

DANA y COITCV

Abril 2025

Orden del día

- **Colegios Profesionales ante situaciones de emergencia**
- Afectación DANA
 - Ciudadano
 - Empresas
 - Administración pública: servicios públicos, incluyendo emergencias
- Primeros días post-DANA
- Telecomunicaciones a prueba de DANA

El Colegio Oficial de Ingenieros de Telecomunicación de la Comunidad Valenciana (COITCV)

Tras la catástrofe, el Colegio Oficial de Ingenieros de Telecomunicación de la Comunidad Valenciana (COITCV) ha desempeñado un papel activo y coordinado, impulsando diversas iniciativas orientadas a la evaluación de daños, la asistencia técnica y la recuperación de infraestructuras esenciales determinando lecciones aprendidas y planes de mejora. Su actuación se ha articulado a través de varias líneas estratégicas de apoyo, así como mediante colaboraciones con instituciones, administraciones públicas y otros agentes implicados en la gestión de la emergencia y la reconstrucción. A continuación, se presentan de forma esquematizada las principales conclusiones y recomendaciones resultado de esta labor.

Orden del día

- Colegios Profesionales ante situaciones de emergencia
- **Afectación DANA**
 - Ciudadano
 - Empresas
 - Administración pública: servicios públicos, incluyendo emergencias
- Primeros días post-DANA
- Telecomunicaciones a prueba de DANA

Afectación

- **Impacto** que tuvo la Dana **en términos de líneas de comunicación** afectadas, de acuerdo a la información ministerial del número de líneas afectadas por la DANA en telefonía
 - líneas de **telefonía fija** inicialmente afectadas **220.000**
 - líneas de **telefonía móvil** inicialmente afectadas **300.000**

	Telefonía fija			Telefonía Móvil		
	Afectadas	Recuperadas	%	Afectadas	Recuperadas	%
05/11/2024	220.000	200.500	91	300.000	204.000	68
06/11/2024	220.000	202.000	92	300.000	252.000	84
07/11/2024	220.000	204.000	93	300.000	263.000	88
08/11/2024	220.000	207.000	94	300.000	274.000	91
09/11/2024	220.000	209.000	95	300.000	282.000	94
10/11/2024	220.000	210.000	95	300.000	284.000	95
11/11/2024	220.000	211.000	96	300.000	285.000	95
12/11/2024	220.000	212.000	97	300.000	287.000	96
13/11/2024	220.000	215.000	98	300.000	297.000	99
14/11/2024	220.000	216.000	98	300.000	297.000	99
15/11/2024	220.000	217.000	98	300.000	298.000	99
16/11/2024	220.000	217.000	98	300.000	298.000	99
17/11/2024	220.000	217.000	98	300.000	298.000	99

(fuente: [La Moncloa. 17/11/2024. Actualización de datos del Gobierno de España \[Info DANA\]](#))

Afectación: Ciudadano

- **7 días después de la DANA**, 5 de noviembre de 2024
 - Recuperación de 200.500 líneas de telefonía fija (**91%** de las 220.000 inicialmente afectadas)
 - Recuperación de 204.000 líneas de telefonía móvil (**68%** de las 300.000 inicialmente afectadas)
- **15 días después de la DANA**, 13 de noviembre de 2024
 - Recuperación de 215.000 líneas de telefonía fija (**98%** de las inicialmente afectadas)
 - Recuperación de 297.000 líneas de telefonía móvil (**99%** de las inicialmente afectadas)

👉 Sin embargo, muchos servicios se cubren en **precario**, con **soluciones transitorias** y **sin redundancia de la red** al perder un volumen tan alto de conexiones, lo cual deja a la red más vulnerable ante congestiones y nuevos fallos. Se reconoce que muchas de las soluciones iniciales fueron temporales y que hay que trabajar en la robustez de la infraestructura a largo plazo

