizar nuestro trabajo como Responsables TIC. Desde búsqueda de información meteorológica, pasando por consulta de bases de datos específicas, hasta el mantenimiento del contacto con nuestros seres queridos en nuestro país de procedencia, son miles las posibles aplicaciones a nuestro alcance.

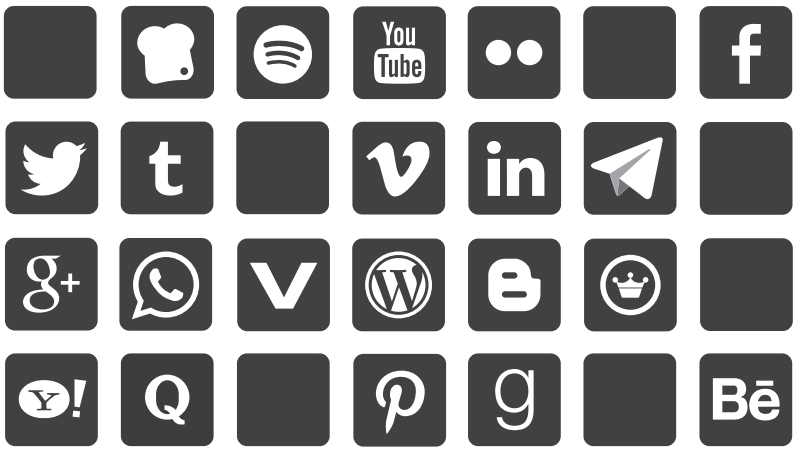
No es foro este libro para concienciar al lector sobre los problemas de seguridad en la red de redes, pero sí que tenemos que poner el acento en la problemática que supone el manejo de datos sensibles, y sobre todo la repercusión que tendrá en nuestras operaciones el uso indebido de esta información. Muchos de los datos que circulan tras una catástrofe natural pueden ser utilizados para **sembrar el pánico entre la ciudadanía.** No queremos decir con esto que no se use internet, sino que se use con cabeza.

Si añadimos a nuestro autocontrol, dosis de tecnología, haciendo uso de páginas web seguras, firmas digitales en nuestros documentos, el resultado será francamente superior.

Tampoco podemos confiar todas nuestras comunicaciones a internet como único método de enlace. Lo primero porque estaríamos incumpliendo una de las reglas del planeamiento que un Responsable TIC debe mantener a toda costa, es decir, tener siempre algún medio alternativo o de respaldo al principal. Y en segundo lugar porque la capacidad de la red no es ilimitada. A medida que un volumen cada vez mayor del tráfico se traslada a Internet, se corre el riesgo de la **saturación y de caída de servicios.**

Los servicios que se pueden prestar en internet en las fases previas de una emergencia son por todos conocidos. Cuando se intuye algún problema los internautas acuden a las páginas especializadas ávidos de información que llevarse a sus pantallas. Existen algunos ejemplos. En los Estados Unidos, los servidores que facilitan información sobre las tormentas del Centro Nacional de Huracanes y la Administración Nacional Oceanográfica y Atmosférica quedaron fuera de servicio el año 2.008 al recibir millones de consultas simultáneamente cuando se acercaba una tormenta. En

REDES SOCIALES Y EMERGENCIAS



SITIOS DE INTERNET RELACIONADOS CON EMERGENCIAS

- **Reliefweb**
  www.reliefweb.int
- **Prevention Web**
  www.preventionweb.net
- **Organización Mundial de la salud**
  www.who.int
- **Centro Regional de Información sobre Desastres en América Latina y El Caribe**
  www.crid.or.cr
- **Red de Información Humanitaria para América Latina y El Caribe**
  www.redhum.org
- **Organización Panamericana de la Salud. Área de Preparativos para Situaciones de Emergencias y Socorro en Casos de Desastres**
  www.paho.org/desastres
- **Centers for Disease Control (CDC)**
  www.cdc.gov
- **Estrategia Internacional para la Reducción de Desastres**
  www.eird.org
- **Oficina de Coordinación para Asuntos Humanitarios de las Naciones Unidas**
  www.ochaonline.un.org
- **Federación Internacional de Sociedades de la Cruz Roja y la Media Luna Roja**
  www.cruzroja.org
  www.ifrc.org
- **European Union Humanitarian Aid and Civil Protection Portal ERCC (Emergency Response Coordination Centre)**
  ercportal.jrc.ec.europa.eu

España cada CCAA y la propia Dirección General de la Protección Civil y Emergencias (DGPCyE), disponen de sus **portales web informativos.**

Sin embargo todavía no son muchas las que se han decidido por adentrarse en el mundo de las **redes sociales.** Desde Facebook o Twitter se podría informar de posibles accidentes y catástrofes, o incluso se puede ayudar a la gestión de acciones informativas a la población. Un estudio del Instituto de Geofísica de los Estados Unidos (USGS) ha demostrado que el uso de Twitter en caso de catástrofes naturales es mucho más eficaz que la información web, y hasta 20 minutos más rápido que el uso de SMS o la radio. El USGS mantiene en desarrollo diversos experimentos en la Bahía de San Francisco para estudiar cómo se producen las telecomunicaciones por Twitter en caso de emergencia y cómo se difunden los mensajes de alerta y prevención que puedan estar dictados por un organismo oficial que coordine las tareas "post catástrofe".

En el terremoto de Chile del 27 de febrero de 2010 también se abrió una interesante **discusión sobre el rol jugado por las redes sociales.** Tanto Twitter como Facebook se transformaron en valiosas fuentes con las últimas novedades que acontecían después del terremoto. La red se llenó de personas privadas que contactaban con familiares para contar que estaban bien, otros para buscar a gente desaparecida, canalizar ayuda y reproducir la información de prensa con la que se contaba en ese momento. También las instituciones relacionadas con la gestión de la crisis, como la Oficina Nacional de Emergencia del Ministerio del Interior (ONEMI) y diferentes Ministerios entregaban información oficial a través de sus cuentas en redes sociales[113].

El más reciente caso de catástrofe natural se dio con el **huracán Sandy, en Nueva York.** En total, se enviaron más de 20 millones de mensajes en twitter relativos a la tormenta. Las palabras "sandy" y "hurricane" fueron las más utilizadas en esa red social. Ya hemos hablado de internet como plataforma recaudatoria para beneficio de los damnificados. Por ejemplo con Sandy se lanzaron **Tweets Patrocinados** para @RedCross (cuenta de la Cruz Roja norteamericana), @FEMA, (Agencia Federal para la Gestión de Emergencias), @NYCMayorsOffice y muchas otras cuentas gubernamentales.

Otro ejemplo de uso correcto y de la flexibilidad que puede ofrecer internet se produjo con la iniciativa que tomaron las operadoras Vodafone y Telecom Italia tras los terremotos de L'Aquila de 2009. Pidieron a sus clientes que **abrieran sus redes Wifi domésticas,** de modo que cualquier persona en situación de emergencia se pudiera conectar desde una tableta o un móvil, ya que las infraestructuras de telefonía móvil habían quedado muy dañadas.

113. Según un estudio de SocialMetrix, empresa especialista en el estudio de redes sociales, analizó la información contenida en este sitio entre el 27 de febrero y el 2 de marzo de 2010. En su búsqueda de tweets relacionados con Chile, terremoto, búsqueda de personas, ofrecimiento o petición de ayuda, SocialMetrix detectó que 7.380 usuarios se involucraron, generando más de 23.313 tweets donde aparecía la palabra Chile, 8.965 donde el tema principal fue la búsqueda de personas y 8.240 relacionados con ayuda a las zonas afectadas.

114. La Resolución N° 640 y la Recomendación M.1042 de la UIT reconocen formalmente el valor de este recurso.

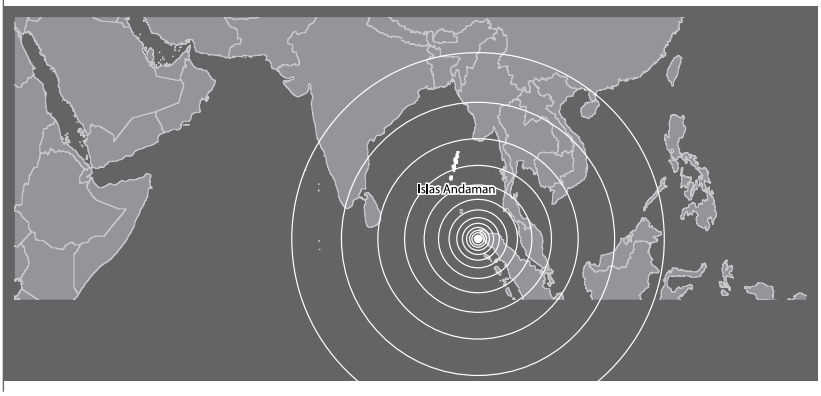
115. Algunos ejemplos de intervención de radioaficionados:
- Terremotos: Nicaragua (1972), Guatemala (1976), Italia (1976 y 1980), Rumania (1977), India (1979), Argelia (1980), México (1985), la Unión Soviética (1988), Filipinas (1990), los Estados Unidos (1964, 1989 y 1994).
- Inundaciones: Honduras (1977) India (ruptura de dique en 1979), Estados Unidos (1977, 1986, 1990 y 1993).
- Erupciones volcánicas: Estados Unidos (1980), Colombia (1985).
- Tornados: Canadá (1987), Estados Unidos en varias ocasiones cada año.
- Vertidos químicos: Mississauga, Canadá (1979).

RADIOAFICIONADOS TSUNAMI 26 DE DICIEMBRE DE 2004 OCÉANO ÍNDICO

Un grupo de radioaficionados de la India organizó a finales del 2004 un viaje de estudios a las Islas Andaman. El destino quiso que estuvieran transmitiendo desde allí cuando se produjo el tsunami en diciembre de 2004.

El equipo portátil que utilizaron para dar a las estaciones de radioaficionados del mundo entero la posibilidad de ponerse en contacto por primera vez con las Islas Andaman, al ser el único equipo que seguía funcionando después de que se produjo la catástrofe.

Una vez movilizada la ayuda exterior, los primeros equipos de socorro establecieron sus propias comunicaciones y otras estaciones de radioaficionados fueron enviadas a islas vecinas. Las estaciones de radioaficionados siguieron funcionando como el único enlace para todas las personas que deseaban ponerse en contacto con amigos o parientes en el extranjero.



RADIOAFICIONADOS

Un clásico. Es un **Servicio de Radiocomunicaciones** recogido en el Reglamento de Radiocomunicaciones de Ginebra de 1998. **La Unión Internacional de Radioaficionados** (IARU), que es la federación de las asociaciones nacionales de radioaficionados que existen en la mayoría de los países, representa los intereses del Servicio de Radioaficionados en la Unión Internacional de Telecomunicaciones[114] (UIT) y en las conferencias internacionales.

Históricamente, los radioaficionados fueron los primeros en poner a disposición de los gobiernos sus redes de comunicaciones locales durante los desastres e inmediatamente después de ocurridos estos.

Un **radioaficionado** según la RAE es una persona autorizada que emite y recibe mensajes radiados privados, usando bandas de frecuencia administrativamente establecidas. Son un **ejemplo de cómo una simple afición alcanza cotas de eficacia extremas** en situaciones de catástrofe. Son cientos los ejemplos[115] en los que la participación de radioaficionados ha salvado la coordinación de las acciones en una emergencia. El radioaficionado, debidamente entrenado con anterioridad, presta sus servicios en los casos en que las comunicaciones normales sean insuficientes, estén saturadas o fuera de servicio. Lo hace en cualquier tipo de banda y con multitud de equipos. Desde radios de LF hasta comunicaciones vía satélite.

El paso del hobby (radioafición) al compromiso (comunicaciones de emergencia) es muy significativo y requiere ante todo compromiso. Es complementar la aptitud alcanzada con el entrenamiento y conocimiento de los medios, con la actitud, entendida como la voluntad para encarar las actividades que se tienen que desarrollar en el transcurso de una emergencia. Es decir, esto significa que se espera mucho más de un operador de comunicaciones de emergencia que simplemente conectar un equipo y transmitir.

En España es la **Orden ITC/1791/2006 sobre Reglamento de Radioaficionados** la que regula su funcionamiento.

Son dos los tipos de redes de radiocomunicaciones del servicio de radioaficionados que pueden encontrarse en las operaciones de socorro. **Redes de corto alcance** basadas en VHF y UHF que facilitan las comunicaciones tácticas y operativas en el sitio de la catástrofe y sus alrededores. **Redes de medio y largo alcance,** basadas en HF fundamentalmente, que ofrecen enlace desde el sitio de la catástrofe hasta Centros de Coordinación fuera del área afectada, con las sedes de los organismos intervinientes, o con organismos internacionales. En este último tipo variará la antena y el tipo de propagación seleccionada para cambiar entre el medio[116] y el largo alcance.

Como alternativa a los equipos radio encontramos los llamados **satélites de radioaficionados,** que son probablemente la disciplina menos conocida de ellos. En este momento el servicio de radioaficionados no funciona con satélites geoestacionarios ni constelaciones de satélites propios por lo que de momento no pueden ofrecer una cobertura mundial constante, pero se espera una gran evolución en los próximos años.

En caso de emergencia las estaciones del servicio de radioaficionados pueden ser contactadas por estaciones de otros servicios como por ejemplo las del servicio marítimo o del servicio aeronáutico que veremos más adelante en este mismo capítulo.

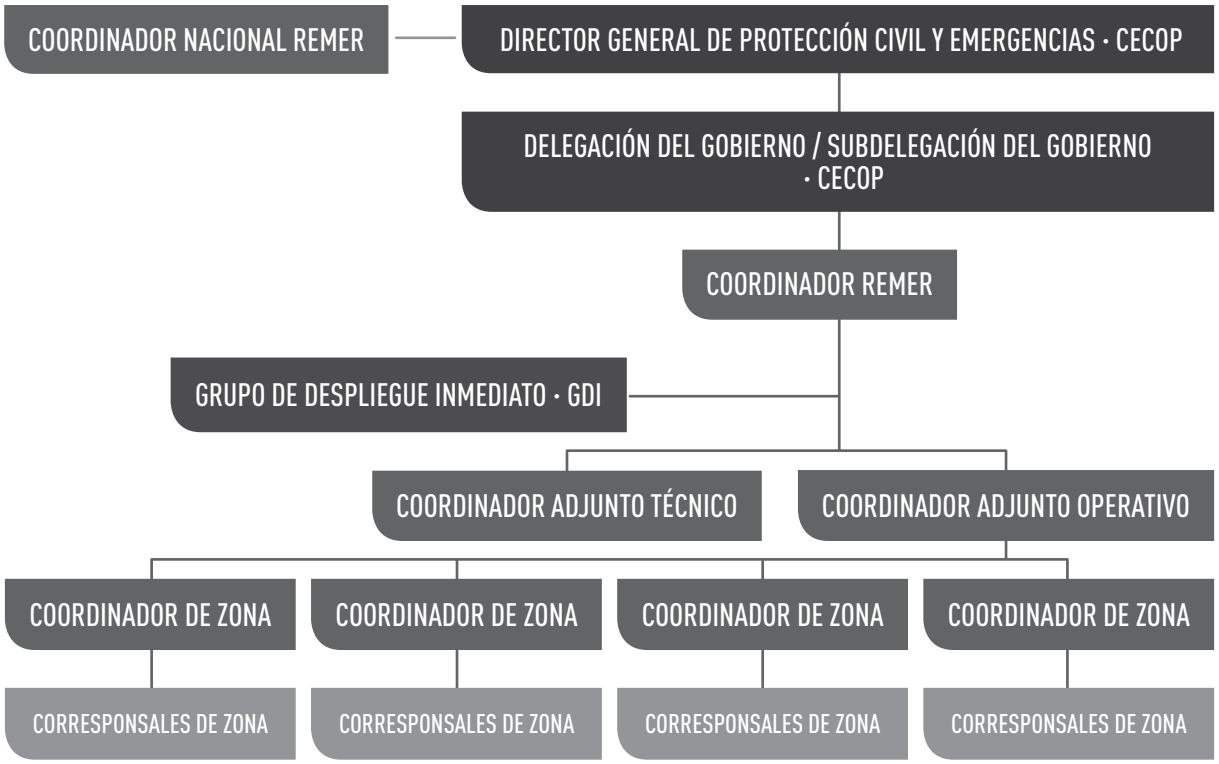
Los modos de comunicación empleados son: radiotelegrafía, comunicación de mensajes, enlaces de datos en la banda de ondas decamétricas, radiocomunicaciones de paquetes fuera de línea, radiotelefonía en banda lateral única con portadora suprimida, modulación en frecuencia y comunicación de imágenes vía fax o televisión.

Aunque la mayoría de ellos pertenecen a grupos organizados y muestran un gran sentido de la disciplina y la responsabilidad, **la exactitud de su información puede ser muy variable.** Para evitar el peligro de que se transmitan informaciones inexactas, no confirmadas o no fidedignas, es necesario desarrollar una coordinación directa y estrecha entre estos grupos y los responsables de las telecomunicaciones de emergencia. En la mayoría de los países, los radioaficionados obtienen sus **licencias del gobierno** y suele ser muy restrictiva su obtención.

En todo momento hay alguna emisora disponible que puede erigirse protagonista en una emergencia. Independientemente de los recursos adicionales que se pudieran movilizar, existen los llamados **grupos del servicio de emergencia de radioaficionados o ARES,** que están formados por aficionados que han obtenido su licencia y se han registrado voluntariamente para prestar servicios durante una catástrofe.

116. Se pueden establecer comunicaciones a distancias medias de 60-150 km. mediante la propagación por ondas ionosféricas con incidencia casi vertical (NVIS) en la parte inferior de la banda de frecuencias de ondas decamétricas hasta unos 7 MHz.

