



GUÍA INTEGRADA

Plan Analógico Mínimo Viable (PAMV)

Continuidad operativa de empresas, administraciones e instituciones ante apagones de larga duración.

Octubre de 2026

Documento de trabajo para adaptación organizativa. No sustituye asesoramiento jurídico, técnico, energético ni de seguridad específico.



Índice

Plan Analógico Mínimo Viable (PAMV) — Guía integrada

01	Resumen ejecutivo	3	02	Planteamiento: resiliencia, no catastrofismo	4
03	Alcance y relación con otros planes	5	04	Principios rectores	6
05	Fundamentos y evidencia	7	06	Modelo de resiliencia por capas	9
07	Metodología de construcción del PAMV	10	08	Estructura del PAMV	12
09	Ejemplo aplicado: pyme comercial	16	10	Ejemplo aplicado: admón. pública local	19
11	Programa de simulacros	21	12	Errores frecuentes	22
13	Hoja de ruta de implantación	23	14	Conclusiones	24
15	Fuentes y referencias	25			

Resumen ejecutivo

La digitalización, la automatización y la inteligencia artificial han aumentado la eficiencia de empresas, administraciones e instituciones, pero también han creado dependencias simultáneas de electricidad, conectividad, dispositivos, sistemas de pago, identidades digitales y proveedores tecnológicos. Un apagón prolongado puede interrumpir al mismo tiempo ventas, cobros, comunicaciones, logística, atención sanitaria, servicios públicos y toma de decisiones.

El Plan Analógico Mínimo Viable (PAMV) es una capacidad organizativa, no solamente un documento. Define el conjunto mínimo de funciones críticas, personas autorizadas, información esencial, recursos físicos y procedimientos impresos necesarios para operar de forma segura durante una interrupción eléctrica o de comunicaciones.

La evidencia disponible muestra que existen marcos maduros en el sector eléctrico, las infraestructuras financieras y la administración pública. Sin embargo, el apagón ibérico del 28 de abril de 2025 evidenció una brecha relevante en pymes, comercio minorista, servicios locales y hogares. Las grandes infraestructuras mantuvieron mejor su operativa gracias a redundancia, energía alternativa y capacidades offline; muchos pequeños establecimientos no disponían de medidas equivalentes.

La resiliencia no se consigue únicamente con generadores, backups o servicios en la nube. Requiere saber qué debe seguir funcionando, quién puede decidir sin sistemas, con qué medios se comunica la organización, qué información debe estar disponible en papel y cómo se entrena a las personas para ejecutar el plan.

Planteamiento: resiliencia, no catastrofismo

El objetivo no es anticipar un colapso social ni promover desconfianza hacia la tecnología. Es aplicar un principio básico de gestión de riesgos: identificar escenarios de baja probabilidad y alto impacto, y preparar respuestas proporcionadas.

El informe del National Infrastructure Advisory Council (NIAC) para CISA analiza apagones catastróficos como eventos de larga duración, gran escala y efectos en cascada sobre agua, comunicaciones, transporte, sanidad y servicios financieros. Concluye que los planes y recursos existentes podrían quedar superados por un evento de esa magnitud y recomienda un enfoque integrado entre gobiernos, empresas, comunidades y ciudadanos.

La resiliencia puede describirse mediante tres capacidades:

01 — RESISTIR

Mantener lo esencial

Mantener servicios esenciales durante la interrupción.

02 — DEGRADARSE

De forma controlada

Reducir servicios sin perder seguridad, legalidad o capacidad de decisión.

03 — RECUPERAR

De forma ordenada

Volver al funcionamiento normal verificando sistemas, datos y responsabilidades.

El PAMV se sitúa especialmente en la segunda capacidad: no busca que todo siga igual, sino que lo esencial pueda continuar.