Afectación: Empresas

- Las empresas, al igual que los ciudadanos, sufrieron las **mismas caídas de telefonía fija y móvil.**
 - A nivel de comunicaciones y sistemas, un aspecto de mayor impacto fue la pérdida de los **servidores y centros de datos (CPDs)**, instalados en algunas de las sedes en los polígonos industriales.
 - Los porcentajes de recuperación de los servicios en empresas no son tan altos ni tan rápidos como los generales que se han listado en el apartado de ciudadano.
- 👉 A destacar: Las empresas con un **estado de digitalización avanzado**, con back-up en la nube, pudieron **mitigar mejor la pérdida**

Afectación: Administración Pública

- Dentro de la afectación, es importante valorar qué servicios de telecomunicaciones se han visto afectados en la administración pública, ya que disponen de servicios críticos y relevantes, tales como:
 - Servicio de Emergencias (112, red COMDES,...)
 - Hospitales y centros de salud
 - Igualdad: residencias, sedes tuteladas, ..
 - Colegios
 - Juzgados
 - FGV
 - Archivo
 - Etc.

Afectación: Daños más comunes

Entre los daños más comunes se encuentran:

- **Rotura de cables:**
 - Las inundaciones y los deslizamientos de tierra provocaron la rotura de cables subterráneos, interrumpiendo las conexiones de internet, telefonía fija y móvil en numerosas zonas
- **Daños en antenas, repetidores, líneas aéreas (tanto cables como postes de madera u hormigón), armarios en intemperie, etc.:** Las fuertes ráfagas de viento, las fuertes lluvias y el arrastre y la caída de objetos dañaron antenas, repetidores, armarios de comunicaciones, postes, cables aéreos, afectando la cobertura en áreas amplias
- **Inundación de centrales telefónicas, centros de datos, infraestructura de comunicaciones en edificios, etc.:** El agua penetró en algunas instalaciones, dañando equipos electrónicos y sistemas de almacenamiento de datos
- **Alta dependencia de energía eléctrica:** Equipos de comunicaciones que dejan de funcionar, cuando la alimentación eléctrica deja de existir.
 - La autonomía de los nodos depende del nivel Jerárquico del nodo así como del estado de las baterías
 - Niveles de autonomía de más de 8 horas no suelen ser normales
- **Lodos solidificados en canalizaciones = conductos obturados**

Nota: algunos operadores pueden compartir infraestructura por lo que en una zona pueden verse afectados varios de ellos

Afectación: Daños más comunes

Entre los daños más comunes, a nivel de edificios o sedes, se encuentran:

- **Falta de suministro eléctrico**, lo que dejó inoperativas muchas instalaciones.
- **Daños en infraestructuras de telecomunicaciones de los operadores**, afectando la conectividad.
- **Problemas en el equipamiento de las sedes (instalaciones y equipos mojados)**, dificultando la operatividad interna. En este punto, es importante resaltar, que en caso la instalación interna esté muy dañada, los servicios no puedan restaurarse aunque los operadores de energía o telecomunicaciones hayan realizado su trabajo en la parte exterior o de campo.

Orden del día

- Colegios Profesionales ante situaciones de emergencia
- Afectación DANA
 - Ciudadano
 - Empresas
 - Administración pública: servicios públicos, incluyendo emergencias
- **Primeros días post-DANA**
- Telecomunicaciones a prueba de DANA

Primeros días post-DANA

Acciones que se llevaron a cabo para reestablecer los servicios de comunicaciones tanto a usuarios, como a empresas y servicios de administración pública:

- Las **operadoras de telecomunicaciones iniciaron la recuperación de servicios** afectados por inundación, caídas eléctricas, etc. Desplazaron numerosos técnicos con problemas de acceso (vías inundadas, bloqueadas, cortadas por fuerzas de seguridad). Hubo que tramitar **salvoconductos** para permitir acceso e incluso facilitar traslado de técnicos.
- Por parte de GVA, fue necesario **coordinar el reparto de recursos para dar cobertura al menos con 1 operador a todos los municipios afectados**: unidades móviles, unidades satelitales. Cuando una población tenía restablecido el servicio de algún operador se reasignaban los recursos móviles.