REMER: ORGANIZACIÓN BÁSICA



En nuestro país tenemos que hablar de la **REMER**, explicada en detalle en uno de los anexos de este libro. La **Red Radio de Emergencia** de la Dirección General de Protección Civil y Emergencias (DGPCyE), es la organización formada por cerca de 7.000 radioaficionados españoles encargada de ayudar en los casos de catástrofe.

SERVICIO DE RADIOCOMUNICACIONES MARÍTIMAS

La Conferencia de los Gobiernos firmantes del **Convenio Internacional para la Seguridad de la Vida Humana en el Mar (SOLAS)** de 1974, aprobó el 9 de noviembre de 1988 una serie de enmiendas referentes a las radiocomunicaciones para el Sistema Mundial de Socorro y Seguridad Marítimos (SMSSM) que regula su propio sistema de comunicaciones de emergencia entre embarcaciones y centros costeros de salvamento marítimo.

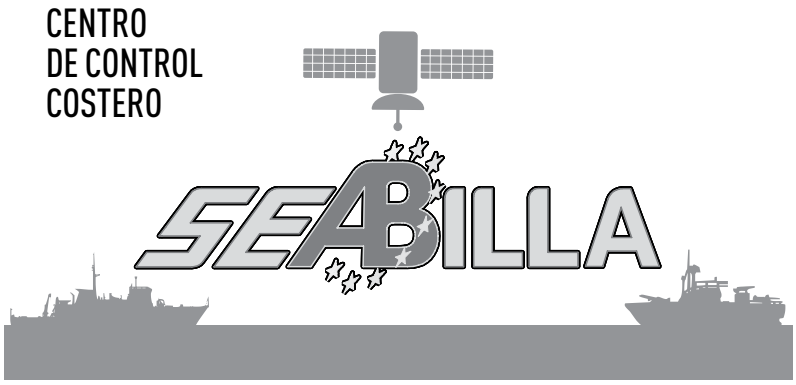
Los barcos en la mar mantienen enlace permanentemente con la línea marítima a la que pertenecen mediante servicios telefónicos por satélite, fundamentalmente Inmarsat, o a través de estaciones costeras radioeléctricas VHF y HF costeras.

El servicio de radiocomunicaciones marítimas utiliza frecuencias en canales definidos dentro de las bandas de frecuencias que se le han atribuido. Los modos de comunicación son la **fonía (voz) y los datos.** El télex solía ser muy común, pero el correo electrónico está sustituyendo cada vez más esta forma de mensajes escritos.

Si resulta necesaria la comunicación con estaciones del servicio marítimo en una situación de emergencia, esa explotación está autorizada en virtud de la regla general que permite la utilización de todos los enlaces de telecomunicaciones disponibles para el tráfico de emergencia. Incluso dado el momento se podría incluso comunicar con buques que transportan suministros de socorro.

Estas estaciones costeras ofrecen diferentes servicios a los barcos como **integraciones radio-hilo** para integrar, normalmente en VHF, las comunicaciones radio de los barcos con las líneas telefónicas de las redes públicas RTPC. Por lo general, las estaciones costeras aceptan el tráfico relacionado con las situaciones de catástrofe y emergencia, aunque éstas se estén desarrollando en tierra.

Son diferentes los procedimientos que se emplean. Lo más sencillo es mantener un contacto permanente con alguna red de teletipos a través de satélite, aunque todavía existen redes de radiodifusión. Hoy día además es frecuente que los barcos cuenten con correo electrónico en alguna estación costera, generalmente mediante un **sistema de almacenamiento y retransmisión** vía HF o satélite.



En España es el **Real Decreto 1185/2006**, de 16 de octubre, por el que se aprueba el Reglamento por el que se regulan las radiocomunicaciones marítimas a bordo de los buques civiles españoles. En él se definen según el tipo de barco los equipamientos de telecomunicaciones que deben estar instalados y certificados antes de salir al mar.

Estos barcos llevan una serie de **sistemas de enlace permanentemente activados** en aras de la seguridad de los tripulantes. Para las comunicaciones de corto alcance (entre 10 y 25 km.) la frecuencia normalizada de los servicios de socorro en la banda de ondas métricas es **156,8 MHz.** La ley exige que los barcos hagan **escucha 24 horas del día** en esta frecuencia.

Los barcos suelen disponer también de un **sistema automático de llamada selectiva denominado DSC** en el canal 70 de la banda de ondas métricas. Para utilizar este servicio, se necesita el código de **identidad del servicio móvil marítimo (MMSI) del barco.** El MMSI es el número que identifica a cada estación de barco a efectos de seguridad y radiocomunicaciones, y que debe ser programado en los equipos automáticos de radiocomunicaciones de llamada selectiva digital de los buques (VHF, MF y HF) y en las radiobalizas por satélite del **sistema Cospas-Sarsat**[117]. Además, las estaciones costeras también tienen un MMSI. Este código se asigna junto con el distintivo de llamada de la estación.

SISTEMA DE VIGILANCIA MARITIMA

El proyecto SEABILLA es un proyecto de la Unión Europea, dentro del Séptimo Programa Marco que tiene por objeto definir una arquitectura eficiente en coste para los sistemas de vigilancia marítima europea, integrando segmento espacial, terrestre, marítimo y aéreo, e incluyendo los sistemas actualmente ya desplegados.

Una de las ideas es aplicar soluciones innovadoras para incrementar las capacidades de los sistemas de vigilancia actuales y de telecomunicaciones entre buques y estaciones costeras para contribuir a desarrollar y mejorar los sistemas de detección, identificación y seguimiento de barcos sospechosos.

117. En los buques nacionales, la radiobaliza de localización de siniestros por satélite de Cospas-Sarsat de 406 MHz, de activación automática, deberá estar instalada en la misma cubierta del puente de navegación.

SERVICIO DE RADIOCOMUNICACIONES AERONÁUTICAS

Lo que ya se ha dicho más arriba sobre el enlace en situaciones de emergencia con respecto al servicio de radiocomunicaciones marítimas se aplica en su mayor parte también al servicio aeronáutico. El servicio de radiocomunicaciones aeronáuticas dispone de sistemas específicos radio, telegráficos y telefónicos para establecer comunicaciones con las aeronaves y entre ellas y las estaciones terrenas, normalmente torres de control aeronáutico. Además disponen de frecuencias concretas para **equipos de radionavegación** utilizados cuando se realizan vuelos en instrumental[118].

El servicio aeronáutico dispone de **estaciones aeronáuticas terrestres** a lo largo de todo el mundo, similares a las de las estaciones de radiocomunicaciones marítimas que existen a lo largo de las costas descritas anteriormente. Estas emisoras tienen a su cargo el **Servicio Móvil Aeronáutico,** es decir, el servicio de radiocomunicación establecido entre una estación fija aeronáutica (operando generalmente en aeropuertos y aeródromos civiles o militares) y una aeronave en vuelo. Se utilizan para transmitir informaciones operacionales sobre los vuelos entre los pilotos y sus bases, pudiendo realizar integraciones radio-hilo con la red telefónica pública. En caso de accidente aéreo, proveen las medidas necesarias para una rápida búsqueda y salvamento de los posibles sobrevivientes.

El Servicio Móvil Aeronáutico opera en onda corta (HF) entre las siguientes frecuencias asignadas por la Unión Internacional de Telecomunicaciones:

2.850 a 3.025 KHz	3.400 a 3.500 KHz	4.650 a 4.700 KHz	5.450 a 5.680 KHz
6.525 a 6.685 KHz	8.815 a 8.965 KHz	10.005 a 10.100 KHz	11.275 a 11.400 KHz
13.260 a 13.360 KHz	17.900 a 17.970 KHz	21.924 a 22.000 KHz	

También opera en la llamada "**Banda Aeronáutica**" en VHF-AM entre 117,975 y 136 MHz siendo utilizada esta banda para las comunicaciones aeroterrestres en las proximidades de los aeropuertos en donde se hallan situadas las estaciones fijas. En caso aeronaves militares también usan la banda UHF.

Las aeronaves llevan diferentes equipos para materializar el enlace con tierra. Van desde modernos **equipos satelitales** con capacidad de enlace en movimiento (SOTM-Sat on the move), a las clásicas **radios**. En la Banda Aeronáutica predominando el trabajo en modulación **AM**, en contraposición a las que se utilizan en tierra que trabajan en FM.

También existen aeronaves, tanto helicópteros como aviones que van dotados de radios **HF**[119] para cubrir grandes distancias, aunque no es del gusto de los pilotos por el ruido existente en esta banda. Las radiocomunicaciones aeronáuticas en la banda de HF poseen a menudo un **sistema de llamada selectiva (SELCAL)**, que funciona como una especie de sistema de radiomensajería y permite a la tripulación ignorar las llamadas que no se dirigen específicamente a ella. Cuando se detecta una llamada para la aeronave el sistema la pasa a los cascos de la tripulación automáticamente.

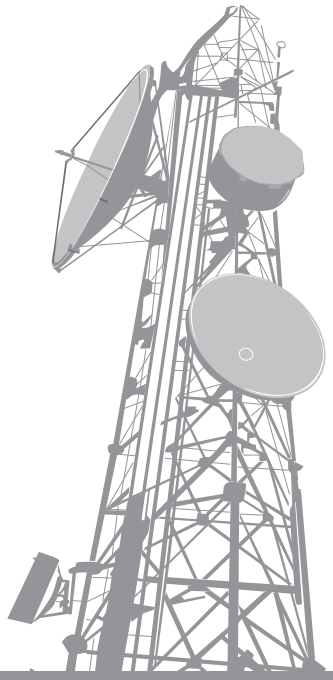
Por ejemplo en una emergencia de gran calado es normal utilizar la vía aérea para cubrir necesidades logísticas de lugares remotos o aislados lanzando suministros con paracaídas. En este caso se tendría que hacer uso de los llamados **equipos de radiocomunicaciones de banda aérea,** que no

118. El Vuelo Instrumental o IFR *(Instrumental Flight Rules)* son el conjunto de normas y procedimientos recogidos en el Reglamento de Circulación Aérea que regulan el vuelo de aeronaves con base en el uso de instrumentos para la navegación, lo cual implica que no es necesario tener contacto visual con el terreno, como ocurre en el Vuelo Visual (o VFR -*Visual Flight Rules*). Este IFR permite el vuelo de aeronaves cuando la capacidad de los pilotos está reducida para ver y evitar colisiones. Para ello, los controladores aplican criterios de separación entre aeronaves mediante el cálculo de tiempo, de las distancias y de las velocidades entre los mismos. Obtienen tales datos de dos modos: bien mediante la velocidad, la altura, el rumbo o la posición que les transmite el piloto, bien mediante la pantalla de radar, que obtiene esos mismos datos gracias a un emisor de radio en la aeronave llamado transpondedor. También los pilotos se valen de las cartas de navegación aeronáutica para saber su posición.

119. Suelen trabajar en Banda Lateral Superior.

deja de ser una radio con canales compatibles con los del avión. Si la emergencia está relacionada con el siniestro de una aeronave, es el SAR (Search and Rescue) quien debe enviar un medio aéreo, atraves del RCC (Rescue Coordination Center).

Los helicópteros últimamente montan **sistemas telefónicos híbridos GSM/GPRS-Satélite.** Usan los enlaces de telefonía móvil cuando vuelan a baja cota y reciben señal de la red terrestre, pasando a satélite cuando vuelan a cotas superiores sin cobertura GSM/GPRS. El sistema IRIDIUM ha dado un magnífico resultado en las operaciones aeromóviles militares llevadas a cabo en Afganistán.



ESTACIONES AERONÁUTICAS

Las frecuencias de llamada de aeronaves para casos de emergencia o desastre aéreo son las siguientes: 2.182; 3.023; 5.680; 8.364 KHz; 121,5 MHz y 406 MHz. Las aeronaves hacen escucha en esta frecuencia, **121,5 MHz (AM)** a lo largo de la ruta. Esta frecuencia también es controlada por satélites que pueden determinar la posición de una radiollamada en dicha frecuencia. Estas frecuencias además se integran en **balizas** que portan los pilotos o embarcaciones, pudiendo mediante **satélite COSPAS. SARSAT** obtener la posición exacta del personal a rescatar.

Las frecuencias utilizadas para **búsqueda y rescate** son las de 10.003, 14.993 y 19.993 KHz.

Existe una frecuencia de conversación oficiosa entre pilotos **llamada la "correlativa",** 123,45 MHz, que aunque no está atribuida por ningún organismo puede ser usada en una operación de emergencia. Lo normal es que el piloto vaya introduciendo manualmente la frecuencia de los centros de control del tráfico aéreo de la región que vaya sobrevolando en cada momento.

En el trascurso de una gran emergencia en la que se precisen una cantidad importante de aeronaves se suele dictar un **NOTAM** *(Notices to Airmen)* o **aviso a los pilotos,** que incluye información relativa a la seguridad y por ejemplo los lugares de lanzamiento de cargas, las pistas de aterrizaje habilitadas y los detalles de frecuencias e indicativos instaurados en la zona para facilitar el tránsito aéreo.

PRINCIPALES TIPOS

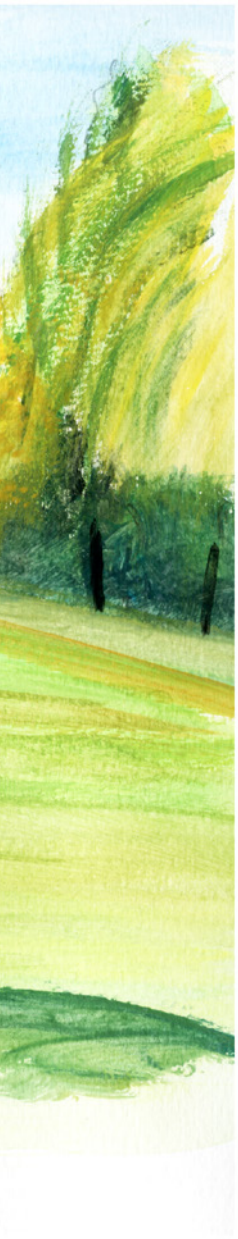
Dan información meteorológica. Utilizan además de la radio (AM/FM), el radioteletipo (RTTY) y el facsímil (FAX).

- Radioayudas aeronáuticas: encontramos varios tipos de estaciones que emiten señales destinadas a facilitar y garantizar la navegabilidad de las aeronaves durante el vuelo y asistirlas durante la etapa de aproximación a la pista para aterrizar. Así tenemos:
- Radiofaros no direccionales-NDB *(No Directional Beacon):* se trata de emisoras situadas en tierra en una posición seleccionada para que en conjunción con el equipo de la aeronave constituyan una guía para que el piloto fije su rumbo hacia la posición geográfica desde donde aquellas transmiten.
- Radiofaros Omnidireccionales en VHF - VOR *(Very High Omnidirectional Range):* estos radiofaros proporcionan información del azimut en los 360° a las aeronaves que se hallan dentro de su cobertura de radiación. Operan en la banda de VHF entre los 112 y 117,975 MHz.
- Equipos radiotelemétricos en UHF - DME (*Distance Measuring Equipment):* estas estaciones proporcionan al piloto información de la "distancia oblicua" que existe entre la aeronave en vuelo y el equipo en tierra.
- Sistemas de aterrizaje por instrumentos - ILS *(Instrument Landing System):* es una -Sistemas de aterrizaje por instrumentos - ILS (Instrument Landing System): es una radioayuda utilizada para la aproximación final y el aterrizaje de las aeronaves.


RESCATE

CAPÍTULO 16

ORGANISMOS DE NORMALIZACIÓN Y REGULACIÓN



Antes de continuar, una advertencia. Este capítulo es arduo. La información que contiene es accesoria. Continúe leyéndolo sólo si tiene interés o necesita saber "algo" de la normativa y las organizaciones existentes que están relacionadas con el enlace en las emergencias.

Si pese a la advertencia continua pertinaz en el empeño, trataremos de hacerlo lo más llevadero posible.

CONVENIO DE TAMPERE DEL AÑO 1998

El **importante papel que desarrollan los sistemas de enlace terrestres** no han sido reconocidos hasta hace poco tiempo. No ocurría así con los sistemas de aeronaves y de salvamento marítimo que desde hace siglos disfrutan de ciertos privilegios, como son la exención de pagos e impuestos y la alta prioridad de sus emisiones.

Los antecedentes de este convenio los encontramos en la **Conferencia Internacional sobre comunicaciones de socorro en casos de catástrofe** (Ginebra, 1990), y en la **Declaración de Tampere sobre comunicaciones de socorro en casos de catástrofe del año 1991**. En esta última reunión se decidió realizar acciones en favor de unos sistemas fiables de telecomunicaciones para la mitigación de las catástrofes y las operaciones de socorro y de la preparación de un convenio internacional sobre comunicaciones en caso de catástrofe que facilitase la utilización de esos sistemas.

Los 17 artículos, que constituyen un **tratado internacional jurídicamente vinculante,** fueron adoptados de forma unánime por delegados de 75 países, en la **Conferencia Intergubernamental sobre las Telecomunicaciones de Urgencia en el año 1998** que se realizó de nuevo en Tampere.

El Tratado quedó a partir de ese momento abierto a la adhesión con la mediación de la **Oficina de las Naciones Unidas para la Coordinación de Asuntos Humanitarios (OCHA),** a la espera del número requerido de 30 ratificaciones para entrar en vigor, lo que no ocurrió hasta el 8 de enero de 2005.