Alcance y relación con otros planes

Documento	Finalidad	Relación con el PAMV
Plan de emergencia	Evacuación, incendio, seguridad física y primera respuesta	Se activa antes o en paralelo si hay riesgo para personas
Plan de recuperación tecnológica	Restauración de sistemas, datos y aplicaciones	Se activa cuando se recupera energía o conectividad
Plan de continuidad de negocio	Gestión integral de interrupciones y riesgos	El PAMV es su componente de operación analógica
Plan de crisis	Dirección estratégica y comunicación en crisis	Define mando, portavocía y decisiones de alto nivel
Plan de seguridad	Protección de personas, activos e información	Define accesos, custodia, control y seguridad física

Regla de delimitación: el PAMV responde a la pregunta «¿qué podemos seguir haciendo ahora, con seguridad y trazabilidad, sin sistemas digitales?». No intenta replicar toda la actividad habitual.

Principios rectores

Principio	Aplicación práctica
Proporcionalidad	Adaptar el plan al tamaño, riesgo, actividad y recursos de la organización.
Minimalismo operativo	Mantener solo funciones indispensables para seguridad, legalidad, servicio esencial y recuperación.
Autoridad explícita	Cada decisión crítica debe tener titular, suplente y límites de actuación.
Redundancia inteligente	Priorizar comunicaciones, energía, accesos, pagos y registros esenciales.
Trazabilidad	Registrar toda decisión, gasto, entrega o incidencia, incluso manualmente.
Protección de datos	Información en papel mínima, necesaria, custodiada y destruida de forma controlada.
Ejercicio real	Validar el plan mediante simulacros periódicos.
Interoperabilidad	Coordinar con proveedores, clientes, emergencias, administraciones y otras sedes.

Fundamentos y evidencia

5.1 CISA y NIAC

El estudio *Surviving a Catastrophic Power Outage*, elaborado por el NIAC y publicado a través de CISA, plantea que un apagón catastrófico puede durar semanas o meses, afectar a amplios territorios y provocar fallos en cascada en agua, comunicaciones, transporte, sanidad, combustible y servicios financieros. Recomienda un enfoque de sistema, no sectorial, y una preparación que llegue hasta administraciones locales, empresas y hogares.

5.2 FERC, NERC y black start

El *black start* es la capacidad de arrancar generación sin energía externa y reconstruir progresivamente el sistema eléctrico tras un apagón generalizado. FERC y NERC han evaluado la disponibilidad de recursos de black start y next start, subrayando la importancia de planes, pruebas, combustible, coordinación y formación.

La lección organizativa es directa: disponer de un recurso no equivale a tener capacidad operativa. Hace falta procedimiento, personas entrenadas, comunicación y ensayo.

5.3 Continuidad operativa pública

Los marcos de Continuity of Operations (COOP) de FEMA y de administraciones locales estructuran la continuidad en torno a funciones esenciales, personal crítico, sucesión de mando, comunicaciones alternativas, registros vitales, instalaciones alternativas y ejercicios periódicos.

La plantilla de la ciudad de Boston aplica la misma lógica al sector privado: funciones esenciales, prioridad de recuperación, responsables, suplentes, interdependencias, recursos, estrategias de continuidad y restauración, comunicaciones y pruebas.

5.4 Banco de España y apagón de 2025

El Banco de España analizó el impacto del apagón del 28 de abril de 2025 sobre los sistemas de pago. Concluyó que las infraestructuras financieras críticas funcionaron correctamente, pero que las transacciones minoristas cayeron fuertemente porque muchas operaciones comerciales no pudieron continuar.

Las transacciones con tarjeta disminuyeron alrededor del 55 % respecto a un día comparable; en pequeños comercios, la caída superó el 80 % en los momentos más críticos. Las grandes superficies resistieron mejor por disponer con mayor frecuencia de generadores, terminales autónomas y autorización offline.

El Banco recomienda extender el pago con tarjeta offline, reforzar la redundancia de comunicaciones con operadores duales y enrutamiento físicamente separado, instalar cajeros en ubicaciones críticas y promover reservas modestas de efectivo en los hogares.