Primeros días post-DANA

Acciones que se llevaron a cabo para reestablecer los servicios de comunicaciones tanto a usuarios, como a empresas y servicios de administración pública:

- Puntos de **comunicación por satélite** para poder atender las comunicaciones críticas
- Reparar la **red de alimentación eléctrica** para poder reestablecer el servicio de las estaciones base, gestionando **grupos electrógenos** donde no era posible en el corto plazo
- Desplazamiento de más de una decena de **unidades móviles** (camiones) para dotar de servicio de cobertura móvil 2G, 3G, 4G y 5G a la población.

Orden del día

- Colegios Profesionales ante situaciones de emergencia
- Afectación DANA
 - Ciudadano
 - Empresas
 - Administración pública: servicios públicos, incluyendo emergencias
- Primeros días post-DANA
- **Telecomunicaciones a prueba de DANA**

Telecomunicaciones a prueba de DANA

Los eventos climáticos extremos como la DANA han puesto a prueba nuestras infraestructuras de telecomunicaciones. Ahora es el momento de reflexionar y mejorar

- Fecha: **6 de Marzo de 2025**
- Sesión dirigida a **colegiados** que quieran aportar su experiencia. **El objetivo de la reunión se ha basado en:**
 - ◆ **Impacto de la DANA** y cómo respondimos
 - ◆ **Lecciones aprendidas** de fallos y aciertos
 - ◆ **Recomendaciones para un futuro más resiliente**
- **4 vectores de análisis:** Analizaremos el problema desde **cuatro perspectivas clave:**  **Ciudadano** |  **Empresa** |  **Servicio Público** |  **Emergencias**
- **Índice:**
 - ✓ Impacto en la cobertura móvil y fija
 - ✓ Afectación en infraestructuras de comunicación: redes de acceso, transporte, conmutación, agregación y core, gestión y control, seguridad, etc.
 - ✓ Energía y telecomunicaciones
 - ✓ Efectividad de redes de emergencia y protocolos de comunicación: Tetra, 112, Sistema Red de Alerta Nacional (RAN-PWS), disponibilidad de unidades de emergencia: unidades móviles, conexión vía satélite para servicios críticos, etc.
 - ✓ Vulnerabilidades en Servidores, centros de datos, CPD's
 - ✓ Vulnerabilidad IoT
 - ✓ Comunicaciones satelitales
 - ✓ Propuestas y recomendaciones: Recomendaciones en materia de redes de emergencia y protocolos de comunicaciones de emergencia; Empresas que quieran restaurar sus sistemas "a prueba de dana"; AAPP (centros sanitarios, hospitales, colegios, ...); Normativa; ...

 **Tu conocimiento puede marcar la diferencia.** Súmate a la reunión y ayúdanos a construir telecomunicaciones más preparadas para futuras emergencias

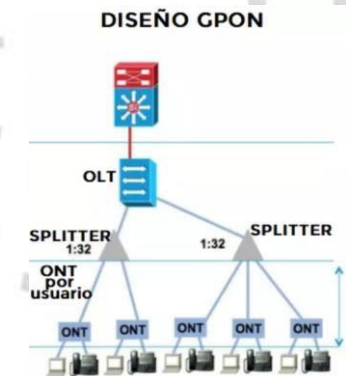
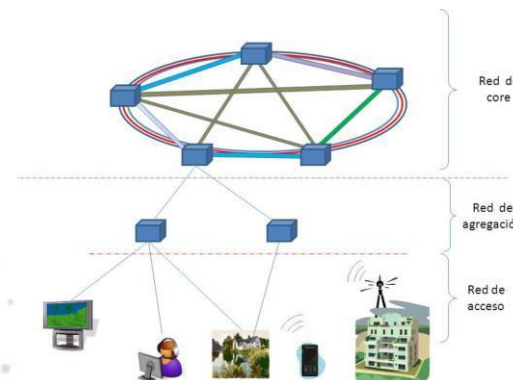
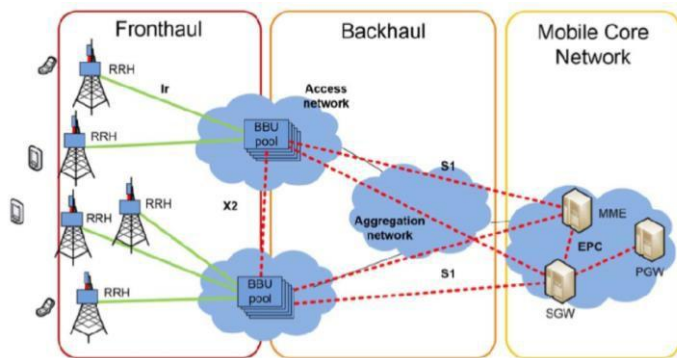
Telecomunicaciones a prueba de DANA