El **Convenio de Tampere** ***"Sobre el suministro de recursos de telecomunicaciones para la mitigación de catástrofes y las operaciones de socorro en caso de catástrofe",*** reconoce el papel clave de las telecomunicaciones terrenas en la prevención y mitigación de grandes catástrofes, comprometiéndose las naciones firmantes a prestarse ayuda en la rehabilitación de infraestructuras de telecomunicación. Es decir **el objeto es facilitar la cooperación internacional en materia TIC.**

En el preámbulo del convenio se remarca que los organismos humanitarios de socorro y asistencia requieren recursos de telecomunicaciones fiables y flexibles. Además señala que la función esencial de las telecomunicaciones es **facilitar la seguridad del personal de socorro y asistencia humanitaria, y que el despliegue eficaz y oportuno de los recursos de telecomunicaciones** y un flujo de información rápido, eficaz, exacto y veraz resulten esenciales para **reducir la pérdida de vidas.**

Aunque es únicamente una **declaración de expertos,** se incide en la necesidad de crear un instrumento jurídico internacional sobre el suministro de telecomunicaciones para mitigar las emergencias. En la declaración se instaba al Coordinador del Socorro de Emergencia de las Naciones Unidas a que cooperase con la UIT.

Además se instaba a las administraciones a reducir y/o suprimir las barreras reglamentarias para **facilitar el rápido despliegue y el uso eficaz de los recursos de telecomunicaciones en las operaciones de socorro.** Por último dio lugar a la creación del **Grupo de Trabajo sobre Telecomunicaciones en Situaciones de Emergencia (WGET).**

España no se adhirió a este convenio hasta febrero de 2006 (en la actualidad hay más de 60 países) y fue publicado en el BOE número 81 el 5 abril del mismo año. Se puede leer el Acuerdo de Adhesión español en el **Anexo 2 de este libro.**

El Convenio de Tampere es muy importante en nuestro ámbito de actuación por su **trascendencia en dos aspectos fundamentales.** El primero de ellos abría la puerta a la **asistencia y ayuda entre países en materia de telecomunicaciones** en caso de catástrofes.

El segundo daba lugar al nacimiento de una serie de normativa que instaba a los países firmantes a implementar en sus sistemas de telecomunicaciones **recomendaciones para fortalecer dichos sistemas y hacerlos muchos más resistentes y menos vulnerables** a los desastres provocados por la naturaleza.

La **ayuda en materia de telecomunicaciones** se puede prestar de forma directa a instituciones nacionales en un lugar afectado por una catástrofe, e incluso en el

OCHA

reliefweb

Entre los recursos que ***OCHA*** pone a disposición de las organizaciones de ayuda humanitaria está ***ReliefWeb***, sitio donde se recopila información relevante, fiable, útil y permanentemente actualizada de todas las catástrofes activas en el mundo, sin dejar a un lado las "emergencias olvidadas". Información como mapas, informes de estado, recomendaciones, necesidades, etc.

El objetivo no es sólo ser un repositorio de información útil para la comunidad internacional de ayuda humanitaria, sino también el convertirse en el canal de intercambio de información y coordinación entre todas las organizaciones humanitarias involucradas en la mitigación de una catástrofe.

contexto de otras actividades de socorro. Es importante señalar que este **acuerdo protege los intereses de los Estados** que solicitan y reciben la asistencia y que prevé la concertación de **acuerdos bilaterales o multilaterales** entre los organismos que prestan la asistencia y el Estado que la solicita.

La asistencia es siempre flexible en formas y duración. Se centra fundamentalmente en asignar **privilegios, inmunidades y facilidades al personal TIC que despliega** en las zonas afectadas, y establece el posible pago o reembolso de gastos o cánones por parte del país que solicitó la ayuda. Es decir, no tiene por qué ser gratis, aunque lo normal es que sí lo sea. Por último facilita la **resolución de obstáculos normativos y administrativos** para usar el material de enlace que se envía a la emergencia.

Las **Naciones Unidas** a través de la OCHA cumple funciones de **coordinador de las operaciones** y convoca regularmente al Grupo de Trabajo WGET, un foro en el que participan, aparte de los organismos de las Naciones Unidas, numerosas organizaciones internacionales, nacionales, gubernamentales y no gubernamentales, y expertos de la empresa privada y las universidades especializadas en la intervención en ese tipo de situaciones.

De un lado, cuando una desgracia relevante acontece, se desencadena la participación de todas las agencias de respuesta haciendo uso de las redes comunes y propias de la ONU. Si la intervención internacional es necesaria, la interacción de todos los sistemas de enlace se establece mediante el mecanismo del WGET y se designa un **Coordinador de Telecomunicaciones (TCO) común**, para optimizar el uso de las redes en el país afectado.

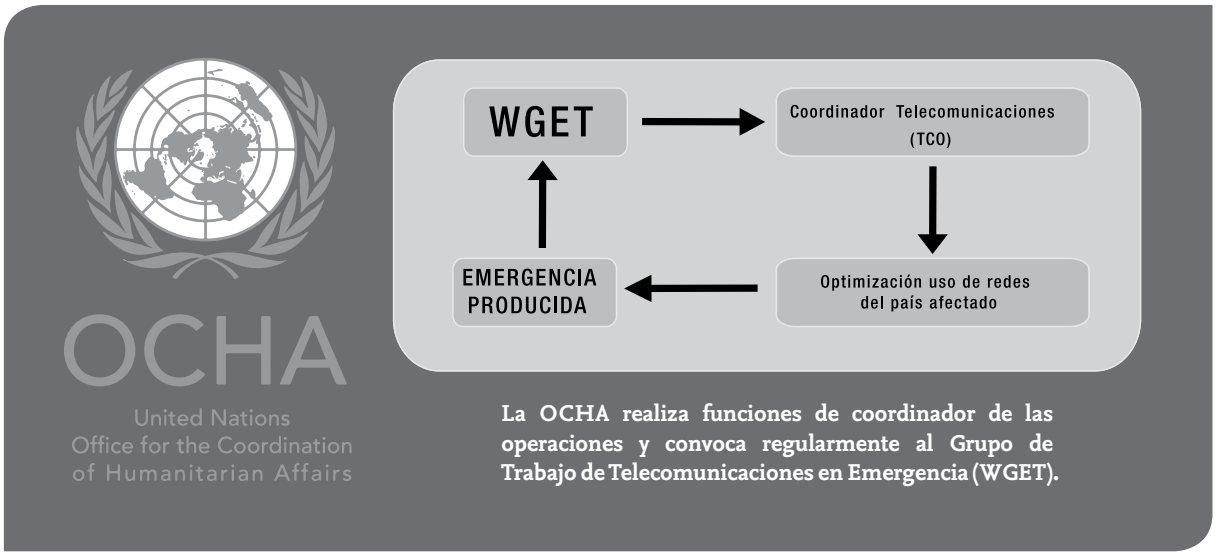
Finalizamos este apartado afirmando que el papel clave que desempeñan las telecomunicaciones de emergencia ha sido también reconocido en **otros documentos** aparte del Convenio de Tampere[120], productos mayoritariamente de conferencias internacionales auspiciadas por la ITU y la ONU.

120. Entre otros:
- Recomendación 12 de la Conferencia Mundial de Desarrollo de las Telecomunicaciones, Estambul 2002.
- Resolución 34 de la Conferencia Mundial de Desarrollo de las Telecomunicaciones, Estambul 2002.
- Resolución 36 de la Conferencia de Plenipotenciarios de la UIT, Marrakech 2002.
- Revisión del Artículo 25 del Reglamento de Radiocomunicaciones (RR) por la Conferencia Mundial de Radiocomunicaciones, Ginebra 2003.

ORGANISMOS REGULADORES DE NORMALIZACIÓN Y CERTIFICACIÓN A NIVEL MUNDIAL.

Las entidades mencionadas anteriormente son sólo unos ejemplos que respaldan la existencia de los llamados "**reguladores" de las telecomunicaciones** en emergencia.

Los organismos reguladores son esas instituciones que **intentan aunar esfuerzos** en aras de la buena coordinación en materia del enlace en emergencias. Además dado



La OCHA realiza funciones de coordinador de las operaciones y convoca regularmente al Grupo de Trabajo de Telecomunicaciones en Emergencia (WGET).

que en muchas ocasiones estaremos hablando de recursos limitados, como pudieran ser el ancho de banda de un satélite, o el espectro de frecuencias disponibles para una transmisión radio, se deben dictar unas normas mínimas que protejan a los usuarios y operadores.

Es decir estos organismos de normalización y regulación son los encargados de dictar **"las reglas del juego del enlace en emergencias".**

La clasificación más elemental de los entes reguladores concierne a la ubicación geográfica. Así tendremos reguladores internacionales, regionales (continentales normalmente) y nacionales.

Sin ninguna duda el organismo de telecomunicaciones internacional más conocido es la **Unión Internacional de Telecomunicaciones (UIT)**[121]. En esta organización se aúnan esfuerzos públicos y privados para alcanzar las más altas cotas de coordinación y compatibilidad entre redes y servicios de telecomunicaciones. A medida que se amplía la utilización de las tecnologías de telecomunicaciones y de los sistemas de radiocomunicaciones en un mundo globalizado, la labor que realiza la UIT crece en importancia. La UIT ayuda a los gobiernos y a la industria de las telecomunicaciones a resolver una gran cantidad de asuntos que serían difíciles de solventarse a nivel bilateral.

Está formada por más de 190 estados miembros y alrededor de 700 miembros sectoriales y asociados. Es además **la organización más importante de la ONU en materia TIC** y tuvo su origen en las Conferencias Internacionales de Radiotelegráfica y Telegráfica de Madrid del año 1932[122].

El artículo 1, sección 2, de la Constitución de la UIT señala que **ésta "deberá promover la adopción de medidas destinadas a garantizar la seguridad de la vida humana, mediante la coordinación de los servicios de telecomunicaciones".**

La UIT coopera estrechamente con el **Coordinador del Socorro de Emergencia de las Naciones Unidas** y el **Jefe de la Oficina de la OCHA,** y es miembro del **Grupo de Trabajo sobre Telecomunicaciones en Situaciones de Emergencia (WGET)** anteriormente mencionado.

121. ITU: *International Telecommunication Union* (en inglés).

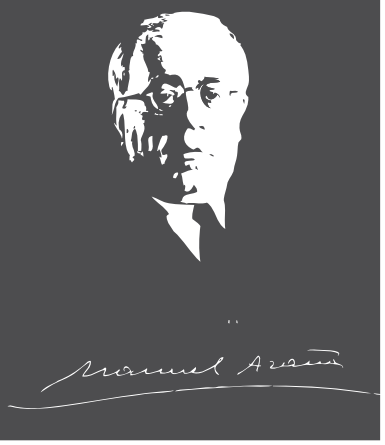
122. Por aquella época la dictadura de Primo de Rivera intentaba potenciar la imagen internacional de España promocionando acontecimientos que tuvieran repercusión periodística. Se estaba preparando la Exposición Internacional de Barcelona en 1930, y, simultáneamente, la Exposición Iberoamericana de Sevilla. La reunión de las Conferencias Internacionales Radiotelegráfica y Telegráfica se podía enmarcar dentro de las mismas intenciones. La Presidencia de las Conferencias correspondió al ministro de Comunicaciones, Santiago Casares Quiroga. La Delegación oficial española la componían 15 funcionarios del Ministerio de Comunicaciones, encabezados por el Director General Miguel Sastre Picatoste. Como debían actuar simultáneamente ambas Conferencias, actuaron como Jefes suplentes en la Conferencia Telegráfica: Gabriel Hombre y Pedro Gamir y en la Conferencia Radiotelegráfica Ramón Miguel Nieto y el Coronel de Ingenieros Tomás Fernández Quintana. Además de los funcionarios del Ministerio de Comunicaciones, formaban parte de la delegación oficial tres representantes del Ministerio de la Guerra y otros tres del Ministerio de Marina.

CONFERENCIA DE MADRID DE 1932

Como anécdota puede ser interesante traer aquí el texto del telegrama del Rey Alfonso XIII a la Conferenecia de Washington, al conocer la aceptación de Madrid como sede de la próxima Conferencia. Dirigido al Embajador de España, decía así:

"Enterado con satisfacción acuerdo Conferencia Internacional Radiotelegráfica de celebrar próxima reunión en Madrid; presente saludos en mi nombre a los Señores Delegados, participándoles el placer que tendré de recibirles en 1932 en esta capital. Alfonso".

La profecía del rey no se cumplió y no fue él quien presidió la apertura de las Conferencias en el Palacio del Senado, sino el presidente del Gobierno de la República, Manuel azada. El cambio de régimen no afectó a la invitación que España, como estado, había hecho y el funcionamiento de la UTI se independizaba de las circunstancias políticas.



Sus objetivos son:

- Promover el desarrollo, la explotación racional y ampliar la cooperación internacional para la mejora de toda clase de instalaciones y servicios de telecomunicaciones.
- Promover el desarrollo de las telecomunicaciones en los países en desarrollo y la extensión de los beneficios de las telecomunicaciones, acrecentar su empleo y generalizar lo más posible su uso a todos los habitantes del planeta.
- Y promover la adopción de un enfoque más amplio de las cuestiones de las telecomunicaciones en la economía y la sociedad mundiales de la información.

Con el fin de alcanzar estos objetivos, la labor de la UIT se articula en torno a tres Sectores:

- Sector de Radiocomunicaciones (UIT–R).
- Sector de Normalización de las Telecomunicaciones (UIT–T).
- Sector de Desarrollo de las Telecomunicaciones (UIT–D).

De conformidad con el artículo 12.2 del Convenio de Tampere, este último sector aludido, el de Desarrollo de la UIT, presta asesoramiento y apoyo en la creación de una reglamentación y legislación de las telecomunicaciones en diversos países encaminada a una aplicación satisfactoria de dicho Convenio.

Sin embargo la rama más conocida es la del **Sector de Radiocomunicaciones (UIT–R)**, cuya misión es la de coordinar de manera coherente los servicios inalámbricos, desempeñando un papel fundamental en la gestión del espectro de frecuencias radioeléctricas y de las órbitas de los satélites.

ORGANISMOS REGULADORES DE NORMALIZACIÓN Y CERTIFICACIÓN EUROPEOS

A nivel regional debemos hacer mención a las diferentes **Direcciones Generales** que informan a la Comisión Europea y que tienen algún tipo de relación con las telecomunicaciones. La de Competencia, la de Investigación y Desarrollo Científico y por supuesto la **DG XIII de Telecomunicaciones, Industrias de la Información e Innovación** son las que proponen las leyes al Parlamento Europeo para su aprobación inicial que luego ratifica nuestro **Ministerio de Industria, Energía y Turismo** en el Consejo de Ministros correspondiente (esto en el año 2013 porque luego se crean y desaparecen otros ministerios que asumen estas responsabilidades).

También mencionaremos el **Instituto Europeo de Estandarización de las Telecomunicaciones (ETSI).** Este organismo tiene por meta disponer del foro adecuado para la elaboración de las normas de telecomunicación que faciliten la estandarización del sector, y por lo tanto el avance hacia el **Mercado Único Europeo de Telecomunicaciones.** En el ETSI participan como miembros no sólo las Administraciones, sino también los operadores de red, la industria, los centros de investigación y los usuarios de los servicios de telecomunicaciones.

El ETSI suele desarrollar en detalle los trabajos empezados por la ITU que en ocasiones deja abiertas diferentes opciones en sus recomendaciones. Por tanto el ETSI es la organización clave en el contexto europeo para la elaboración de normas tanto en el sector de las telecomunicaciones como para la convergencia de este sector con los de tecnologías de la información.

MARCO NORMATIVO MUNDIAL Y EUROPEO DE LAS TELECOMUNICACIONES EN EMERGENCIAS

El control y reglamentación de las telecomunicaciones hasta hace unas décadas era de carácter exclusivo de la soberanía de cada nación, sin embargo la propia naturaleza de las ondas electromagnéticas que mayoritariamente utilizan los medios de comunicación a distancia, se escapaban de las fronteras físicas nacionales. Por este motivo, la **reglamentación internacional es indispensable,** quedando la reglamentación nacional sólo para complementar las directrices marcadas a nivel internacional, y para algunas cuestiones que se ciñan estrictamente a las fronteras interiores de cada país.

Por tanto los organismos internacionales mencionados con anterioridad son los encargados de controlar, normalizar y proponer la implantación de **leyes, reglamentos, normas, recomendaciones y estándares** que permitan que los equipos implicados guarden unas normas comunes que hagan viables las telecomunicaciones a nivel mundial.

Las **leyes** fijan el marco jurídico, los **reglamentos** suelen detallar en profundidad la ley. Las **normas** son de obligado cumplimiento mientras que las **recomendaciones** y **estándares** son de aceptación voluntaria, que no se convierten en norma hasta que algún gobierno decide elevarlo a este rango a través de la publicación, por ejemplo en un Boletín Oficial.

Las leyes relacionadas con las TIC en Europa empiezan cuando la UE traza unos objetivos, primero mediante **Libros Verdes**[123] y luego mediante **Directivas**[124].

ORGANISMOS REGULADORES DE NORMALIZACIÓN Y CERTIFICACIÓN ESPAÑOLES.

Corresponde al **Ministerio de Industria, Energía y Turismo** la propuesta y ejecución de la política del Gobierno en materia de energía, desarrollo industrial, turismo, telecomunicaciones y de la sociedad de la información. En nuestro caso es la **Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI)** quien ejerce las funciones reguladoras en este ámbito de forma genérica, sin contar con ningún órgano que se encargue de la gestión del enlace en las emergencias.

Recordamos en este apartado que el apartado final del capítulo 8 dedicado a la interoperabilidad propusimos la creación de un **Comisionado Nacional TIC de Emergencias**, para ocuparse específicamente de este asunto.