5.5 ENTSO-E

El informe del panel de expertos de ENTSO-E identifica causas técnicas y recomendaciones para reforzar la resiliencia del sistema eléctrico europeo. La interrupción tuvo efectos inmediatos sobre telecomunicaciones, pagos, movilidad y actividad económica.

La implicación es importante: recuperar electricidad no equivale a recuperar actividad. Una organización puede tener energía antes de recuperar conectividad, sistemas, datos, personal o capacidad de cobro.

Modelo de resiliencia por capas

Capa	Finalidad	Ejemplos
Digital avanzada	Eficiencia, analítica, IA y automatización	ERP, CRM, IA generativa, analítica, automatización
Digital resistente	Operar con fallos parciales	Backups aislados, nube redundante, modo offline, doble operador
Energía y comunicaciones	Sostener funciones críticas	Baterías, generadores, solar, radio, satélite, teléfono fijo
Analógica esencial	Decidir, registrar y servir sin sistemas	Protocolos impresos, formularios, talonarios, sellos, efectivo, actas
Personas y gobernanza	Decidir y coordinar	Cadena de mando, suplencias, formación, simulacros, autoridad delegada

Error frecuente: comprar un generador y considerarlo un plan. Un generador debe ir acompañado de un análisis de cargas prioritarias, capacidad, combustible, mantenimiento, arranque, ventilación, seguridad y personal autorizado.

Metodología de construcción del PAMV

7.1 Definir escenarios de diseño

Nivel	Escenario	Horizonte	Objetivo
Nivel 1	Apagón breve	Hasta 4 horas	Seguridad, información y continuidad parcial
Nivel 2	Apagón extendido	24–72 horas	Operación degradada y funciones críticas
Nivel 3	Apagón grave	Más de 72 horas	Operación autónoma y coordinación externa

7.2 Análisis de impacto

Criterio	Pregunta guía	Puntuación
Seguridad	¿Su parada puede causar daño a personas?	1–5
Legal	¿Su parada incumple obligaciones legales, contractuales o sectoriales?	1–5
Económico	¿Su parada genera pérdidas relevantes o impide cobrar?	1–5
Reputacional	¿Su parada daña gravemente la confianza de clientes o ciudadanos?	1–5
Operativo	¿Su parada bloquea otras funciones esenciales?	1–5
Social	¿Su parada afecta a personas vulnerables o servicios públicos básicos?	1–5

Las funciones con mayor puntuación agregada, o con impacto crítico en cualquier criterio, deben incorporarse al PAMV.

7.3 Identificar dependencias

Energía: iluminación, seguridad, refrigeración, comunicaciones, equipos médicos, servidores y accesos.

Conectividad: móvil, Internet, telefonía fija, satélite, redes privadas y TPV.

Datos: ERP, CRM, historiales, inventarios, precios, autorizaciones y contratos.

Personas: mandos, técnicos, personal de guardia, suplentes y proveedores.

Logística: transporte, combustible, almacén, entregas, agua, alimentos y material crítico.

Externos: banca, aseguradora, emergencias, administración, proveedores tecnológicos y energéticos.

7.4 Definir el modo degradado

Decisión	Criterio recomendado
Mantener	Funciones que protegen vidas, seguridad, derechos esenciales u obligaciones legales
Reducir	Funciones necesarias pero susceptibles de operar con controles manuales y menor capacidad
Posponer	Funciones importantes pero no urgentes, como campañas, informes o trámites no críticos
Suspender	Funciones que no pueden ejecutarse con trazabilidad, seguridad o legalidad suficientes

Estructura del PAMV

8.1 Ficha de activación

Campo	Contenido mínimo
Código del plan	Identificador y versión
Objetivo	Mantener funciones esenciales durante interrupción eléctrica o de comunicaciones
Activación	Criterios objetivos y autoridad competente
Alcance	Sedes, servicios, personal y procesos incluidos
Duración de diseño	4 horas, 72 horas y hasta 30 días
Ubicación del plan	Copia física, copia alternativa y responsable de custodia
Revisión	Fecha, responsable y próxima revisión