1. Hemos identificado a personas “clave” que puedan aportar alto valor a la sesión
 2. Garantizar que en la sesión se habla de todos estos aspectos
 - Emergencias (Tetra, 112, sistema de alerta temprana,...)
 - CPD's
 - IoT
 - Comunicaciones satelitales
 - Acceso:
 - Servicio Móvil voz/datos: Red de Acceso Radio (Estaciones base BTS-BSC/NodeB/ gNodeB /small cells/ xxx),
 - Servicio Fijo voz/datos: (xDSL, FTTx, HFC, inalámbrica (WiMAX, ...)),
 - Servicio Internet: Cualquiera de las redes de acceso para servicio móvil o fijo
 - Servicio Emergencias: Red de Acceso Radio (TETRA,...), satélite, ...
 - Otras tecnologías de acceso por si se quieren analizar: SIGFOX/LORA, ...
- Conmutación, agregación y CORE
 - Móvil: (MSC, HLR/HSS, SGSN/GGSN, ...)
 - Fijo: (DSLAM, OLT/ONT, ...), separando entre elementos que están en central telefónica y los que no lo están
 - Transporte (FO, DWDM, radio, satélite, redes IP/MPLS),
 - Servicios
 - Móvil (IMS, VoLTE, SMS, Internet,...),
 - Fijo (VoIP, IPTV, Internet,...),
 - Gestión y Control (OSS/BSS),
 - Seguridad (VPNs, FW, cifrado, ...)

Telecomunicaciones a prueba de DANA

Posibles conclusiones

- Redes telecomunicaciones, al igual que en energía, tienen un esquema jerarquizado. Se ha de clasificar los **sistemas “clave” de telecomunicaciones, y puntos críticos de fallo, para reforzar dichos puntos:**
 - Inversión en refuerzo de red de emergencias (medios humanos + técnicos)
 - Propuesta de redundancias en puntos críticos (p.e. red agregación/transporte, troncal, red de emergencias, ...) **eligiendo o combinando**, entre los distintos tipos de Redundancia en Redes de Telecomunicaciones
- 1 Redundancia de Enlaces y Tecnologías:** Uso de múltiples rutas físicas o lógicas para la transmisión de datos, combinando distintas tecnologías
 - 2 Redundancia de Equipos:** Implementación de hardware duplicado para funciones críticas.
 - 3 Redundancia de Nodos:** Duplicación de servidores, switches o nodos clave en la red.
 - 4 Redundancia de Energía:** Uso de fuentes de energía independientes para evitar fallos por cortes eléctricos. Ejemplo: UPS, generadores, alimentación dual en equipos de red.
 - 5 Redundancia de Rutas de Fibra Óptica:** Implementación de trayectorias físicas diversas para evitar cortes de fibra. Ejemplo: anillos de fibra óptica.