La SETSI, aparte de la consabida **publicación de normativa**, realiza estudios técnicos, **promociona las TIC, autoriza licencias** para la prestación de servicios y **controla e inspecciona emisiones** gracias a una red de estaciones fijas y móviles que despliega por todo el Territorio Nacional para controlar entre otras las bandas de HF, VHF, UHF y SHF. Una de las misiones más conocidas de esta entidad es la publicación del **Cuadro Nacional de Atribución de Frecuencias (CNAF)**, que a través el BOE, asigna las frecuencias atribuidas a cada servicio de radiocomunicaciones.

En paralelo encontramos la **Comisión del Mercado de las Telecomunicaciones (CMT)** que es la **Autoridad Nacional de Regulación (ANR)**[125] del sector de las telecomunicaciones en España. Fue creada en 1996, durante el proceso de liberalización del sector de las telecomunicaciones, como organismo público regulador independiente de los mercados nacionales de comunicaciones electrónicas, sin ninguna relación con el mundo de las emergencias, al menos a priori.

Para la certificación a nivel nacional está la **Asociación Española de Normalización y Certificación (AENOR),** que es una entidad privada encargada de la normalización y certificación de diferentes sectores, entre los que se encuentran el de las telecomunicaciones.

MARCO NORMATIVO ESPAÑOL DE LAS TELECOMUNICACIONES EN EMERGENCIAS.

No es mucha la normativa que atañe directamente a este concepto en nuestro país. Para ser sinceros diremos que, **en realidad, es bastante escasa**. Lo es en cuanto a telecomunicaciones genéricas, y mucho más en la específica del mundo de las emergencias.

Cabría plantearse si el déficit se debe a la priorización en los órganos legisladores o simplemente a un desinterés prolongado en el tiempo. Lo cierto es que los padres de la constitución sí que vieron la importancia de un sector estratégico, y en el artículo 149.1 de la **Constitución Española**, en su apartado 21, dice que "los correos y telecomunicaciones; cables aéreos, submarinos y radiocomunicación, son **competencia exclusiva del Estado Central**".

123. El Libro Verde es un instrumento de la UE que define el programa de acción comunitario y las directrices de su política en el ámbito de referencia tratado.

124. La Directiva es un acto, no directamente aplicable, que obliga a los Estados Miembros a traspasarlo a la legislación nacional.

125. Las denominadas Autoridades Reguladoras Nacionales (ARN) son las estructuras administrativas que regulan las TIC en cada Estado, separadas de la Administración, lo que hace que a priori sean independientes y autónomas. Su función es de arbitraje y regulatoria.

Tendríamos que remontarnos a la **Ley Orgánica 2/1985 de Protección Civil,** para encontrar (siendo muy generosos) un atisbo de "conciencia legisladora" que se preocupara en España por el enlace en situaciones de emergencia. Nos estamos refiriendo a la Disposición Final Tercera que decía que el Gobierno crearía la **Red de Alarma Nacional,** dependiente de los órganos de protección civil del Estado, que a tales efectos se coordinaría con los órganos correspondientes del Ministerio de Defensa, para alertar a la población que pudiera resultar afectada por una emergencia que ocurriera en caso de guerra o en tiempo de paz.

El **Real Decreto 1378/1985**, de 1 de agosto, sobre medidas provisionales para la actuación en situaciones de emergencia en los casos de grave riesgo, catástrofe o calamidad pública, tenía por objeto establecer las medidas provisionales necesarias para la actuación de los órganos y autoridades competentes en los casos de grave riesgo, catástrofe o calamidad pública que pudieran producirse hasta que se aprobaran los planes referidos en el artículo 8 de la Ley 2/1985. Aunque este Real Decreto tenía un marcado carácter de provisionalidad, en su artículo 2 marcaba que correspondía a la Protección Civil "**la articulación de un sistema de transmisiones que garantizara las comunicaciones entre servicios y autoridades**". Esta articulación nunca se llego a plantear.

Avanzaremos hasta el siglo XXI para encontrar la siguiente referencia. **La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones,** modificó la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, e instauró un régimen plenamente liberalizado en la prestación de servicios y el establecimiento y explotación de redes de telecomunicaciones.

LA MARAÑA SUBACUÁTICA

En 1858 se tendió el primer cable submarino usado como enlace de telegrafía entre América y Europa. Apenas soportó los embates del mar y las mandíbulas de los tiburones durante 20 días, pero a pesar de ello transmitió algo más de 700 mensajes telegráficos entre continentes.

En esta ley aparecen algunas referencias al asunto que nos compete, aunque solamente de manera tangencial. En primer lugar exonera a las Administraciones Públicas de pagar la tasa en los supuestos de reserva de dominio público radioeléctrico para la prestación de servicios obligatorios de interés general que tenga exclusivamente **por objeto la defensa nacional, la seguridad pública y las emergencias.**

En segundo lugar indica que corresponde al extinto Ministerio de Ciencia y Tecnología ejecutar la **Política de Defensa Nacional[126], en el sector de telecomunicaciones.** A tal efecto coordinará con el Ministerio de Defensa a fin de asegurar la compatibilidad con los servicios civiles. Además indica que en el ámbito de **Protección Civil** el Ministerio de Ciencia y Tecnología cooperará con el Ministerio de Interior y con los órganos de las CCAA competentes.

Por último el **Real Decreto 1181/2008** por el que se estructuraba orgánicamente el

126. En este caso Defensa Nacional incluye tanto la Defensa Civil (Protección Civil) como la Defensa Militar.

Ministerio de Interior apuntaba que le correspondía a la **Dirección General de Protección Civil y Emergencias (DGPCyE)** la organización y mantenimiento de las **redes propias de comunicación para emergencias** y de otras infraestructuras destinadas a facilitar la gestión operativa de las emergencias. Este Real Decreto aunque no las nombra específicamente, se refería en concreto a dos redes, **RECOSAT**[127] (Sistema integral de comunicaciones de emergencia vía satélite de la Dirección General de Protección Civil y Emergencias) y **REMER** (Red Radio de Emergencia) que se rigen por resoluciones de la DGPCyE. Aquí se puede apreciar un olvido importante por parte del legislador, ya que no hace referencia a la Secretaria de Estado de Seguridad que es la responsable de la red más importante que posee el Ministerio de Interior, la Red **SIRDEE** (Sistema Integrado Radio Digital de Emergencias de España). Todas estas redes se detallan en el Anexo 3.

Hasta esta última referencia la conclusión a la que llegamos es que **se ha legislado muy poco con respecto al enlace en emergencias.** Sin embargo resulta llamativo que **sí que ha sido una preocupación prioritaria el tema TIC para las emergencias, sobre todo a nivel Comunidad Autónoma**, como demuestra que casi todas han desarrollado sus propias redes y sistemas para asegurar un buen servicio al ciudadano.

Llegamos al año 2010, cuando se comienzan a aprobar los **Planes Estatales ante distintos riesgos (inundaciones, seísmos, volcánico...).** Por primera vez aparece un Anexo específico de Telecomunicaciones y de Sistemas de Información. En éstos se menciona que en el caso de una emergencia declarada de interés nacional en la que no se puedan emplear las TIC basadas sobre infraestructura fija por haber sido dañadas o inutilizadas, los nodos a emplear serán los que actualmente dispone la **Unidad Militar de Emergencias (UME)** para apoyar a la propia Dirección Operativa de la Emergencia, pero también a la Administración General del Estado, órganos de las Comunidades Autónomas y otros organismos y empresas relacionados con la gestión de emergencias que precisen auxilio en este ámbito.

Además se menciona de forma expresa a la **Red Nacional de Emergencias (RENEM)**. La RENEM es un sistema de sistemas de información y telecomunicaciones que integra 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, que tiene como misión asegurar el intercambio de información relevante para la gestión y coordinación de las emergencias de cualquier tipo.

Desde el año 2007, se han emprendido diversas actuaciones a nivel nacional, como la aprobación por la **Secretaría de Estado de Seguridad del Ministerio del Interior,** de un primer **Plan Nacional de Protección de Infraestructuras Críticas**[128], así como la elaboración del *Catálogo Nacional de Infraestructuras Estratégicas* cuya custodia pertenece al **Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC).** Dicho catálogo es el instrumento que contiene toda la información y valoración de las infraestructuras estratégicas de España, entre las que se hallan incluidas aquellas clasificadas como

127. El sistema RECOSAT se ha desmantelado en el año 2013.

128. Las Infraestructuras Críticas (IC), según se definen en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, es el conjunto de recursos, servicios, tecnologías de la información y redes, que en el caso de sufrir un ataque, causarían gran impacto en la seguridad, tanto física como económica, de los ciudadanos o en el buen funcionamiento del Gobierno de la Nación. La citada Ley tiene como objetivos primordiales, establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de Infraestructuras Críticas, previa identificación y designación de las mismas, impulsando, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo. Asimismo regula las especiales obligaciones que deben asumir tanto las Administraciones Públicas como los operadores privados de aquellas infraestructuras que se determinen como Infraestructuras Críticas.

Críticas o Críticas Europeas según el reglamento de la **Directiva de la UE 2008/114/CE**, del 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

Las Infraestructuras Críticas según el Plan Nacional de Protección de Infraestructuras Críticas se pueden dividir en **doce (12) sectores estratégicos:**

- Centrales y redes de energía.
- **Tecnologías de la información y las comunicaciones (TIC).**
- Sistema financiero y tributario (por ejemplo, banca, valores e inversiones).
- Sector sanitario.
- Espacio.
- Instalaciones de investigación.
- Alimentación.
- Agua (embalses, almacenamiento, tratamiento y redes).
- Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico).
- Industria nuclear.
- Industria química.
- Administración (servicios básicos, instalaciones, redes de información, activos, y principales lugares y monumentos nacionales).

En el sector estratégico de las TIC, la **Ley 8/2011 identifica al Ministerio de Defensa como agente del sistema de protección de infraestructuras críticas** y como tal estará encargado de impulsar, en el ámbito de sus competencias, las políticas de seguridad del Gobierno sobre dicho sector y de velar por su aplicación, actuando igualmente como punto de contacto especializado en la materia. Además, el **Reglamento de Protección de las Infraestructuras Críticas, aprobado por Real Decreto 704/2011** de 20 de mayo de 2011, detalla en su artículo octavo todas las competencias en la materia, colaborando con la Secretaría de Estado de Seguridad del Ministerio del Interior. Por último, el **Centro Criptológico Nacional (CCN)** apoya al CNPIC en el tratamiento de los ciberataques sobre infraestructuras críticas y en la actualización de información sobre **vulnerabilidades SCADA[129] e incidentes de seguridad informáticos relacionados con infraestructuras críticas.**

129. SCADA acrónimo de Supervisión, Control y Adquisición de Datos (en inglés *Supervisory Control And Data Acquisition*)

En este contexto de delimitación de funciones, cabe añadir que la propia **Comisión para la Reforma de las Administraciones Públicas (CORA)** creada por el Gobierno mediante **Acuerdo de Consejo de Ministros de 26 de octubre de 2012,** ha elevado un reciente documento denominado "**Medidas para la racionalización de Infraestructuras y Servicios TIC en la Administración General del Estado**", entre los que se encuentran la Informática y la Administración Electrónica.

Incluye las siguientes medidas: consolidación de infraestructuras comunes, centralización de las compras TIC, nuevo modelo de organización de las TIC en la AGE, prestación común de servicios de certificación electrónica a la AGE; y en cuyas "Conclusiones, Recomendaciones y Propuestas" señala lo siguiente: "**La racionalización en el uso de infraestructuras y elementos tecnológicos comunes,** unida a una consultoría previa que justifique la necesidad real de las inversiones, y a las posibilidades de reutilización de aplicaciones y servicios, abre un universo de actuaciones enfocadas a la obtención de ahorro mediante un uso inteligente de los recursos".

Por otro lado, como **consecuencia de los trabajos de la CORA,** el 20 de septiembre de 2013 fue publicado el Real Decreto 695/2013 mediante el cual se crea la "**Dirección de Tecnologías de la Información y de las Comunicaciones (TIC) de la AGE**", con rango de Subsecretaría dependiente de los **Ministerios de la Presidencia y de Hacienda y AAPP.** En la Disposición adicional primera de dicho RD se establece que en el plazo de tres (3) meses se procedería al análisis y, en su caso, **reforma de los órganos colegiados relacionados con la administración electrónica y tecnologías de la información y de las comunicaciones.** ¿Podría asumir los cometidos del **Comisionado Nacional TIC de Emergencias** que reclamábamos en capítulo dedicado a la interoperabilidad? El tiempo lo dirá.

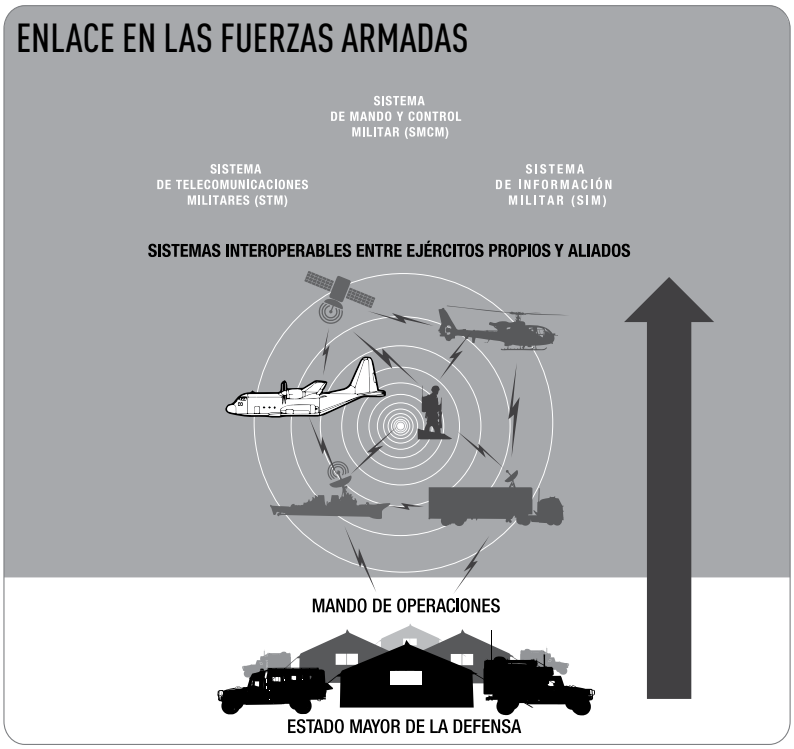
Sin embargo a nuestro entender, los objetivos de la Administración Electrónica, la Agenda Digital de España o el Plan Mejora no deben condicionar o distorsionar otros objetivos. Se debe **delimitar el verdadero alcance de la Administración Electrónica dentro de todo el ámbito público**. Es decir, se debe apostar por una clara delimitación que aporte sencillez a un conjunto que aparentemente se presenta como complejo al haber mezclado diversos objetivos e intereses sin una priorización adecuada.

Un caso concreto afecta a los TIC/CIS de las Fuerzas Armadas y del MINISDEF relacionados con la Seguridad y Defensa Nacional, que deberían separarse del resto de sistemas de la Administración General del Estado.

RELACIÓN DE ORGANISMOS MILITARES CON EL ENLACE EN LAS EMERGENCIAS

Finalizaremos el capítulo, y el libro, hablando de la normativa y organismos de las Fuerzas Armadas relacionados con el enlace en emergencias.

Las Fuerzas Armadas aparte de las funciones que les pueden ser propias por su organización, equipamiento e instrucción y adiestramiento de sus componentes, pueden abarcar un gran abanico de situaciones en las que sus características específicas permiten



utilizar a la institución castrense en actividades y cometidos entre las que se encuentra el apoyo durante las emergencias.

Con respecto a la normativa diremos brevemente que casi no existe una normativa *"ad hoc"*. Existe una **pequeña excepción** que comentaremos al final de este apartado. Por lo general los ejércitos regulan sus **Sistemas de Telecomunicaciones e Información (CIS)** para asegurar el cumplimiento de las misiones que legalmente tienen atribuidos en cada país, pero casi ninguno cuenta con una regulación específica para el enlace durante una catástrofe o emergencia.

Con respecto a las organizaciones de control del CIS/TIC, podemos poner como ejemplo que una organización como la OTAN, tiene una componente especializada en Protección Civil. Nos referimos al Comité Permanente de Planes Civiles de Emergencia, **NATO Civil Emergency Planing Committee (CEPC)**[130]. Sin embargo no trata el asunto de telecomunicaciones, delegando en la Agencia de Comunicaciones y de Información, **NATO Communications and Information (NCI) Agency,** todo lo relativo a estos asuntos.

Cuando se desencadena una operación de apoyo a las autoridades nacionales en caso de emergencias civiles, son las unidades militares nacionales o internacionales intervinientes las que ponen en juego sus propios sistemas CIS.

En nuestro país, a nivel **Ministerio de Defensa,** existen organismos dedicados a la gestión de los sistemas de telecomunicaciones y de información. A nivel Órgano Central, dentro de la Secretaría de Estado de Defensa, es la **Dirección General de Infraestructura** la que a través de

130. El CEPC tiene como áreas de actuación dentro de la OTAN las siguientes:
- Apoyo con medios civiles a las operaciones militares aliadas del art. 5
- Apoyo a las operaciones No-artículo 5 (Crisis Response Operations)
- Apoyo a las autoridades nacionales en caso de emergencias civiles
- Apoyo a las autoridades nacionales en la protección de la población contra los efectos de armas de destrucción masiva
- Cooperación con los "partners"de la Alianza.