8.2 Funciones críticas

Campo	Ejemplo
Función	Atención presencial y emisión de comprobantes
Prioridad	Crítica
Objetivo de reanudación	Antes de 2 horas
Responsable	Director de tienda
Suplente	Responsable de turno
Dependencias	Electricidad, TPV, conectividad, caja y personal
Modo analógico	Venta manual, talonario, efectivo, validación por responsable
Límites	No vender productos con verificación digital obligatoria
Escalado	Cerrar venta si no puede garantizarse trazabilidad o seguridad

8.3 Gobernanza sin sistemas

Rol	Titular	Suplente	Autoridad en modo analógico
Director de crisis	Gerencia / Alcaldía	Dirección de operaciones	Activar plan, suspender servicios, autorizar gastos
Coordinador operativo	Operaciones / Secretaría	Jefe de turno	Distribuir personal, abrir o cerrar sede
Resp. de seguridad	Instalaciones / Prevención	Supervisor	Evacuar, controlar accesos, cortar suministros
Resp. de comunicación	Comunicación / RR. HH.	Atención al público	Informar a empleados, clientes y proveedores
Resp. financiero	Administración / Tesorería	Tesorero	Autorizar pagos esenciales y uso de efectivo

Debe existir una cadena de sustitución de al menos tres niveles. Si el titular no está localizable, el suplente debe poder actuar sin esperar instrucciones digitales.

8.4 Comunicaciones PACE

Nivel	Canal	Uso
Primario	Móvil, correo, Teams, Slack	Coordinación habitual
Alternativo	Teléfono fijo, SMS, mensajería física	Aviso a mandos y contactos clave
Contingencia	Radio VHF/UHF, satélite, red privada	Coordinación entre sedes o servicios
Emergencia	Punto de encuentro, pizarra, altavoces, mensajero	Instrucciones inmediatas

8.5 Registros vitales

- Listado de empleados, roles, contactos de emergencia y suplencias.
- Contactos de clientes clave, proveedores críticos, técnicos, seguros y autoridades.
- Procedimientos de apertura, cierre, seguridad, evacuación y activación.
- Plantillas de actas, autorizaciones, partes de incidencia, recibos y entregas.
- Inventario mínimo de productos, medicamentos, piezas o materiales.
- Listado de personas con necesidades especiales, solo cuando sea legal, necesario y proporcionado.
- Copia física o cifrada de contratos, pólizas, licencias y protocolos.

Regla de protección de datos: imprimir solo el mínimo necesario; restringir el acceso; custodiar bajo llave; registrar accesos cuando proceda; y destruir de forma segura cuando deje de ser necesario.

8.6 Energía y cargas prioritarias

Prioridad	Tipo de carga	Ejemplos
1	Vida y seguridad	Iluminación de evacuación, alarmas, comunicaciones, equipos médicos
2	Continuidad crítica	Telefonía, radio, TPV offline, servidores mínimos, refrigeración esencial
3	Operación reducida	Puestos de trabajo seleccionados, impresoras, cámaras
4	No prioritaria	Pantallas, climatización general, decoración, equipos no esenciales

8.7 Procedimiento de activación

1. Confirmar duración prevista y estado de seguridad.
2. Activar al director de crisis por canal alternativo.
3. Convocar al equipo crítico en el punto de encuentro.
4. Abrir la carpeta física del PAMV.
5. Comunicar el modo de operación a empleados, clientes y proveedores.
6. Activar funciones críticas por orden de prioridad.
7. Registrar decisiones, incidencias y gastos en el parte manual.
8. Revisar cada 4 horas personas, energía, comunicaciones, seguridad y suministros.
9. Decidir entre mantener operación, reducir servicio, reubicarse o suspender.
10. Al recuperar suministro, validar sistemas antes de volver al modo normal.