Telecomunicaciones a prueba de DANA

Posibles conclusiones

- **Rotura de cables:** canalizaciones robustas (prisma canalización + hormigón), en lugar de soterramientos simples, para enlaces agregados (agregación/transporte) y diversidad de caminos para proveer backup
- **Daños en antenas, repetidores, líneas aéreas (tanto cables como postes), armarios en intemperie, etc.:** diversidad de caminos para proveer backup al menos para enlaces agregados
- **Inundación de centrales, centros de datos, infraestructura de comunicaciones en edificios, etc. :** infraestructuras de comunicaciones y CPDs en plantas elevadas (no en sótanos ni en plantas bajas en zonas inundables)
- **Alta dependencia de energía eléctrica:**
 - **Tecnologías pasivas,** sin equipos activos en el recorrido, son menos vulnerables que otras (**FTTH frente a HFC**).
 - El diseño GPON utilizado por FTTH es muy simple pero potente: Permite conseguir altas velocidades a la red, gracias a la fibra con consumo eléctrico mínimo.
 - Los equipos con alimentación eléctrica están en la central telefónica del operador (OLT), y en casa de los clientes (ONT). El resto de los elementos de red son elementos pasivos, es decir, que no necesitan alimentación (fibra óptica, divisores ópticos pasivos, etc.)
 - Aumento del número de **grupos electrógenos o generadores portátiles tipo maleta para hacer uso en emergencias**
 - Uso de fuentes de energía independientes para evitar fallos por cortes eléctricos (UPS, generadores, alimentación dual en equipos de red, aumento del número de grupos electrógenos ante emergencias,...)
- **Lodos solidificados en canalizaciones = conductos obturados.** Limpieza de conductos previo a que se solidifiquen los lodos y el fango

Telecomunicaciones a prueba de DANA

Posibles conclusiones

- **Diversidad de tecnologías** para enlaces redundados y/o uso de **tecnologías complementarias**, por ejemplo, satélite, que además ha demostrado ser una buena solución **ante emergencias**:
 - 1 **Rápida Implementación**: sólo requiere el terminal satelital y una fuente de energía.
 - 2 **Cobertura Global**: puede brindar conectividad en zonas sin acceso a redes móviles o fibra óptica.
 - 3 **Portabilidad**: la antena y el router son compactos y pueden instalarse en vehículos de emergencia o refugios temporales.
 - 4 **Velocidades Altas**: ofrece hasta 250 Mbps en descarga, permitiendo videollamadas, telemedicina y transmisión de datos en tiempo real.
 - 5 **Baja Latencia (~20-50 ms)**: suficiente para comunicación de voz y datos de misión crítica.
- Integración de todas las fuentes de información (sensores) y **uso de IA para obtener conocimiento que permita la ayuda en la toma de decisiones**
- Recomendación de **cambios en normativas**, por ejemplo, armarios de comunicaciones y CPDs en plantas elevadas (no en sótanos ni en plantas bajas en zonas inundables)
- Necesidad de **oficina técnica de coordinación en fase de reconstrucción**.
 - Todo proyecto de infraestructura ya sea terrestre o aérea, debe contemplar las necesidades de Telecomunicaciones
 - Se ha de garantizar que los servicios en “precario” no caen en la etapa de reconstrucción, y se dejan en su versión definitiva

Telecomunicaciones a prueba de DANA

Posibles conclusiones

- **Diseño de red** en función de mapas de inundabilidad: Evitar instalación de infraestructura de telecomunicaciones, al menos para agregación/transporte, cerca de barrancos y zonas inundables
- **Protocolos, coordinación y Planes a prueba de DANA, aprobados y probados (simulacros):**
 1. El Plan de Recuperación y Reconstrucción debe culminar con un “**Plan de Gestión de Continuidad de las Telecomunicaciones**”
 - Business Continuity Plan (BCP): **Estrategia integral** para mantener la operatividad del negocio en caso de una interrupción.
 - Disaster Recovery Plan (DRP): **Plan específico** para restaurar sistemas de TI y telecomunicaciones después de un desastre.
de manera que **exista un plan de continuidad y de recuperación ante desastres aprobado, y que se realicen simulacros de manera periódica**
 2. **Salvoconductos:** En las horas y días posteriores a la catástrofe hubo un problema importante de accesos a las zonas afectadas por parte de los operarios.
 3. **Energía y Telecomunicaciones:** Debida a la alta dependencia de la energía y las telecomunicaciones, es necesaria una mayor coordinación entre las compañías eléctricas y telecomunicaciones, en los días inmediatamente posteriores a la catástrofe, para priorizar en función de los planes de cada cual, es decir, que el operador moverá sus grupos electrógenos a lugares donde no esté previsto que lo haga la compañía eléctrica, etc.