Para el desarrollo de estas actividades, el CEPC realiza sus habituales reuniones de trabajo con los miembros de la Representaciones Permanentes de cada país. Sin embargo, este Comité convoca dos reuniones plenarias (primavera y otoño), en formato "sólo países OTAN" (28 naciones), así como con los miembros del EAPC (23 naciones).

la **Subdirección General TIC** desempeña sus labores.

En El Estado Mayor de la Defensa (EMAD), es la División de Sistemas de Telecomunicaciones y de Información (DIVCIS_EMAD), mientras que en los Ejércitos y Armada se cuenta con Jefaturas CIS y de Asistencia Técnica (JCISAT) específicas.

También dentro del EMAD se creó en febrero de 2013 el nuevo Mando **Conjunto de Ciberdefensa**. Entre sus cometidos se encuentran garantizar el libre acceso al ciberespacio con el fin de cumplir las misiones asignadas a las Fuerzas Armadas, con especial atención a las unidades desplegadas en el exterior; ejercer la respuesta oportuna, legítima y proporcionada ante amenazas o agresiones que puedan afectar a la Defensa Nacional y representar al Ministerio de Defensa en este campo en el ámbito nacional e internacional. Es de suponer que sería el responsable junto al Centro Nacional de Inteligencia (CNI) de responder a las emergencias relacionadas con las TIC/CIS.

Sin embargo, dada la misión concreta que la **Unidad Militar de Emergencias** tiene atribuida dentro del Sistema Nacional de Protección Civil, ésta cuenta con **un sistema de telecomunicaciones específico** para cumplir con sus cometidos y para apoyar a aquellos organismos que lo precisen, tal y como se contempla en los planes estatales de los distintos riesgos anteriormente mencionados.

La UME dispone de una **Sección de Estado Mayor** dedicada en exclusiva al planeamiento de sus sistemas y de un **Batallón de Transmisiones** especializado en implementar las redes necesarias para la conducción de emergencias en el caso de que fallaran las redes de telecomunicaciones permanentes. En caso de que la emergencia sobrepasara las capacidades de este Batallón, la UME recurriría al resto de medios CIS de las Fuerzas Armadas.

La **excepción** a la que hacíamos referencia al principio de este apartado en materia de legislación en el ámbito de las TIC relacionadas con las emergencias se refiere Real Decreto 1097/2011, de 22 de julio, por el que se aprobó el **Protocolo de Intervención de la Unidad Militar de Emergencias.** En el apartado noveno señala, por un lado que la Administración General del Estado le facilitará el acceso a las redes y sistemas de alerta y emergencias existentes y que el Ministerio de Defensa suscribirá con las comunidades autónomas los acuerdos de colaboración necesarios para el **acceso de la UME a sus redes de alerta y emergencia,** con el fin de que la UME pueda cumplimentar satisfactoriamente las misiones asignadas.

El CIS de la UME, es un caso de éxito que partió del marco del **Plan Director CIS del MINISDEF, del Concepto NEC de la OTAN, y de la aplicación con rigor de la metodología de trabajo proporcionada por el NAF v.2 de 2004.** Este sistema se desarrolló y diseñó sobre la base de una Arquitectura de Referencia CIS, de las que emanaron otras arquitecturas objetivo, y de los más de cien (100) proyectos para su implementación, con una **Oficina de Programa** que supo optimizar los recursos y ser extremadamente exigente con las empresas contratistas.

Uno de los principios más importante del diseño de la arquitectura de referencia CIS de la UME fue el uso de **una sola red,** la WAN de propósito general, **prolongada al entorno táctico mediante determinados enlaces del sistema de telecomunicaciones militares** (terrestres y satelitales), pero con la innovación de haber implantado un sistema de comunicaciones satélite **basado en tecnología IP** como banda base, con técnicas de calidad de servicio que permiten incrementar o rebajar la capacidad del enlace en función del servicio requerido. Ello supuso un uso más que eficiente de los gestores de ancho de banda y permitió la implantación de un **sistema de gestión dinámica del espectro** de los enlaces vía satélite ahorrando alrededor de un 60% del ancho de banda. De esta forma y aplicando técnicas de autodescubrimiento, el enlace satélite y conexión de cualquier nodo desplegable a la red de la UME tarda en establecerse alrededor de un minuto, lo que en comparación con otros sistemas, tanto civiles como militares, es un auténtico logro ya que éstos necesitan de incluso semanas de antelación para tener acceso a tramas de satélite.

Este innovador cambio ha permitido que las redes TIC/CIS desplegables de la UME, en el ámbito táctico, desde el nivel táctico más bajo (Sección) hasta el más elevado (Puesto de Mando Desplegable del Jefe de la UME) **sean una perfecta prolongación de la red permanente,** sin solución de continuidad en una infraestructura civil y militar plenamente integrada. En cuanto a la seguridad se implantó un **doble sistema simultáneo de cifrado IP,** uno certificado por el CCN y otro basado en el estándar IPSEC, lo que supone una protección adicional en caso de fallo de alguno de los dos. Sistemas seguros en una sola red.

Otro punto de innovación importante fue el desarrollo de **una red multiservicio** basada en el protocolo IP, que permitió la

convergencia sobre la misma, de todos los servicios como telefonía IP, videoconferencia, fax, réplicas de datos de sistemas de información, etc., lo que supuso un gran ahorro de costes y simplicidad del diseño de los nodos. **En definitiva, sistemas tecnológicamente avanzados seguros en una sola red y con uso eficiente de los recursos disponibles.**

REDES MILITARES E INFRAESTRUCTURAS CRÍTICAS.

Teniendo en cuenta estas referencias normativas, parece evidente la necesidad de **catalogar el sistema de telecomunicaciones de las Fuerzas Armadas y sus sistemas de información** específicos como una **infraestructura crítica de la nación,** estando obligado el Ministerio de Defensa a jugar un doble papel en este sector: como agente del sistema de protección respecto al sector TIC a escala nacional, y como operador crítico de sus propios sistemas.

No se entendería, por ejemplo, que en caso de una emergencia nacional, el General Jefe de la Unidad Militar de Emergencias (UME) asumiese su papel como Director Operativo sobre una infraestructura de mando y control cuyo componente CIS no ofreciese las garantías de protección de una infraestructura crítica. A día de hoy, la Red Nacional de Emergencias (RENEM) pilotada por la UME se basa fundamentalmente en la Red Global de Telecomunicaciones (RGT) del Ministerio de Defensa. En resumen, la emergencia nacional se gestiona sobre las redes militares. ¿Cómo no van a ser éstas una infraestructura crítica para la nación? ¿Cumple con los requisitos de una infraestructura crítica? La respuesta es claramente **afirmativa**.

BIBLIOGRAFÍA

Acuerdo de Consejo de Ministros de 26 de octubre de 2012, "Medidas para la racionalización de Infraestructuras y Servicios TIC en la Administración General del Estado".

ADP 6-0. Mission Command. USA Headquarters Department of The Army. May 2012.

"A guide to radio communications standards for emergency responders". United Nations Development Programme (UNDP) and the European Commission Humanitarian Office (ECHO) Through the Disaster Preparedness Programme (DIPECHO) Regional Initiative in Disaster Risk Reduction. March, 2010.

BENITO PERTUSA, Rubén. "Telecomunicaciones y Emergencias". Psicosocial & Emergencias. Publicación Semestral N°8. Artículos y Reflexiones. Mayo de 2010.

"Command and Control in a Network Enabled Enviroment. Catalysing the art of C2". Command and Control Centre of Excellence. August 2010.

Constitución Española. 1978.

Curso de Capacitación en Protección Civil. Unidad Didáctica 5, Tema 2 "Las Telecomunicaciones". Escuela Nacional de Protección Civil. 2009.

Diccionario de la Lengua Española. Real Academia Española. 22 Edición. Espasa Calpe. 2001.

DO2-002. "Doctrina Telecomunicaciones". (Derogada). Mando de Adiestramiento y Doctrina del Ejército de Tierra español. Octubre de 1999.

DO2-008. "Doctrina Mando y Control". Mando de Adiestramiento y Doctrina del Ejército de Tierra español. Julio de 2005.

"Establishing Governance to Achieve Statewide Communications Interoperability". A Guide for Statewide Communication Interoperability Plan (SCIP) Implementation. Department of Homeland Security. December 2008.

FÉLIZ, Mercedes y DE SAN BENITO, David. "SOS Emergencias: nuevo desafío para las TIC". Asociación Española de Usuarios de Internet. Agosto de 2007.

FÉLIZ, Mercedes y MOLINA, Marta. "Las Telecomunicaciones, al servicio de las emergencias". Artículos de la Sociedad de la Información. Febrero de 2006.

Field Manual 3-28. Civil Support Operations. USA Headquarters Department of The Army. August 2010.

Field Manual 6-0. Mission Command: Command and Control of Army forces. USA Headquarters Department of The Army. August 2003.

GARCÍA–LEGAZ PONCE, Jaime. "Liberalización, competencia y regulación de las telecomunicaciones en España". Economía Industrial. N° 337. 2001.

"Gestión de la información y comunicación en emergencias y desastres". Guía para equipos de respuesta. Área de Preparativos para Situaciones de Emergencia y Socorro en Casos de Desastre Panamá. Julio 2009.

GONZALEZ ARRIBAS, Ángel. "El Coordinador TIC". Departamenteo TIC del CRIF " Las Acacias". 2009.

HERNANDO RÁBANOS, Jose María. "Redes móviles de emergencia". Cátedra Telefónica Sostenibilidad en Comunicaciones Móviles de la UPM. Responsabilidad Corporativa y Sostenibilidad. Cuaderno Red de Cátedras Telefónica. 2010.

HERNANDO RAMIREZ, Luis. "Copilación Curso Básico de Comunicaciones en Emergencias ITU". 2010.

HUIDOBRO MOYA, José Manuel. "Manual de Telecomunicaciones". Editorial RA-MA. 2003.

HUIDOBRO MOYA, José Manuel. "Todo sobre Comunicaciones" (Tercera Edición). Editorial Paraninfo. 1999.

IBÁÑEZ PEIRÓ, Ángel. "La Información Pública y la legislación en materia de Protección Civil y Emergencias". Mayo de 2012.

"Incident Command System". Introduction and Overview. Canadian Interagency Forest Fire Centre. 2002.

"Information Technology for Counterterrorism. Immediate actions and future possibilities". The National Academies Press. Governing Board of the National Research Council. USA National Academy of Sciences. 2003.

"Introducción a los sistemas de comunicación a través de formaciones rocosas". Sistema HEYPHONE y NICOLA. Grupo de Exploraciones Subterráneas de la Sociedad Excursionista de Málaga. Andalucía Subterránea N° 18. 2009.

"Interoperability Business –case: An introduction to Ongoing Local Funding". Department of Homeland Security. December 2008.

IZU BELLOSO, Miguel. "De la Protección Civil a la Gestión de Emergencias." Evolucion del marco normativo. 2009.

"Las Transmisiones Militares Permanentes". Más de un Siglo de historia del Regimiento de Transmisiones 22. Ministerio de Defensa. Diciembre de 2011.

Ley Orgánica 2/1985 de Protección Civil.

Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

"Los Mayores ante las TIC". Accesibilidad y Asequibilidad. Fundación Vodafone España. 2010.

"Los desastres naturales y la protección de la salud". Publicación Científica N° 575. Organización Panamericana de la Salud. 2000.

"Manual de Usuario del POSITRON". Aplicaciones de la Atencion de Emergencias de SOS Navarra. Agencia Navarra de Emergencias. 2010.

"Manual de XEOCODE". Consellería do Medio Rural. Dirección Xeral de Montes e Industrias Forestais. Xunta de Galica. 2008.

"Manual sobre telecomunicaciones de emergencia". Unión Internacional de Telecomunicaiones (UIT/ITU). Edición 2005.

"Manual 17: Multi-Agency Incident Management". Part III. Emergency Management Practice Volume 3— Guidelines. Australian Emergency Manual Series. 1998.

"Manual 32: Leadership". Part IV. Skills for Emergency Services Personnel. Australian Emergency Manual Series. 1998.

"Manual 38: Communications". Second Edition. Part IV. Skill for Emergency Services Personnel. Australian Emergency Manual Series. 1998.

MARTINEZ, Bernat. "Las TIC como herramienta en las situaciones de Emergencia". Cuadernos Internacionales de tecnología para el desarrollo humano. Junio 2007.

"Memoria Militar de España". Centro Cultural Conde Duque. Concejalía de Cultura. Ayuntamiento de Madrid. 1986.

MOLLÁ RAMOS, Miguel. "La tecnología aplicada a la gestión de emergencias". Módulo XV. Máster en Protección Civil y Gestión de Emergencias de la Universidad de Valencia. 2006.

MUÑOZ LORENTE, Gerardo. "Valencianaos en la guerra del Rif (1909). Editorial Club Universitario (ECU). 2010.

"NECP Capabilities Assetment Guide". Working together, we can achieve our vision. Department of Homeland Security. March 2010.

OLIVÉ ROIG, Sebastián. "Madrid 1932: nace la Unión Internacional de Telecomunicaciones". Foro Histórico de Telecomunicaciones. 2007.

ORDEN ITC/1791/2006, de 5 de junio, por la que se aprueba el Reglamento de uso del dominio público radioeléctrico por aficionados.

ORTA, Carlos. "Incendios en Túneles". Bomberos de Navarra. 2001.

OR3-501. "Orientaciones Sistemas de Telecomunicaciones e Información (CIS)". Mando de Adiestramiento y Doctrina del Ejército de Tierra español. Noviembre de 2007.

PD1-001. "Doctrina para el Empleo de las Fuerzas Terrestres". Mando de Adiestramiento y Doctrina del Ejército de Tierra español. Diciembre de 2011.

"PLADIGA: Plan de Prevención e Defensa contra os Incendios Forestais de Galicia". Secretaría Xeral do Medio Rural e Montes da Consellería do Medio Rural e do Mar. 2012.

PRENSKY, Marc. "Enseñar a nativos digitales". Ediciones SM. 2011.

"Procedimiento de Rescate en Espacios Confinados Naturales". Batallón de Intervención en Emergencias V. Unidad Militar de Emergencias. 2011.

"Rapport de retour d'experience des Forces Terrestres". Cahier du retex. Gestion de la crise post tsunami par les forces d´autodéfense Terre japonaises. Mars - Septembre 2011.

Real Decreto 1181/2008 sobre reestructuración del Ministerio de Interior.

Real Decreto 1378/1985, de 1 de agosto, sobre medidas provisionales para la actuación en situaciones de emergencia en los casos de grave riesgo, catástrofe o calamidad pública.

Real Decreto 704/2011 de 20 de mayo de 2011, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas.

Real Decreto 1070/2012, de 13 de julio, por el que se aprueba el Plan estatal de protección civil ante el Riesgo Químico.

Real Decreto 695/2013 mediante el cual se crea la "Dirección de Tecnologías de la Información y de las Comunicaciones (TIC) de la AGE".

REBOREDO RODRÍGUEZ, Marcos. "Comunicaciones seguras ante situaciones de emergencia en túneles ferroviarios". Dpto. de Ingeniería y Sistemas. REVENGA Ingenieros. 2011.

Resolución de 29 de marzo de 2010, de la Subsecretaría, por la que se publica el Acuerdo de Consejo de Ministros de 26 de marzo de 2010, por el que se aprueba el Plan Estatal de Protección Civil ante el Riesgo Sísmico.

Resolución de 2 de agosto de 2011, de la Subsecretaría del Ministerio de Interior, por la que se publica el Acuerdo del Consejo de Ministros de 29 de julio de 2011, por el que se aprueba el Plan Estatal de Protección Civil ante el Riesgo de Inundaciones.

RINCÓN VEGA, José Miguel. "Evaluación de los sistemas de Información y Comunicación (SIC)". Universidad del País Vasco (UPV/EHU). 2000.

RUIZ BOADA, Francisco. "Plan de Emergencia del Túnel de Somport". MAPFRE seguridad. N° 81. 2001.

SANCHEZ, Carolina. "Director TIC: el ritmo tecnológico en sus manos". Buen Negocio n° 6. 2006

SANTACREU RÍOS, Luis Juan, "Comunicaciones y transmisiones. Aspectos Técnicos", Colección Manuales Docentes n° 21 Seguridad y Emergencias. Universidad de las Palmas de Gran Canaria, 2008.

SIERRA, Jorge (LU1AS). "Conceptos generales sobre comunicaciones de emergencia". Coordinador de Emergencias de IARU - Región 2.

"The Federal Response to Hurricane Katrina: lessons learned". The White House Reports. September 2005.