8.8 Registro de incidentes

Hora	Hecho	Decisión	Responsable	Impacto	Acción siguiente
11:20	Corte eléctrico general	Activar PAMV	Director de operaciones	Tienda cerrada temporalmente	Aviso a empleados
11:35	Móvil sin cobertura	Activar radio	Coordinador	Comunicación interna operativa	Contacto con proveedor
12:10	Cliente necesita factura	Emisión manual	Responsable de tienda	Riesgo bajo	Registro en talonario

Ejemplo aplicado: pyme comercial

Perfil: comercio minorista con tienda física, entre 8 y 20 empleados, TPV, ERP, tienda online, cámaras, alarmas, cámaras frigoríficas y proveedores locales.

9.1 Funciones críticas

Función crítica	Prioridad	Objetivo	Responsable	Suplente	Modo analógico
Seguridad de personas y local	Crítica	Inmediato	Resp. de tienda	Jefe de turno	Evacuación, control de accesos, alumbrado de emergencia
Comunicación interna	Crítica	1 hora	Gerente	Resp. de tienda	Radio, teléfono fijo, punto de encuentro
Atención presencial	Alta	2 horas	Resp. de tienda	Jefe de turno	Venta manual, catálogo impreso, talonario
Cobro y trazabilidad	Crítica	2 horas	Resp. de caja	Adjunto de tienda	Efectivo, talonario, arqueo manual
Conservación de productos	Alta	2 horas	Resp. de almacén	Empleado designado	Cierre de neveras, termómetro, prioridad de consumo
Comunicación con proveedores	Media	24 horas	Compras	Gerente	Teléfono fijo, contacto impreso, pedidos diferidos
Registro de incidencias	Alta	Inmediato	Gerente	Resp. de tienda	Cuaderno foliado, actas y partes

9.2 Kit físico de la tienda

Elemento	Cantidad	Ubicación	Responsable
Carpeta física del PAMV	1	Caja fuerte o despacho	Gerente
Linternas con baterías	4	Recepción, almacén, caja y salida	Instalaciones
Power banks cargados	4	Caja fuerte y despacho	Resp. de tienda
Radios de dos vías	2–4	Recepción y almacén	Jefe de turno
Teléfono fijo analógico	1	Mostrador	Gerente
Talonarios de ventas y recibos	2	Caja	Resp. de caja
Calculadora autónoma	1	Caja	Resp. de caja
Efectivo de contingencia	Importe definido	Caja fuerte	Resp. financiero
Formularios de incidencias	20	Carpeta PAMV	Gerente
Listado de contactos	1	Carpeta PAMV	Gerente
Mapa de evacuación	2	Entrada y almacén	Seguridad
Termómetro manual	1	Almacén	Resp. de almacén
Llaves y candados físicos	Según acceso	Caja fuerte	Seguridad

9.3 Reglas de decisión

- Si no hay luz durante menos de 60 minutos, mantener la tienda abierta solo si hay seguridad, iluminación y cobro trazable.
- Si la interrupción supera 60 minutos sin energía alternativa, cerrar la venta al público y activar el modo de conservación.
- Si el TPV no funciona pero hay luz, vender solo mediante efectivo o procedimiento offline autorizado.
- Si no hay conectividad pero existe TPV autónomo, aplicar el límite de importe y el procedimiento de autorización offline definido por la entidad de pago.
- Si no puede garantizarse trazabilidad, seguridad o legalidad, reducir o suspender el servicio.

9.4 Simulacro sin luz para la pyme

Minuto	Actividad	Resultado esperado
0–10	Simular corte eléctrico y pérdida de móvil e Internet	Activación del plan
10–20	Abrir carpeta física y verificar cadena de mando	Responsable y suplente identificados
20–35	Probar radio, teléfono fijo y punto de encuentro	Comunicación alternativa operativa
35–55	Ejecutar una venta simulada sin TPV	Registro manual y decisión de cobro
55–70	Simular incidencia en cámara frigorífica	Registro de temperatura y decisión
70–80	Redactar parte de incidencia	Trazabilidad de decisiones
80–90	Debriefing y actualización	Acciones correctivas asignadas

Reglas: no usar móvil, correo, ERP, TPV ni buscador; asignar roles reales; documentar cada decisión; y evaluar si el plan puede ejecutarse sin ayuda de quien lo redactó.