Telecomunicaciones a prueba de DANA: Resumen sesión con colegiados 6/3/25



Lecciones aprendidas

1. Limitaciones en la Recopilación de Datos

 *Problema:*

- Los sistemas no están diseñados para captar información detallada en situaciones de catástrofes.
- La información disponible estaba pensada para averías individuales, no para una emergencia masiva.
- No se incluyeron datos específicos sobre la afectación a empresas ni infraestructuras críticas más allá de líneas fijas y móviles.

Aprendizaje:



- Es necesario desarrollar un sistema de recopilación de datos en tiempo real con métricas más detalladas.
- Se deben diferenciar los impactos en ciudadanos, empresas, servicios públicos y emergencias.

Lecciones aprendidas

2. Dependencia Crítica de la Energía Eléctrica

Problema:

- Muchas estaciones base de telecomunicaciones dejaron de funcionar porque la infraestructura eléctrica colapsó.
- La autonomía de las baterías de las BTS es limitada (3-4 horas), insuficiente para un evento prolongado.
- Se identificó que tecnologías pasivas como **FTTH resistieron mejor** que otras como **HFC**, que dependen de nodos activos en la calle.

Aprendizaje:

- La resiliencia de las telecomunicaciones depende directamente de la disponibilidad de energía.
- Los operadores deben mejorar los sistemas de respaldo y coordinar con las compañías eléctricas.

Lecciones aprendidas

3. Falta de Protocolos de Actuación y Coordinación

Problema:

- Los primeros días fueron caóticos porque no existía un protocolo claro de actuación entre operadores, administraciones y cuerpos de emergencia.
- No estaba definido cómo gestionar los accesos prioritarios a las zonas afectadas ni cómo coordinar el despliegue de soluciones temporales.
- Se evidenció una **falta de interoperabilidad entre redes de comunicación de emergencia** (policía, bomberos, ejército, operadores).

Aprendizaje:

- La coordinación previa y los simulacros evitarían bloqueos y retrasos en la respuesta.
- Se necesitan procedimientos estandarizados para que cada actor sepa qué hacer sin improvisaciones.

Lecciones aprendidas

4. Uso Deficiente de Soluciones Satelitales

Problema:

- El satélite fue clave en algunas zonas, pero su despliegue no fue inmediato porque no había un plan predefinido.
- Este recurso se utilizó en emergencias, pero también precisa de energía eléctrica, lo que retrasó su puesta en marcha.
- España dispone de sistemas satelitales listos para emergencias, pero se activaron una semana después del evento.

Aprendizaje:

- La conectividad satelital debe ser parte del protocolo de respuesta y su despliegue debe estar previsto en cuestión de horas, no días.
- Los kits de emergencia deben incluir energía auxiliar junto con los sistemas satelitales.

Lecciones aprendidas

5. Vulnerabilidad de la Infraestructura de Telecomunicaciones

Problema:

- Se dañaron **miles de postes, arquetas y cámaras de registro**, lo que dificultó la recuperación del servicio.
- En muchas zonas rurales, los cables suelen ser aéreos (uso de postes) y las soluciones de contingencia de la emergencia han dejado cables enterrados sin protección, lo que los hace extremadamente vulnerables.
- En áreas urbanas, equipos críticos como armarios de telecomunicaciones se instalaron en sótanos o plantas bajas, exponiéndolos a inundaciones.