PÁGINAS WEB CONSULTADAS

- Actualidad Humanitaria. Plataforma de Información sobre acción humanitaria.
  www.actualidadhumanitaria.com
- Agencia Española de Cooperación Internacional para el Desarrollo (AECID).
  www.aecid.es
- Asociación de Ususarios de Internet.
  www.aui.ws
- Australian Emergency Management.
  www.em.gov.au
- Comité Internacional de la Cruz Roja (CICR).
  www.icrc.org
- Command & Control Centre of Excellence.
  www.c2coe.org
- Correos.
  www.correos.es
- Crisis and Emergency Risk Communication.
  www.bt.cdc.gov
- Departamento de Seguridad del Territorio Nacional de los EEUU.
  www.dhs.gov
- Direccion General de Proteccion Civil y Emergencias.
  www.proteccioncivil.org
- Escuela CIS de la OTAN.
  www.nciss.nato.int
- Estrategia Internacional de las Naciones para la Reducción de Desastres (UNISDR).
  www.unisdr.org
- Federal Emergency Management Agency.
  www.fema.gov
- Fundación Madri+d.
  www.madrimasd.org
- Global Disaster Alert and Coordination System.
  www.gdacs.org
- Marina Mercante.
  www.fomento.gob.es/direcciones_generales/marina_mercante
- Ministerio de Agricultura.
  www.magrama.gob.es
- Oficina de Asuntos Gubernamentales y del Consumidor, de la Comisión Federal de Comunicaciones de los EEUU.
  www.fcc.gov
- Oficina de Ayuda Humanitaria de la Comisión Europea (ECHO).
  www.ec.europa.eu/echo
- Oficina para la Coordinación de los Asuntos Humanitarios de Naciones Unidas (OCHA).
  www.unocha.org
- Pacific Disater Centre.
  www.pdc.org/iweb
- Portal Emergency Response Centre ERC.
  ercportal.jrc.ec.europa.eu
- Portal General de Emergencias.
  www.e-mergencia.com
- Proyecto GEMYC-D (Gestión de Emergencias Distribuido), desarrollado por FEDETEC y el Departamento de Ingeniería de Sistemas Telemáticos de la UPM.
  web.dit.upm.es
- Real Academia Española
  www.rae.es
- Redhum.
  www.redhum.org
- RENEM.
  portal.renem.es
- Telecomunicaciones de Emergencia.
  emercomms.ipellejero.es
- Unión Europea.
  ec.europa.eu/echo/policies/disaster_response
- Unión Internacional de Telecomunicaciones.
  www.itu.int
- US Department of Homeland Security, SAFECOM program.
  www.safecomprogram.gov
- Virtual OSOCC.
  vosocc.unocha.org
- Web Relief.
  www.reliefweb.int
- Wikitel.
  es.wikitel.info
- Wikipedia.
  es.wikipedia.org

Perfil del autor en Twitter
@RodolfoArroyoR

Página del autor en Facebook
"Rodolfo Arroyo"

Página del libro en Facebook
"El enlace en las emergencias"

Perfil del autor en Google +
"Rodolfo Arroyo de la Rosa"

Perfil del autor en LinkedIn
"Rodolfo Arroyo de la Rosa"

ANEXO 1

ADHESION DE ESPAÑA AL CONVENIO DE TAMPERE

6084.- INSTRUMENTO de Adhesión de España al Convenio de Tampere sobre el suministro de recursos de telecomunicaciones para la mitigación de catástrofes y las operaciones de socorro en caso de catástrofes, hecho en Tampere el 18 de junio de 1998.

JUAN CARLOS I REY DE ESPAÑA

Concedida por las Cortes Generales la autorización prevista en el artículo 94.1 de la Constitución y, por consiguiente, cumplidos los requisitos exigidos por la Legislación española, extiendo el presente Instrumento de Adhesión de España al Convenio de Tampere sobre el suministro de recursos de telecomunicaciones para la mitigación de catástrofes y las operaciones de socorro en caso de catástrofes, hecho en Tampere (Finlandia) el 18 de junio de 1998 para que mediante su depósito y, de conformidad con lo dispuesto en su artículo 12, España pase a ser Parte de dicho Convenio.

En fe de lo cual firmo el presente Instrumento, debidamente sellado y refrendado por el infrascrito Ministro de Asuntos Exteriores y de Cooperación, con la siguiente reserva:

«En la medida en que ciertas disposiciones del Convenio de Tampere sobre el suministro de recursos de telecomunicaciones para la mitigación de catástrofes y las operaciones de socorro en caso de catástrofe, están comprendidas en el área de responsabilidad de la Comunidad Europea, España no podrá implementar dichas decisiones. Para este objeto las Comunidades Europeas deben ser Parte del Convenio.»

Dado en Madrid, a 10 de febrero de 2006.

JUAN CARLOS R.

El Ministro de Asuntos Exteriores y de Cooperación,
MIGUEL ÁNGEL MORATINOS CUYAUBÉ

CONVENIO DE TAMPERE SOBRE EL SUMINISTRO DE RECURSOS DE TELECOMUNICACIONES PARA LA MITIGACIÓN DE CATÁSTROFES Y LAS OPERACIONES DE SOCORRO EN CASO DE CATÁSTROFE

Los Estados Partes en el presente Convenio, Reconociendo que la magnitud, complejidad, frecuencia y repercusiones de las catástrofes están aumentando a un ritmo extraordinario, lo que afecta de forma particularmente grave a los países en desarrollo,

Recordando que los organismos humanitarios de socorro y asistencia requieren recursos de telecomunicaciones fiables y flexibles para realizar sus actividades vitales,

Recordando además la función esencial de los recursos de telecomunicaciones para facilitar la seguridad del personal de socorro y asistencia humanitaria,

Recordando asimismo la función vital de la radiodifusión para difundir en caso de catástrofe información precisa a las poblaciones amenazadas,

Convencidos de que el despliegue eficaz y oportuno de los recursos de telecomunicaciones y un flujo de información rápido, eficaz, exacto y veraz resultan esenciales para reducir la pérdida de vidas y el sufrimiento humanos y los daños a las cosas y al medio ambiente ocasionados por las catástrofes,

Preocupados por el impacto de las catástrofes en las instalaciones de telecomunicaciones y el flujo de información,

Conscientes de las necesidades especiales de asistencia técnica de los países menos desarrollados y propensos a las catástrofes, con objeto de producir recursos de telecomunicaciones para la mitigación de catástrofes y las operaciones de socorro,

Reafirmando la absoluta prioridad adjudicada a las comunicaciones de emergencia para salvar vidas humanas en más de cincuenta instrumentos jurídicos internacionales y, concretamente, en la Constitución de la Unión Internacional de Telecomunicaciones,

Tomando nota de la historia de la cooperación y coordinación internacionales en lo que concierne a la mitigación de las catástrofes y las operaciones de socorro en casos de catástrofe, lo que incluye el despliegue y la utilización oportunos de los recursos de telecomunicaciones que, según se ha demostrado, contribuyen a salvar vidas humanas,

Tomando nota asimismo de las Actas de la Conferencia Internacional sobre comunicaciones de socorro en casos de catástrofe (Ginebra, 1990), en las que se señala la eficacia de los sistemas de telecomunicaciones en la reacción frente a las catástrofes y la rehabilitación subsiguiente,

Tomando nota asimismo del llamamiento urgente que se hace en la Declaración de Tampere sobre comunicaciones de socorro en casos de catástrofe (Tampere, 1991) en favor de unos sistemas fiables de telecomunicaciones para la mitigación de las catástrofes y las operaciones de socorro y de la preparación de un convenio internacional sobre comunicaciones en caso de catástrofe que facilite la utilización de esos sistemas,

Tomando nota asimismo de la Resolución 44/236 de la Asamblea General de las Naciones Unidas, en la que se proclama el período 1990-2000 Decenio Internacional para la reducción de los desastres naturales, y la Resolución 46/182, en la que se pide una intensificación de la coordinación internacional de la asistencia humanitaria de emergencia,

Tomando nota asimismo del destacado papel que se asigna a los recursos de comunicaciones en la Estrategia y Plan de Acción de Yokohama en favor de un mundo más seguro, aprobados por la Conferencia Mundial sobre reducción de desastres naturales, celebrada en Yokohama en 1994,

Tomando nota asimismo de la Resolución 7 de la Conferencia Mundial de Desarrollo de las Telecomunicaciones (Buenos Aires, 1994), reafirmada en la Resolución 36 de la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones (Kyoto, 1994), en la que se insta a los gobiernos a que tomen todas las disposiciones prácticas necesarias para facilitar el rápido despliegue y el uso eficaz del equipo de telecomunicaciones, con objeto de mitigar los efectos de las catástrofes y para las operaciones de socorro en caso de catástrofe, reduciendo y, cuando sea posible, suprimiendo los obstáculos reglamentarios e intensificando la cooperación entre los Estados,

Tomando nota asimismo de la Resolución 644 de la Conferencia Mundial de Radiocomunicaciones (Ginebra, 1997), en la que se insta a los gobiernos a dar su pleno apoyo a la adopción del presente Convenio y su aplicación en el plano nacional,

Tomando nota asimismo de la Resolución 19 de la Conferencia Mundial de Desarrollo de las Telecomunicaciones (La Valetta, 1998), en la que se insta a los gobiernos a que prosigan el examen del presente Convenio para determinar si contemplan apoyar la adopción del mismo,

Tomando nota asimismo de la Resolución 51/94 de la Asamblea General de las Naciones Unidas, en la que se propugna la creación de un procedimiento transparente y ordenado para poner en práctica mecanismos eficaces para la coordinación de la asistencia en caso de catástrofe, así como para la introducción de ReliefWeb como sistema mundial de información para la difusión de información fiable y oportuna sobre emergencias y catástrofes naturales,

Remitiéndose a las conclusiones del Grupo de Trabajo sobre telecomunicaciones de emergencia en lo que concierne al papel crucial que desempeñan las telecomunicaciones en la mitigación de los efectos de las catástrofes y en las operaciones de socorro en caso de catástrofe,

Apoyándose en las actividades de un gran número de Estados, organismos de las Naciones Unidas, organizaciones gubernamentales, intergubernamentales y no gubernamentales, organismos humanitarios, proveedores de equipo y servicios de telecomunicaciones, medios de comunicación social, universidades y organizaciones de socorro, con objeto de mejorar y facilitar las comunicaciones en caso de catástrofe,

Deseosos de garantizar una aportación rápida y fiable de recursos de telecomunicaciones para atenuar los efectos de las catástrofes y realizar operaciones de socorro en caso de catástrofe, y

Deseosos además de facilitar la cooperación internacional para mitigar el impacto de las catástrofes, han convenido en lo siguiente:

ARTÍCULO 1. DEFINICIONES.

A los efectos del presente Convenio, salvo cuando el contexto en que se usan indique lo contrario, los términos que figuran a continuación tendrán el significado que se especifica:

1. Por «Estado Parte» se entiende todo Estado que haya manifestado su consentimiento en obligarse por el presente Convenio.

2. Por «Estado Parte asistente» se entiende un Estado Parte en el presente Convenio que proporcione asistencia de telecomunicaciones en aplicación del Convenio.

3. Por «Estado Parte solicitante» se entiende un Estado Parte en el presente Convenio que solicite asistencia de telecomunicaciones en aplicación del Convenio.

4. Por «el presente Convenio» se entiende el Convenio de Tampere sobre el suministro de recursos de telecomunicaciones para la mitigación de catástrofes y las operaciones de socorro en caso de catástrofe.

5. Por «depositario» se entiende el depositario del presente Convenio según lo estipulado en el artículo 16.

6. Por «catástrofe» se entiende una grave perturbación del funcionamiento de la sociedad que suponga una amenaza considerable y generalizada para la vida humana, la salud, las cosas o el medio ambiente, con independencia de que la catástrofe sea ocasionada por un accidente, la naturaleza o las actividades humanas y de que sobrevenga súbitamente o como resultado de un proceso dilatado y complejo.

7. Por «mitigación de catástrofes» se entiende las medidas encaminadas a prevenir, predecir, observar y/o mitigar los efectos de las catástrofes, así como para prepararse y reaccionar ante las mismas.

8. Por «peligro para la salud» se entiende el brote repentino de una enfermedad infecciosa, por ejemplo, una epidemia o pandemia, o cualquier otro evento que amenace de manera significativa la vida o la salud humanas y pueda desencadenar una catástrofe.

9. Por «peligro natural» se entiende un evento o proceso, como terremotos, incendios, inundaciones, vendavales, desprendimientos de tierras, aludes, ciclones, tsunamis, plagas de insectos, sequías o erupciones volcánicas, que puedan desencadenar una catástrofe.

10. Por «organización no gubernamental» se entiende toda organización, incluidas las entidades privadas o sociedades, distinta del Estado o de una organización gubernamental o intergubernamental, interesada en la mitigación de las catástrofes y las operaciones de socorro o en el suministro de recursos de telecomunicaciones para la mitigación de las catástrofes y las operaciones de socorro.

11. Por «entidad no estatal» se entiende toda entidad, distinta del Estado, con inclusión de las organizaciones no gubernamentales y del Movimiento de la Cruz Roja y de la Media Luna Roja, interesada en la mitigación de las catástrofes y en las operaciones de socorro o en el suministro de recursos de telecomunicaciones para la mitigación de las catástrofes y las operaciones de socorro.

12. Por «operaciones de socorro» se entiende las actividades orientadas a reducir la pérdida de vidas y el sufrimiento humano y los daños materiales y/o al medio ambiente como consecuencia de una catástrofe.

13. Por «asistencia de telecomunicaciones» se entiende la prestación de recursos de telecomunicaciones o de cualquier otro recurso o apoyo destinado a facilitar la utilización de los recursos de telecomunicaciones.

14. Por «recursos de telecomunicaciones» se entiende el personal, el equipo, los materiales, la información, la capacitación, el espectro de radiofrecuencias, las redes o los medios de transmisión o cualquier otro recurso que requieran las telecomunicaciones.

15. Por «telecomunicaciones» se entiende la transmisión, emisión o recepción de signos, señales, mensajes escritos, imágenes, sonido o información de toda índole, por cable, ondas radioeléctricas, fibra óptica u otro sistema electromagnético.

ARTÍCULO 2. COORDINACIÓN.

1. El coordinador del socorro de emergencia de las Naciones unidas será el coordinador de las operaciones a los efectos del presente Convenio y cumplirá las funciones de coordinador de las operaciones especificadas en los artículos 3, 4, 6, 7, 8 y 9.

2. El coordinador de las operaciones recabará la cooperación de otros organismos apropiados de las Naciones Unidas, particularmente la Unión Internacional de Telecomunicaciones, para que le asistan en la consecución de los objetivos del presente Convenio y, en particular, el cumplimiento de las funciones indicadas en los artículos 8 y 9, y para proporcionar el apoyo técnico necesario en consonancia con el objeto respectivo de dichos organismos.

3. Las responsabilidades del coordinador de las operaciones en el marco del presente Convenio estarán circunscritas a las actividades de coordinación de carácter internacional.

ARTÍCULO 3. DISPOSICIONES GENERALES.

1. Los Estados Partes cooperarán entre sí y con las entidades no estatales y las organizaciones intergubernamentales, de conformidad con lo dispuesto en el presente Convenio, para facilitar la utilización de los recursos de telecomunicaciones para la mitigación de catástrofes y las operaciones de socorro en caso de catástrofe.

2. Dicha utilización podrá consistir, entre otras cosas, en lo siguiente:

a) la instalación de equipo de telecomunicaciones terrenales y por satélite para predecir y observar peligros naturales, peligros para la salud y catástrofes, así como para proporcionar información en relación con estos eventos;

b) el intercambio entre los Estados Partes y entre éstos y otros Estados, entidades no estatales y organizaciones intergubernamentales de información acerca de peligros naturales, peligros para la salud y catástrofes, así como la comunicación de dicha información al público, particularmente a las comunidades amenazadas;

c) el suministro sin demora de asistencia de telecomunicaciones para mitigar los efectos de una catástrofe; y

d) la instalación y explotación de recursos fiables y flexibles de telecomunicaciones destinados a las organizaciones de socorro y asistencia humanitarias.

3. Para facilitar dicha utilización, los Estados Partes podrán concertar otros acuerdos o arreglos multinacionales o bilaterales.

4. Los Estados Partes pedirán al coordinador de las operaciones que, en consulta con la Unión Internacional de Telecomunicaciones, el depositario, otras entidades competentes de las Naciones Unidas y organizaciones intergubernamentales y no gubernamentales, haga todo lo posible, de conformidad con lo dispuesto en el presente Convenio, para:

a) elaborar, en consulta con los Estados Partes, modelos de acuerdo que puedan servir de base para concertar acuerdos multilaterales o bilaterales que faciliten el suministro de recursos de telecomunicaciones para mitigar catástrofes y realizar operaciones de socorro;

b) poner a disposición de los Estados Partes, de otros Estados, entidades no estatales y organizaciones intergubernamentales, por medios electrónicos y otros mecanismos apropiados, modelos de acuerdo, mejores prácticas y otra información pertinente con referencia al suministro de recursos de telecomunicaciones para la mitigación de catástrofes y operaciones de socorro en caso de catástrofe;

c) elaborar, aplicar y mantener los procedimientos y sistemas de acopio y difusión de información que resulten necesarios para aplicar el Convenio; y

d) informar a los Estados acerca de las disposiciones del presente Convenio, así como facilitar y apoyar la cooperación entre los Estados Partes prevista en el Convenio.

5. Los Estados Partes cooperarán para mejorar la capacidad de las organizaciones gubernamentales, las entidades no estatales y las organizaciones intergubernamentales que permita establecer mecanismos de entrenamiento en técnicas de manejo y operación de los equipos, así como cursos de aprendizaje en innovación, diseño y construcción de elementos de telecomunicaciones de emergencia que faciliten la prevención, monitoreo y mitigación de las catástrofes.

ARTÍCULO 4. PRESTACIÓN DE ASISTENCIA DE TELECOMUNICACIONES.

1. El Estado Parte que requiera asistencia de telecomunicaciones para mitigar los efectos de una catástrofe y efectuar operaciones de socorro podrá recabarla de cualquier otro Estado Parte, sea directamente o por conducto del coordinador de las operaciones. Si la solicitud se efectúa por conducto del coordinador de las operaciones, éste comunicará inmediatamente dicha solicitud a los demás Estados Partes interesados. Si la asistencia se recaba directamente de otro Estado Parte, el Estado Parte solicitante informará lo antes posible al coordinador de las operaciones.

2. El Estado Parte que solicite asistencia de telecomunicaciones especificará el alcance y el tipo de asistencia requerida, así como las medidas tomadas en aplicación de los artículos 5 y 9 del presente Convenio y, en lo posible, proporcionará al Estado Parte a quien se dirija la petición de asistencia y/o al coordinador de las operaciones cualquier otra información necesaria para determinar en qué medida dicho Estado Parte puede atender la petición.