Ejemplo aplicado: administración pública local

10.1 Funciones críticas

Función crítica	Prioridad	Responsable	Suplente	Modo analógico
Emergencias y protección civil	Crítica	Coordinador de emergencias	Técnico de protección civil	Radio, satélite, mapa impreso, centro de mando
Información a la población	Crítica	Comunicación	Atención ciudadana	Altavoces, carteles, radio local, puntos de información
Servicios sociales esenciales	Alta	Servicios sociales	Trabajador social de guardia	Fichas impresas, teléfono, visitas, registro manual
Personas vulnerables y electrodependientes	Crítica	Servicios sociales	Emergencias	Censo actualizado, llamadas, redes vecinales, puntos de apoyo
Coordinación con emergencias	Crítica	Alcaldía / protección civil	Coordinador de emergencias	Radio, satélite, centro operativo
Seguridad y accesos	Alta	Policía local / instalaciones	Supervisor	Llaves, control manual, patrullas
Registro y actas	Alta	Secretaría	Funcionario de guardia	Actas manuscritas, sellos, registro foliado

10.2 Centro operativo municipal

Energía: generador, baterías, iluminación de emergencia y puntos de carga prioritarios.

Comunicaciones: radio, teléfono fijo, satélite y canal alternativo con emergencias.

Documentación: censo de personas vulnerables, mapas, protocolos, formularios y recursos.

Logística: agua, alimentos básicos, material sanitario, combustible y transporte.

Coordinación: sala de mando, pizarra, turnos, registro de decisiones y enlace con policía, bomberos y sanidad.

El NIAC propone el concepto de enclaves comunitarios: instalaciones existentes que pueden reforzarse para sostener servicios básicos, comunicaciones, energía, alimentos, agua y atención médica durante interrupciones prolongadas.

10.3 Simulacro municipal sin luz

Fase	Duración	Actividad	Resultado
Activación	30 min	Notificación y activación del centro operativo	Equipo de mando convocado
Comunicaciones	45 min	Prueba de radio, fijo, satélite y mensajería física	Canal alternativo operativo
Vulnerables	60 min	Consulta de censo impreso y contacto	Personas localizadas y necesidades identificadas
Coordinación	60 min	Enlace con policía, bomberos, sanidad y servicios sociales	Prioridades compartidas
Información pública	45 min	Mensaje y difusión analógica	Mensaje claro y puntos de información
Registro	45 min	Actas, partes y lecciones aprendidas	Plan actualizado

Programa de simulacros

Tipo	Duración	Alcance	Objetivo
Mesa	60–90 min	Dirección y mandos	Validar activación, roles y decisiones
Funcional	2–4 horas	Equipo operativo	Ejecutar una función crítica en papel
Sin luz	Medio día	Sede o tienda	Probar energía, seguridad, comunicación y servicio
Con personal reducido	Medio día	Equipo real reducido	Probar suplencias y carga operativa
Multiservicio	Jornada completa	Varias organizaciones	Probar coordinación externa
Post-incidente	Tras incidencia real	Responsables implicados	Corregir el plan con evidencia

11.1 Métricas mínimas

Indicador	Objetivo orientativo
Tiempo de activación	Menos de 15 minutos
Localización del equipo crítico	Menos de 20 minutos
Canal alternativo operativo	Menos de 30 minutos
Registro manual de función crítica	Menos de 10 minutos
Cobertura de suplencias	100 % de roles críticos
Cobertura de registros vitales	100 % localizados y actualizados
Acciones correctivas cerradas	100 % antes del siguiente simulacro

Errores frecuentes

- Confundir recuperación informática con continuidad operativa.
- Guardar el plan solo en la nube o en el ordenador corporativo.
- Asignar responsabilidades sin suplentes ni autoridad predelegada.
- Comprar un generador sin análisis de cargas, combustible, mantenimiento y pruebas.
- No disponer de efectivo, llaves, formularios o contactos impresos.
- No probar el plan con personal distinto del que lo redactó.
- No coordinar con proveedores, banca, emergencias u otras administraciones.
- Imprimir datos personales innecesarios o sin control de acceso.
- Actualizar el plan solo después de una crisis.