Aprendizaje:

- Se deben revisar las normativas para proteger mejor la infraestructura clave y evitar ubicaciones vulnerables.
- Las canalizaciones deben estar diseñadas para resistir eventos extremos.

Lecciones aprendidas

6. Falta de Copias de Seguridad en los Ayuntamientos

Problema:

- Varios ayuntamientos perdieron el acceso a sus datacenters, lo que les dejó **sin información sobre sus ciudadanos** en el momento más crítico.
- No existía un sistema de respaldo en la nube accesible en caso de emergencia.
- Aunque se habían recomendado backups, no era una obligación.

Aprendizaje:

- La información esencial de los municipios debe estar siempre accesible a través de sistemas en la nube con redundancia en diferentes localizaciones.
- Se necesitan protocolos claros para la recuperación rápida de datos.

Propuestas de mejora

1. Creación de un Sistema de Información en Tiempo Real para Emergencias

 *Objetivo:*

- Implementar un **dashboard centralizado** donde operadores, administraciones y cuerpos de emergencia puedan ver datos actualizados sobre la afectación en telecomunicaciones.

 *Acciones:*

- Mejorar la granularidad de los datos reportados por operadores al Ministerio.
- Incluir métricas diferenciadas por ciudadanos, empresas y administraciones.
- Automatizar la recopilación de información en base a sensores IoT y uso de inteligencia artificial para obtener información útil que ayude a la toma de decisiones.

Propuestas de mejora

2. Integración Telecomunicaciones-Energía para Respuesta Rápida

Objetivo:

- Establecer una **coordinación directa** entre empresas de telecomunicaciones y eléctricas para restaurar servicios prioritarios.

Acciones:

- Creación de un **protocolo de acceso preferente** a las zonas afectadas para técnicos de ambas industrias.
- Implementación de sistemas de respaldo energético en estaciones base clave.
- Priorización de energías renovables y baterías de larga duración en infraestructuras críticas.

Propuestas de mejora

3. Protocolos de Actuación y Simulacros Periódicos

Objetivo:

- Establecer un **protocolo único y obligatorio** para todos los actores involucrados en la recuperación de telecomunicaciones.

Acciones:

- Realización de simulacros de desastre al menos una vez al año.
- Capacitación específica para administraciones públicas y operadores sobre actuación en emergencias.
- Implementación de planes de contingencia específicos para cada operador.

Propuestas de mejora

4. Despliegue Rápido de Soluciones Satelitales



Objetivo:

- Asegurar una respuesta inmediata mediante tecnología satelital en zonas afectadas.



Acciones:

- Crear una **reserva de equipos satelitales listos para ser desplegados en las primeras 24 horas** de una emergencia.
- Desarrollar planes de contingencia que incluyan generadores eléctricos para el uso de soluciones satelitales.
- Integrar Hispasat como proveedor prioritario de conectividad de emergencia.

Propuestas de mejora

5. Rediseño de la Infraestructura de Telecomunicaciones

 *Objetivo:*

- Hacer las redes más resilientes ante eventos extremos.

 *Acciones:*

- Promover el soterramiento de cables en zonas de alto riesgo.
- Evitar la instalación de equipos críticos en zonas inundables.
- Reforzar las canalizaciones compartidas entre operadores.

Propuestas de mejora

6. Backup Obligatorio de Datos en los Ayuntamientos

 *Objetivo:*

- Garantizar la disponibilidad de la información municipal en todo momento.

 *Acciones:*

- Obligar por ley a los ayuntamientos a tener copias de seguridad en la nube.
- Definir un protocolo para acceder a los datos de manera rápida en caso de emergencia.
- Crear sistemas híbridos de almacenamiento local + nube para garantizar redundancia.

Conclusión

Las telecomunicaciones demostraron ser un servicio **esencial** en la gestión de emergencias, pero la respuesta ante la DANA mostró fallos que pueden corregirse con mejores protocolos, infraestructuras más resilientes y una integración más eficiente con los sistemas energéticos y administrativos. La clave está en la **anticipación, planificación y coordinación**.