3. El Estado Parte a quien se dirija una solicitud de asistencia de telecomunicaciones, sea directamente o por conducto del coordinador de las operaciones, determinará y comunicará sin demora al Estado Parte solicitante si va a proporcionar la asistencia requerida, sea o no directamente, así como el alcance, las condiciones, las restricciones y, en su caso, el coste de dicha asistencia.

4. El Estado Parte que decida suministrar asistencia de telecomunicaciones lo pondrá en conocimiento del coordinador de las operaciones a la mayor brevedad.

5. Los Estados Partes no proporcionarán ninguna asistencia de telecomunicaciones en aplicación del presente Convenio sin el consentimiento del Estado Parte solicitante, el cual conservará la facultad de rechazar total o parcialmente la asistencia de telecomunicaciones ofrecida por otro Estado Parte en cumplimiento del presente Convenio, de conformidad con su propia legislación y política nacional.

6. Los Estados Partes reconocen el derecho de un Estado Parte solicitante a pedir directamente asistencia de telecomunicaciones a entidades no estatales y organizaciones intergubernamentales, así como el derecho de toda entidad no estatal y entidad gubernamental a proporcionar, de acuerdo con la legislación a la que estén sometidas, asistencia de telecomunicaciones a los Estados Partes solicitantes con arreglo al presente artículo.

7. Una entidad no estatal no puede ser «Estado Parte solicitante» ni pedir asistencia de telecomunicaciones en virtud del presente Convenio.

8. Nada de lo dispuesto en el presente Convenio menoscabará el derecho de los Estados Partes a dirigir, controlar, coordinar y supervisar, al amparo de su legislación nacional, la asistencia de telecomunicaciones proporcionada de acuerdo con el presente Convenio dentro de su territorio.

ARTÍCULO 5. PRIVILEGIOS, INMUNIDADES Y FACILIDADES.

1. El Estado Parte solicitante concederá, en la medida en que lo permita su legislación nacional, a las personas físicas que no sean nacionales suyos, así como a las organizaciones que no tengan su sede o su domicilio dentro de su territorio, que actúen con arreglo a lo dispuesto en el presente Convenio para prestar asistencia de telecomunicaciones y que hayan sido notificadas al Estado Parte solicitante y aceptadas por éste, los privilegios, inmunidades y facilidades necesarios para el desempeño adecuado de sus funciones, lo que incluye:

a) inmunidad de arresto o detención o de la jurisdicción penal, civil y administrativa del Estado Parte solicitante, por actos u omisiones

relacionados específica y directamente con el suministro de asistencia de telecomunicaciones;

b) exoneración de impuestos, aranceles u otros gravámenes, con excepción de los incorporados normalmente en el precio de los bienes o servicios, en lo que concierne al desempeño de sus funciones de asistencia, o sobre el equipo, los materiales y otros bienes transportados al territorio del Estado Parte solicitante o adquiridos en éste para prestar asistencia de telecomunicaciones en virtud del presente Convenio;

c) inmunidad contra la confiscación, el embargo o la requisa de dichos equipos, materiales y bienes.

2. En la medida de sus capacidades, el Estado Parte solicitante proporcionará instalaciones y servicios locales para la adecuada y eficaz administración de la asistencia de telecomunicaciones, y cuidará de que se expida sin tardanza la correspondiente licencia al equipo de telecomunicaciones transportado a su territorio en aplicación del presente Convenio, o de que éste sea exonerado de licencia con arreglo a su legislación y reglamentos nacionales.

3. El Estado Parte solicitante garantizará la protección del personal, el equipo y los materiales transportados a su territorio con arreglo a lo estipulado en el presente Convenio.

4. El derecho de propiedad sobre el equipo y los materiales proporcionados en aplicación del presente Convenio no quedará afectado por su utilización de conformidad con lo dispuesto en el mismo. El Estado Parte solicitante garantizará la pronta devolución de dicho equipo, material y bienes al Estado Parte asistente.

5. El Estado Parte solicitante no destinará la instalación o utilización de los recursos de telecomunicaciones proporcionados en aplicación del presente Convenio a fines que no estén directamente relacionados con la predicción, la observación y la mitigación de los efectos de una catástrofe, o con las actividades de preparación y reacción ante ésta o la realización de las operaciones de socorro durante y después de la misma.

6. Lo dispuesto en el presente artículo no obligará a ningún Estado Parte solicitante a conceder privilegios e inmunidades a sus nacionales o residentes permanentes, ni tampoco a las organizaciones con sede o domicilio en su territorio.

7. Sin perjuicio de los privilegios e inmunidades que se les haya concedido de conformidad con el presente artículo, todas las personas que accedan al territorio de un Estado Parte con el objeto de proporcionar asistencia de telecomunicaciones o de facilitar de otro modo la utilización de los recursos de telecomunicaciones en aplicación del presente Convenio, y las organizaciones que proporcionen asistencia de telecomunicaciones o faciliten de otro modo la utilización de los recursos de telecomunicaciones en virtud del presente Convenio, deberán respetar las leyes y reglamentos de dicho Estado Parte. Esas personas y organizaciones no interferirán en los asuntos internos del Estado Parte a cuyo territorio hayan accedido.

8. Lo dispuesto en el presente artículo se entenderá sin perjuicio de los derechos y obligaciones con respecto a los privilegios e inmunidades concedidos a las personas y organizaciones que participen directa o indirectamente en la asistencia de telecomunicaciones, en aplicación de otros acuerdos internacionales (incluidos la Convención sobre prerrogativas e inmunidades de las Naciones Unidas, adoptada por la Asamblea General el 13 de febrero de 1946, y la Convención sobre prerrogativas e inmunidades de los Organismos Especializados, adoptada por la Asamblea General el 21 de noviembre de 1947) o del derecho internacional.

ARTÍCULO 6. TERMINACIÓN DE LA ASISTENCIA.

1. En cualquier momento y mediante notificación escrita, el Estado Parte solicitante o el Estado Parte asistente podrán dar por terminada la asistencia de telecomunicaciones recibida o proporcionada en virtud del artículo 4. Recibida dicha notificación, los Estados Partes interesados consultarán entre sí para proceder de forma adecuada y ordenada a la terminación de dicha asistencia, teniendo presentes los posibles efectos de dicha terminación para la vida humana y para las operaciones de socorro en curso.

2. Los Estados Partes que proporcionen o reciban asistencia de telecomunicaciones en cumplimiento del presente Convenio quedarán sujetos a las disposiciones de éste una vez terminada dicha asistencia.

3. El Estado Parte que solicite la terminación de la asistencia de telecomunicaciones lo comunicará al coordinador de las operaciones, el cual proporcionará la ayuda solicitada y necesaria para facilitar la terminación de la asistencia de telecomunicaciones.

ARTÍCULO 7. PAGO O REEMBOLSO DE GASTOS O CÁNONES.

1. Los Estados Partes podrán subordinar la prestación de asistencia de telecomunicaciones para mitigar catástrofes y realizar operaciones de socorro a un acuerdo de pago o reembolso de los gastos o cánones especificados, teniendo siempre presente lo preceptuado en el párrafo 9 del presente artículo.

2. Cuando se planteen estas condiciones, los Estados Partes establecerán por escrito, con anterioridad al suministro de la asistencia de telecomunicaciones:

a) la obligación de pago o reembolso;

b) el importe de dicho pago o reembolso o las bases sobre las cuales éste haya de calcularse; y

c) cualquier otra condición o restricción aplicable a dicho pago o reembolso, con inclusión, en particular, de la moneda en que habrá de efectuarse dicho pago o reembolso.

3. Las condiciones estipuladas en los párrafos 2 b) y 2 c) del presente artículo podrán ser satisfechas sobre la base de tarifas, tasas o precios comunicados al público.

4. Para que la negociación de los acuerdos de pago o reembolso no retrase indebidamente la prestación de asistencia de telecomunicaciones, el coordinador de las operaciones preparará, en consulta con los Estados Partes, un modelo de acuerdo de pago o reembolso que podrá servir de base para negociar las obligaciones de pago o reembolso en el marco del presente artículo.

5. Ningún Estado Parte estará obligado a abonar o reembolsar gastos o cánones con arreglo al presente Convenio si no ha aceptado expresamente las condiciones establecidas por el Estado Parte asistente de conformidad con lo dispuesto en el párrafo 2 del presente artículo.

6. Si la prestación de asistencia de telecomunicaciones está subordinada al pago o reembolso de gastos o cánones con arreglo al presente artículo, dicho pago o reembolso se efectuará sin demora una vez que el Estado Parte asistente haya solicitado el pago o reembolso.

7. Las cantidades abonadas o reembolsadas por un Estado Parte solicitante en relación con la prestación de asistencia de telecomunicaciones podrán transferirse libremente fuera de la jurisdicción del Estado Parte solicitante sin retraso ni retención alguna.

8. Para determinar si debe condicionarse la prestación de asistencia de telecomunicaciones a un acuerdo sobre el pago o reembolso de los gastos o cánones que se especifiquen, así como sobre el importe de tales gastos o cánones y las condiciones y restricciones aplicables, los Estados Partes tendrán en cuenta, entre otros factores pertinentes, los siguientes:

a) los principios de las Naciones Unidas sobre la asistencia humanitaria;

b) la índole de la catástrofe, peligro natural o peligro para la salud de que se trate;

c) los efectos o los posibles efectos de la catástrofe;

d) el lugar de origen de la catástrofe;

e) la zona afectada o potencialmente afectada por la catástrofe;

f) la existencia de catástrofes anteriores y la probabilidad de que se produzcan en el futuro catástrofes en la zona afectada;

g) la capacidad del Estado afectado por la catástrofe, peligro natural o peligro para la salud para prepararse o reaccionar ante dicho evento; y

h) las necesidades de los países en desarrollo.

9. El presente artículo se aplicará también a las situaciones en que la asistencia de telecomunicaciones sea prestada por una entidad no estatal o una organización gubernamental, siempre que:

a) el Estado Parte solicitante haya dado su acuerdo al suministro de asistencia de telecomunicaciones para la mitigación de la catástrofe y las operaciones de socorro y no haya puesto término a la misma;

b) la entidad no estatal o la organización intergubernamental que proporcione esa asistencia de telecomunicaciones haya notificado al Estado Parte solicitante su voluntad de aplicar el presente artículo y los artículos 4 y 5;

c) la aplicación del presente artículo no sea incompatible con ningún otro acuerdo referente a las relaciones entre el Estado Parte solicitante y la entidad no estatal o la organización intergubernamental que preste esa asistencia de telecomunicaciones.

ARTÍCULO 8. INVENTARIO DE INFORMACIÓN SOBRE ASISTENCIA DE TELECOMUNICACIONES.

1. Los Estados Partes comunicarán al coordinador de las operaciones la autoridad o autoridades:

a) competentes en los asuntos derivados de las disposiciones del presente Convenio y autorizadas para solicitar, ofrecer, aceptar o dar por terminada la asistencia de telecomunicaciones;

b) competentes para identificar los recursos gubernamentales, intergubernamentales o no gubernamentales que podrían ponerse a disposición para facilitar la utilización de recursos de telecomunicaciones para la mitigación de catástrofes y operaciones de socorro, incluida la prestación de asistencia de telecomunicaciones.

2. Los Estados Partes procurarán comunicar sin demora al coordinador de las operaciones los cambios que se hayan producido en la información suministrada en cumplimiento del presente artículo.

3. El coordinador de las operaciones podrá aceptar la notificación por parte de una entidad no estatal o una organización intergubernamental de su propio procedimiento aplicable a la autorización para ofrecer y dar por terminada la asistencia de telecomunicaciones que suministre según lo previsto en el presente artículo.

4. Los Estados Partes, las entidades no estatales o las organizaciones intergubernamentales podrán incluir a su discreción en el material que depositen en poder del coordinador de las operaciones información sobre

recursos específicos de telecomunicaciones y sobre planes para el empleo de dichos recursos en respuesta a una petición de asistencia de telecomunicaciones por un Estado Parte.

5. El coordinador de las operaciones conservará las copias de todas las listas de autoridades y comunicará sin tardanza esa información a los Estados Partes, a otros Estados, a las entidades no estatales y las organizaciones intergubernamentales interesadas, salvo cuando un Estado Parte, una entidad no estatal o una organización intergubernamental haya indicado previamente por escrito que se restrinja la distribución de su información.

6. El coordinador de las operaciones tratará de igual modo el material depositado por entidades no estatales y organizaciones intergubernamentales que el depositado por Estados Partes.

ARTÍCULO 9. OBSTÁCULOS REGLAMENTARIOS.

1. En lo posible y de conformidad con su legislación nacional, los Estados Partes reducirán o suprimirán los obstáculos reglamentarios a la utilización de recursos de telecomunicaciones para mitigar catástrofes y realizar operaciones de socorro, incluida la prestación de asistencia de telecomunicaciones.

2. Entre los obstáculos reglamentarios figuran los siguientes:

a) normas que restringen la importación o exportación de equipos de telecomunicaciones;

b) normas que restringen la utilización de equipo de telecomunicaciones o del espectro de radiofrecuencias;

c) normas que restringen el movimiento del personal que maneja el equipo de telecomunicaciones o que resulta esencial para su utilización eficaz;

d) normas que restringen el tránsito de recursos de telecomunicaciones por el territorio de un Estado Parte; y

e) retrasos en la administración de dichas normas.

3. La reducción de los obstáculos reglamentarios podrá adoptar, entre otras, las siguientes formas:

a) revisar las disposiciones;

b) exonerar a ciertos recursos de telecomunicaciones de la aplicación de dichas normas mientras se están utilizando para mitigar catástrofes y realizar operaciones de socarro;

c) el despacho en aduana anticipado de los recursos de telecomunicaciones destinados a la mitigación de catástrofes y operaciones de socorro, de conformidad con dichas disposiciones;

d) el reconocimiento de la homologación extranjera del equipo de telecomunicaciones y de las licencias de explotación;

e) la inspección simplificada de los recursos de telecomunicaciones destinados a la mitigación de catástrofes y operaciones de socorro, de conformidad con dichas disposiciones; y

f) la suspensión temporal de la aplicación de dichas disposiciones en lo que respecta a la utilización de los recursos de telecomunicaciones para mitigar catástrofes y realizar operaciones de socorro.

4. Cada Estado Parte facilitará, a instancia de los demás Estados Partes y en la medida en que lo permita su legislación nacional, el tránsito hacia su territorio, así como fuera y a través de éste, del personal, el equipo, los materiales y la información que requiera la utilización de recursos de telecomunicaciones para mitigar una catástrofe y realizar operaciones de socorro.

5. Los Estados Partes informarán al coordinador de las operaciones y a los demás Estados Partes, sea directamente o por conducto del coordinador de las operaciones, de:

a) las medidas adoptadas en aplicación del presente Convenio para reducir o eliminar los referidos obstáculos reglamentarios;

b) los procedimientos que pueden seguir, en aplicación del presente Convenio, los Estados Partes, otros Estados, entidades no estatales u organizaciones intergubernamentales para eximir a los recursos de telecomunicaciones especificados que se utilicen para mitigar catástrofes y realizar operaciones de socorro de la aplicación de dichas disposiciones, para aplicar el despacho en aduana anticipado o la inspección simplificada de tales recursos en consonancia con las normas pertinentes, aceptar la homologación extranjera de esos recursos o suspender temporalmente la aplicación de disposiciones que serían normalmente aplicables a dichos recursos; y

c) las condiciones y, en su caso, restricciones, referentes a la aplicación de dichos procedimientos.

6. El coordinador de las operaciones comunicará periódicamente y sin tardanza a los Estados Partes, a otros Estados, a entidades no estatales y organizaciones intergubernamentales una lista actualizada de tales medidas, con indicación del alcance, las condiciones y, en su caso, restricciones aplicables.

7. Nada de lo dispuesto en el presente artículo permitirá la violación o abrogación de las obligaciones y responsabilidades impuestas por la legislación nacional, el derecho internacional o acuerdos multilaterales o bilaterales, incluidas las obligaciones y responsabilidades en materia de inspección aduanera y controles a la exportación.

ARTÍCULO 10. RELACIÓN CON OTROS ACUERDOS INTERNACIONALES.

El presente Convenio no afectará a los derechos y obligaciones de los

Estados Partes derivados de otros acuerdos internacionales o del derecho internacional.

ARTÍCULO 11. SOLUCIÓN DE CONTROVERSIAS.

1. En caso de controversia entre los Estados Partes acerca de la interpretación o aplicación del presente Convenio, los Estados Partes interesados celebrarán consultas entre sí con el objeto de solucionarla. Las consultas se iniciarán sin demora una vez que un Estado Parte comunique por escrito a otro Estado Parte la existencia de una controversia relativa al presente Convenio. El Estado Parte que formule una declaración escrita en tal sentido transmitirá sin tardanza copia de la misma al depositario.

2. Si la controversia entre los Estados Partes no puede resolverse dentro de los seis (6) meses siguientes a la fecha de comunicación de la antedicha declaración escrita, los Estados Partes interesados podrán solicitar los buenos oficios de cualquier otro Estado Parte, u otro Estado, entidad no estatal u organización intergubernamental para facilitar la solución de la controversia.