Hoja de ruta de implantación

Fase	Plazo	Acciones
1. Diagnóstico	2–4 semanas	Identificar funciones críticas, dependencias, riesgos y responsables
2. Diseño	4–6 semanas	Redactar PAMV, definir modos degradado y analógico, preparar carpeta física
3. Dotación	4–8 semanas	Radios, baterías, formularios, efectivo de contingencia, energía y recursos
4. Formación	2 semanas	Formar titulares y suplentes; distribuir tarjetas de bolsillo
5. Simulacro	1 jornada	Ejecutar simulacro sin luz y documentar brechas
6. Mejora	2–4 semanas	Actualizar plan, recursos, contactos y responsabilidades
7. Mantenimiento	Anual	Revisar contactos, inventario, protocolos y repetir simulacro

Conclusiones

Existen estudios, marcos regulatorios y experiencias prácticas sobre continuidad ante apagones prolongados. Los operadores eléctricos disponen de planes de black start; las infraestructuras financieras aplican mecanismos de contingencia; y las administraciones públicas utilizan marcos de continuidad operativa basados en funciones esenciales, sucesión de mando, comunicaciones alternativas, registros vitales y ejercicios.

La experiencia del apagón ibérico de 2025 evidenció que la resiliencia no llega uniformemente a toda la economía. Las grandes organizaciones suelen disponer de más redundancia, energía alternativa y capacidades offline; muchas pymes, pequeños comercios y servicios locales no.

El PAMV ofrece una respuesta proporcionada: no exige abandonar la digitalización, sino garantizar que la organización pueda seguir decidiendo, comunicándose, protegiendo personas y prestando servicios esenciales cuando la infraestructura digital falle. La prueba definitiva no es tener un documento aprobado, sino poder abrir una carpeta física, localizar a las personas adecuadas y operar sin depender de una pantalla.

Fuentes y referencias

1. CISA / National Infrastructure Advisory Council (2018). *Surviving a Catastrophic Power Outage*. [cisa.gov](https://www.cisa.gov)
2. FERC y NERC (2025). *FERC–NERC Staff Report on Grid Operators Having Sufficient "Blackstart" Capability*. [ferc.gov](https://www.ferc.gov)
3. FERC, NERC y Regional Entity (2025). *Blackstart and Next-Start Resource Availability in the Texas Interconnection*. [ferc.gov](https://www.ferc.gov)
4. Pacific Northwest National Laboratory / U.S. Department of Energy (2020). *Electric Grid Blackstart: Trends, Challenges, and Opportunities*. [osti.gov](https://www.osti.gov)
5. FEMA. *Continuity of Operations Plan (COOP) Planning Template*. [fema.gov](https://www.fema.gov)
6. City of Boston, Office of Emergency Management (2025). *Business Continuity Plan Template*. [boston.gov](https://www.boston.gov)
7. Banco de España (2025). *The impact of the 28 April 2025 blackout on Spain's payment systems*. Financial Stability Review, 49. doi.org/10.53479/42425
8. ENTSO-E (2026). *Expert Panel Final Report on the 28 April 2025 Blackout in Continental Spain and Portugal*. entsoe.eu
9. Mayoralas Alises, S. (2026). *Respirar en la oscuridad: lecciones del apagón de abril de 2025 para los pacientes respiratorios electrodependientes*. pmc.ncbi.nlm.nih.gov
10. Prehospital and Disaster Medicine (2026). *Blackout in Spain: Urgent Analysis of Impact on Emergency Medical Services*. [cambridge.org](https://www.cambridge.org)
11. U.S. Government Publishing Office (2017). *Federal Continuity Directive 1*. [gpo.gov](https://www.gpo.gov)
12. Internal Revenue Service (2025). *IRM 10.6.1: Overview of Continuity Planning*. [irs.gov](https://www.irs.gov)