3. En caso de que ninguno de los Estados Partes en la controversia solicite los buenos oficios de otro Estado Parte, u otro Estado, entidad no estatal u organización intergubernamental o si los buenos oficios no facilitan la solución de la controversia dentro de los seis (6) meses siguientes a la fecha en que se solicitaron los buenos oficios, cualquiera de los Estados Partes en la controversia podrá:

a) pedir que ésta se someta a arbitraje obligatorio; o

b) someterla a la decisión de la corte Internacional de Justicia, siempre y cuando los Estados Partes en la controversia hayan aceptado en el momento de la firma o ratificación del presente Convenio o de la adhesión al mismo o en cualquier momento posterior la jurisdicción de la Corte respecto de esa controversia.

4. En caso de que los Estados Partes en la controversia pidan que ésta se someta a arbitraje obligatorio y la sometan a la decisión de la Corte Internacional de Justicia, tendrá precedencia el procedimiento ante la Corte.

5. En caso de controversia entre un Estado Parte que solicite asistencia de telecomunicaciones y una entidad no estatal o una organización intergubernamental que tenga su sede o domicilio fuera del territorio de ese Estado Parte acerca de la prestación de asistencia de telecomunicaciones en virtud del artículo 4, la pretensión de la entidad no estatal o de la organización intergubernamental podrá ser endosada directamente por el Estado Parte en el que dicha entidad no estatal u organización intergubernamental tenga su sede o domicilio como reclamación internacional en virtud del presente artículo, siempre que ello no sea incompatible con ningún otro acuerdo existente entre el Estado Parte y la entidad no estatal o la organización intergubernamental involucrada en la controversia.

6. Al proceder a la firma, ratificación, aceptación o aprobación del presente Convenio o al adherirse al mismo, un Estado podrá declarar que no se considera obligado por los procedimientos de solución de controversia previstos en el párrafo 3 o por alguno de ellos. Los demás Estados Partes no estarán obligados por el procedimiento o los procedimientos de solución de controversias estipulados en el párrafo 3 con respecto al Estado Parte cuya declaración a tal efecto esté en vigor.

ARTÍCULO 12. ENTRADA EN VIGOR.

1. El presente Convenio estará abierto a la firma de todos los Estados Miembros de las Naciones Unidas o de la Unión Internacional de Telecomunicaciones en la Conferencia Intergubernamental sobre Telecomunicaciones de Emergencia en Tampere el 18 de junio de 1998 y, con posterioridad a esa fecha, en la Sede de las Naciones Unidas, en Nueva York, desde el 22 de junio de 1998 hasta el 21 de junio de 2003.

2. Todo Estado podrá manifestar su consentimiento en obligarse por el presente Convenio mediante:

a) la firma (firma definitiva);

b) la firma sujeta a ratificación, aceptación o aprobación, seguida del depósito de un instrumento de ratificación, aceptación o aprobación; o

c) el depósito de un instrumento de adhesión.

3. El Convenio entrará en vigor treinta (30) días después del depósito de los instrumentos de ratificación, aceptación, aprobación o adhesión o de la firma definitiva por treinta (30) Estados.

4. El presente Convenio entrará en vigor para cada Estado que lo haya firmado definitivamente o haya depositado un instrumento de ratificación, aceptación, aprobación o adhesión, una vez cumplido el requisito especificado en el párrafo 3 del presente artículo, treinta (30) días después de la fecha de la firma definitiva o de la manifestación del consentimiento en obligarse.

ARTÍCULO 13. ENMIENDAS.

1. Todo Estado Parte podrá proponer enmiendas al presente Convenio, a cuyo efecto las hará llegar al depositario, el cual las comunicará para aprobación a los demás Estados Partes.

2. Los Estados Partes notificarán al depositario si aceptan o no las enmiendas propuestas dentro de los ciento ochenta (180) días siguientes a la recepción de las mismas.

3. Las enmiendas aprobadas por dos tercios de los Estados Partes se incorporarán a un Protocolo que se abrirá a la firma de todos los Estados Partes en la sede del depositario.

4. El Protocolo entrará en vigor igual que el presente Convenio. Para los Estados que lo hayan firmado definitivamente o hayan depositado un instrumento de ratificación, aceptación, aprobación o adhesión y una vez cumplidos los requisitos estipulados al efecto, el Protocolo entrará en vigor treinta (30) días después de la fecha de la firma definitiva o de la manifestación del consentimiento en obligarse.

ARTÍCULO 14. RESERVAS.

1. Al firmar definitivamente, ratificar o adherirse al presente Convenio o a una modificación del mismo, los Estados Partes podrán formular reservas.

2. Un Estado Parte podrá retirar en todo momento las reservas que haya formulado mediante notificación escrita al depositario. El retiro de una reserva surtirá efecto en el momento de su ratificación al depositario.

ARTÍCULO 15. DENUNCIA.

1. Los Estados Partes podrán denunciar el presente Convenio mediante notificación escrita al depositario.

2. La denuncia surtirá efecto noventa (90) días después de la fecha de depósito de la notificación escrita.

3. A instancia del Estado Parte denunciante, en la fecha en que surta efecto la denuncia dejarán de utilizarse las copias de las listas de autoridades, de las medidas adoptadas y de los procedimientos existentes para reducir los obstáculos reglamentarios, que haya suministrado el Estado Parte que denuncie el presente Convenio.

ARTÍCULO 16. DEPOSITARIO.

El presente Convenio se depositará en poder del Secretario General de las Naciones Unidas.

ARTÍCULO 17. TEXTOS AUTÉNTICOS.

El original del presente Convenio, cuyos textos en árabe, chino, español, francés, inglés y ruso son igualmente auténticos, se depositará en poder del depositario. Sólo se abrirán a la firma en Tampere el 18 de junio de 1998 los textos auténticos en español, francés e inglés. El depositario preparará después lo antes posible los textos auténticos en árabe, chino y ruso.

ESTADOS PARTE

	FIRMA	FECHA DEPÓSITO INSTRUMENTO
Alemania	18-06-1998	
Argentina	11-05-1999	
Barbados		25-07-2003 AD
Benín	18-06-1998	
Brasil	12-03-1999	
Bulgaria	22-09-1999	20-06-2000 R
Burundi	18-06-1998	
Canadá	15-06-1999	18-05-2001 R
Congo	18-06-1998	
Costa Rica	20-06-2003	
Chad	20-10-1999	
Chile	18-06-1998	
Chipre	18-06-1998	14-07-2000 R
Dinamarca (*)	18-06-1998	02-06-2003 R
Dominica		26-12-2000 AD
El Salvador	09-08-2000	18-04-2002 R
Eslovaquia	16-02-2000	06-02-2001 R
España (*)		**27-02-1996 AD**
Estados Unidos	17-11-1998	
Estonia	25-05-1999	
Finlandia	18-06-1998	01-04-1999 R
Gabón	27-04-2001	
Ghana	18-06-1998	
Guinea		08-10-2002 AD

ESTADOS PARTE	FIRMA	FECHA DEPÓSITO INSTRUMENTO
Haití	11-02-1999	
Honduras	25-02-1999	
Hungría	20-06-2003	07-04-2004 R
India	29-11-1999	29-11-1999 R
Islandia	20-06-2003	
Italia	18-06-1998	
Kenya	18-06-1998	12-02-2003 R
Kuwait	18-06-1998	13-06-2002 R
Líbano	17-11-1998 2	7-01-2006 R
Liberia		16-09-2005 AD
Liechtenstein		08-06-2004 AD
Lituania		09-12-2004 AD
Macedonia, (Ex República Yugoslava de)	03-12-1998	
Madagascar	12-09-2002	
Malí	18-06-1998	
Malta	18-06-1998	
Marruecos	01-12-1998	11-03-2003 R
Mauritania	18-06-1998	
Mongolia	18-06-1998	
Nepal	23-04-1999	
Nicaragua	18-06-1998	18-11-1999 R
Níger	18-06-1998	
Omán	19-08-1999	16-04-2003 R
Países Bajos	19-12-2000	06-07-2001 R Por el Reino en Europa y Antillas Neerlandesas 17-07-2001: Aruba
Panamá	20-09-2001	05-03-2006 R
Perú	14-01-1999	27-10-2003 R
Polonia	18-06-1998	
Portugal	18-06-1998	
Reino Unido (*)		18-06-2003 AD
República Checa	04-09-2002	17-06-2003 R
Rumania	18-06-1998	17-11-2005 R
Rusia, Federación de	14-03-2002	
San Vicente y Las Granadinas	14-08-2003 AD	
Santa Lucía	31-01-2000	
Senegal	20-11-1998	
Sri Lanka	05-08-1999	13-10-1999 R
Sudán	04-12-1998	
Suecia (*)	10-06-2003	13-09-2004 R
Suiza	18-06-1998	24-04-2002 R
Tayikistán	18-06-1998	
Tonga		05-08-2003 AD
Uganda	28-10-1998	05-09-2002 R
Uruguay	13-05-2003	
Uzbekistán	06-10-1998	
Venezuela (*)	03-04-2003	13-05-2005 AD

AD: Adhesión;
R: Ratificación.
(*) Reservas y declaraciones.

El presente Convenio entró en vigor de forma general 8 de enero de 2005 y para España entrará en vigor el 29 de marzo de 2006, de conformidad con lo establecido en su artículo 12.

Lo que se hace público para conocimiento general.

Madrid, 24 de marzo de 2006.

El Secretario General Técnico del Ministerio de Asuntos Exteriores, Francisco Fernández Fábregas.

ANEXO 2

REDES ESTATALES DE GESTIÓN DE EMERGENCIAS

REMER

La Red Radio de Emergencia, como Red complementaria de la Red Radio de Mando de la Dirección General de Protección Civil y Emergencias (DGPCyE), es una organización estructurada en el ámbito nacional, constituida actualmente por cerca de 7.000 radioaficionados españoles que prestan su colaboración a los servicios oficiales de Protección Civil al ser requeridos para ello, cuando circunstancias excepcionales lo justifiquen, vinculándose voluntariamente y de modo altruista a la DGPCyE, una vez seguidos los trámites establecidos por la misma.

Su funcionamiento se basa en las comunicaciones radioeléctricas de los radioaficionados sobre unas frecuencias específicas, empleando los protocolos y disciplina de operación, previamente establecidos por la Dirección General de Protección Civil.

Orgánicamente la REMER depende de la DGPCyE, funcionalmente cada estación dependerá de su CECOP, y territorialmente de los Subdelegados o Delegados de Gobierno en las CCAA, como unidades en las que recae la dirección y coordinación de los servicios de Protección Civil a nivel provincial, pudiendo en determinados casos delegar en los alcaldes cuyos municipios estuvieran afectados.

Son objetivos de la Red Radio de Emergencia:

- Establecer un sistema de radiocomunicación en HF y VHF sobre la base de recursos privados que complemente los disponibles por la Administración General del Estado.
- Articular un mecanismo que permita a los radioaficionados colaborar con la Dirección General de Protección Civil y Emergencias, asumiendo voluntariamente los deberes que como ciudadanos/as les corresponda en los casos en que su actuación se haga necesaria.
- Facilitar a los radioaficionados integrados en la Red, su colaboración a nivel operativo y la coordinación entre ellos, así como la incorporación, en caso necesario, de aquellos otros radioaficionados que no perteneciendo a la Red, sea necesario pedir su colaboración, actuando en esta situación la REMER como un sistema de encuadramiento funcional.

La REMER se activa, de acuerdo con las situaciones de emergencia que la requieran, por el Delegado o Subdelegado del Gobierno a través del Coordinador REMER, o por el Coordinador Nacional REMER a propuesta del Director General de Protección Civil y Emergencias.

Las pautas a seguir en las emergencias son:

- Mantener personal y material especializados.
- Ejercitarse continuamente mediante ejercicios y simulacros.
- Ser reconocidos como fuente fiable de información en las situaciones reales.
- Ser claros, verídicos, objetivos y útiles en las emisiones.
- Difundir en todas direcciones, por diferentes medios para llegar a todo el mundo.
- Insistir en la seguridad, informar de los peligros sin caer en el alarmismo.
- Contribuir a la seguridad global, desarrollando la autoprotección y la solidaridad disciplinada.
- Tener preparados con anterioridad buenos intermediarios-relés.
- Adaptar los mensajes para que puedan ser entendidos por toda la población, sin ambigüedades.

Las estaciones de la REMER quedan estructuradas como sigue:

- Estación Directora Central: en el CECOP de la DGPCyE.
- Estación Directora Provincial: En los CECOP de las Delegaciones y Subdelegaciones de Gobierno.
- Estaciones de Zona: según estructuración provincial.
- Estaciones Móviles y Portátiles: para enlace con zonas aisladas y medios de intervención que se precisen.

Todas las estaciones utilizaran las frecuencias de la DGPCyE cuando su intervención sea requerida, independientemente de aquellas otras frecuencias que tengan asignadas en exclusiva por la Secretaria de Estado de Telecomunicaciones.

RENEM

La Red Nacional de Emergencias (RENEM) es un Sistema de Sistemas de Información y Telecomunicaciones que integra 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. Es un conjunto de capacidades TIC que facilitan una coordinación eficaz entre los elementos civiles y militares que participen en operaciones de gestión de crisis y de apoyo a autoridades civiles.

La RENEM tiene como misión asegurar el intercambio de información relevante para la gestión y coordinación de las emergencias de cualquier tipo. Está desplegada a nivel nacional ofreciendo un conjunto de servicios de información y telecomunicaciones a los organismos afiliados. Dicho despliegue es el resultado de los convenios de interconexión/afiliación a la RENEM que los organismos realicen tanto con el Ministerio de Defensa a través de la Unidad Militar de Emergencias.

La RENEM se basa en la interconexión de Nodos CIS. Cada uno de estos nodos 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. Está administrada por el personal del Batallón de Transmisiones de la Unidad Militar de Emergencias.

El sistema interconecta 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 ofrece un "Bus de Servicios" al que acceden todos los usuarios a través de los recursos de telecomunicaciones de la RENEM.

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

Las redes de telecomunicaciones que forman el segmento Terrestre son las siguientes:

- 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 Hacienda y Administraciones Públicas.
- WAN PG. Red de Propósito General de MINISDEF.
- Internet. Accesos Remotos con protocolos seguros.

El segmento satélite materializa las conexiones de los organismos a través de una combinación de redes satélite gubernamental/civil. La ventaja primordial de este medio es que puede garantizar el enlace de los elementos que participan en una emergencia, independientemente del lugar donde se produzcan y del estado de las infraestructuras. Las redes de telecomunicaciones vía satélite que forman este segmento son las siguientes:

- SATÉLITE GUBERNAMENTAL. Red Satélite con carga espacial gubernamental (SPAINSAT y XTAR-EU).
- SATÉLITE CIVIL. Red satélite civil de operadores públicos (INMARSAT).

SIRDEE

El Sistema de Radiocomunicaciones Digitales de Emergencia del Estado, es una red radio Trunking nacional constituida por 52 redes provinciales sobre una superficie de 550.000 kms2.

La red SIRDEE es un sistema basado en tecnología TETRAPOL cuya instalación supuso en el año 2000 el mayor avance tecnológico en España en capacidad de comunicaciones e interoperabilidad de los Cuerpos y Fuerzas de Seguridad del Estado. Con esta red, la Guardia Civil, la Policía Nacional y posteriormente la Unida Militar de Emergencias disponen de un sistema de comunicaciones con cobertura y disponibilidad plena en todo el Territorio Nacional, incluso en caso de catástrofes que afecten las comunicaciones públicas. Además, las características de seguridad de los equipos y sistemas de cifra garantizan la invulnerabilidad de las comunicaciones.

Consta de 70 centros de operaciones complejo que son el elemento de integración entre los sistemas de comunicaciones de las Fuerzas de Seguridad y la atención a las emergencias y peticiones de ayuda de los ciudadanos.

La red fue instalada y en la actualidad es mantenida por Telefónica. El proyecto también está abierto a otros servicios y unidades relacionadas con la seguridad y la coordinación de emergencias (Servicios Sanitarios, Policías Locales, etc.), que pueden integrarse en la red SIRDEE previa solicitud y posterior autorización por parte del Ministerio del Interior. La integración en SIRDEE, frente a la construcción de una red propia, es para cualquier usuario de este tipo la opción más barata: basta con adquirir los terminales, puesto que el Ministerio del Interior ya ha constituido la infraestructura de red a través de repetidores. SIRDEE garantiza una cobertura superior al 90 por ciento del Territorio Nacional a través de repetidores estáticos convencionales.

Asimismo, el Ministerio de Interior distribuye por todas las provincias repetidores de carácter portátil, que permiten conectarse a la red desde cualquier lugar del país. Estos equipos son especialmente útiles en operaciones de asistencia o rescate en casos de catástrofes o sucesos que se producen en lugares de complicada orografía, así como en investigaciones que se desarrollen en puntos remotos.

OTRAS REDES

Existen múltiples proyectos de diferentes ministerios, por desgracia independientes y sin mediar ningún tipo de coordinación entre ellos, para implantar nuevas redes.

Por ejemplo mencionaremos la iniciativa de la Conferencia Sectorial de Agricultura y Desarrollo Rural del Ministerio de Agricultura, Alimentación y Medio Ambiente (MAGRAMA) para la puesta en marcha de un sistema de información y gestión común para la lucha contra los incendios forestales.

En el borrador de Anteproyecto de Ley del Sistema Nacional de Protección Civil (enero del 2014), se hace mención a una nueva red denominada "Red Nacional de Información sobre Protección Civil" y a la "Red de Alerta Nacional de Protección Civil".


EL ENLACE EN LAS EMERGENCIAS
FUERTE Y CLARO

EL ENLACE EN LAS EMERGENCIAS • FUERTE Y CLARO •

DIRECCIÓN GENERAL
DE PROTECCIÓN CIVIL
Y EMERGENCIAS

GOBIERNO
DE ESPAÑA

MINISTERIO
DEL INTERIOR