

Seguridad Informática Básica: Protección de Datos Personales en Emergencias

Autor: EA4IPV

Fecha: 23/03/2026

Categoría: Electrónica y Energía

Etiquetas: Sin etiquetas

Seguridad Informática Básica: Protección de Datos Personales en Emergencias

En una situación de crisis —ya sea un desastre natural, un corte prolongado de suministro eléctrico o un colapso de infraestructuras— la pérdida de datos digitales puede agravar enormemente la emergencia. Documentos de identidad escaneados, historiales médicos, pólizas de seguros, escrituras de propiedad y contactos de emergencia almacenados únicamente en dispositivos electrónicos pueden volverse inaccesibles en el peor momento. En España, el Reglamento General de Protección de Datos (RGPD, Reglamento UE 2016/679) y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) establecen obligaciones sobre la protección de datos personales que aplican también en contextos de emergencia. La preparación informática no es un lujo tecnológico: es una extensión lógica de cualquier plan de contingencia familiar.

Identificación de datos críticos y clasificación por prioridad

El primer paso es inventariar qué información digital es verdaderamente esencial y cuál puede recuperarse por otros medios. No todo tiene el mismo valor en una emergencia.

Categoría

Ejemplos

Prioridad

Formato recomendado

Identidad personal

DNI, pasaporte, libro de familia, certificados de nacimiento

Crítica

PDF escaneado + copia física plastificada

Documentación médica

Historial clínico, recetas crónicas, grupo sanguíneo, alergias

Crítica

PDF + tarjeta resumen en cartera

Documentación financiera

Escrituras, contratos hipotecarios, pólizas de seguros, testamento

Alta

PDF cifrado en dispositivo y copia notarial

Contactos de emergencia

Familiares, médico de cabecera, abogado, veterinario

Alta

Archivo digital + copia impresa

Fotografías y recuerdos

Álbumes familiares, vídeos importantes

Media

Copia en disco externo cifrado

Configuraciones y contraseñas

Accesos bancarios, correo, administración pública

Alta

Gestor de contraseñas offline (KeePassXC)

Consejo práctico: Escanea todos los documentos críticos a 300 DPI mínimo en formato PDF. Guarda los originales en una bolsa estanca ignífuga y las copias digitales en al menos dos soportes físicos distintos almacenados en ubicaciones separadas.

Estrategia de copias de seguridad 3-2-1

La regla 3-2-1 es el estándar de la industria para protección de datos y se adapta perfectamente a escenarios de emergencia: 3 copias de los datos, en 2 tipos de soporte diferentes, con 1 copia fuera del domicilio habitual.

Copia principal en disco duro externo SSD: Un SSD externo de 500 GB a 1 TB (Samsung T7, SanDisk Extreme) es resistente a golpes, compacto y consume poca energía. Se conecta por USB-C y puede alimentarse desde un power bank. Cifra el disco completo con VeraCrypt (software libre, multiplataforma) o BitLocker (incluido en Windows Pro). Actualiza esta copia mensualmente como mínimo.

Copia secundaria en memoria USB de alta resistencia: Una memoria USB de 64-128 GB con certificación IP68 (resistente al agua y al polvo) como la Kingston DataTraveler Max o la SanDisk Ultra Fit. Guárdala en tu mochila de emergencia (Bug Out Bag). Contiene solo los documentos clasificados como prioridad Crítica y Alta.

Copia externa en ubicación alternativa: Deposita una copia cifrada en casa de un familiar de confianza, en una caja de seguridad bancaria o en un servicio de almacenamiento en la nube con cifrado de extremo a extremo (Tresorit, Proton Drive). Esta copia protege contra la destrucción total del domicilio (incendio, inundación).

Importante: Los servicios en la nube dependen de conexión a Internet, que puede no estar disponible durante una emergencia. Nunca confíes exclusivamente en almacenamiento cloud para datos críticos. La copia física local cifrada es tu última línea de defensa.

Herramientas de cifrado accesibles para el usuario doméstico

Cifrar los datos no requiere conocimientos avanzados. Existen herramientas gratuitas y de código abierto que cualquier persona puede configurar en menos de una hora.

Herramienta

Plataforma

Uso principal

Nivel de dificultad

VeraCrypt

Windows, Linux, macOS

Crear volúmenes cifrados o cifrar discos completos

Medio — requiere seguir un asistente paso a paso

BitLocker

Windows Pro/Enterprise

Cifrado transparente de unidades completas

Bajo — se activa desde el panel de control

KeePassXC

Windows, Linux, macOS

Gestor de contraseñas offline con base de datos cifrada

Bajo — interfaz gráfica intuitiva

7-Zip

Windows, Linux

Comprimir y cifrar archivos individuales con AES-256

Bajo — clic derecho > añadir a archivo > poner contraseña

Cryptomator

Windows, Linux, macOS, móvil

Cifrar carpetas antes de subirlas a la nube

Bajo — crea una unidad virtual cifrada

La contraseña de cifrado debe ser robusta: mínimo 16 caracteres combinando mayúsculas, minúsculas, números y símbolos. Una frase de contraseña como «MiPerro*Come3Veces+AlDia!» es más fácil de recordar y más segura que una contraseña corta aleatoria. Anota esta contraseña maestra en papel y guárdala en un lugar seguro separado del dispositivo cifrado.

Protección de dispositivos móviles en evacuación

El teléfono móvil será probablemente el único dispositivo electrónico que lleves en una evacuación. Proteger su contenido y su capacidad de comunicación es prioritario.

Cifrado del dispositivo: Tanto Android (desde la versión 6.0) como iOS cifran el almacenamiento por

defecto si se establece un código de bloqueo. Verifica que tu dispositivo tiene activado el cifrado en Ajustes > Seguridad. Usa un PIN de al menos 6 dígitos o, mejor, una contraseña alfanumérica.

Modo avión y conservación de batería: En situación de emergencia, activa el modo avión para conservar batería y desactívalo solo cuando necesites comunicarte. Desactiva Wi-Fi, Bluetooth, GPS y NFC cuando no sean necesarios. Reduce el brillo al mínimo. Un móvil moderno puede durar 3-5 días en modo avión con uso esporádico.

Aplicaciones offline esenciales: Descarga previamente: mapas offline de tu zona (Google Maps, OsmAnd), guía de primeros auxilios de Cruz Roja, copia de tus documentos en una app de archivos cifrada, y una app de linterna/brújula que no requiera conexión. Almacena estos datos en la memoria interna, no en la tarjeta SD.

Borrado remoto como última defensa: Configura previamente «Encontrar mi dispositivo» (Android) o «Buscar mi iPhone» (iOS). Si pierdes el teléfono durante la emergencia, podrás borrar remotamente todos los datos cuando recuperes conexión, evitando que información sensible caiga en manos de terceros.

Marco legal español sobre protección de datos en emergencias

La legislación española contempla excepciones al tratamiento habitual de datos personales durante situaciones de emergencia, pero mantiene garantías básicas.

Artículo 6.1.d del RGPD: Permite el tratamiento de datos personales sin consentimiento cuando sea necesario para proteger intereses vitales del interesado o de otra persona física. Esto aplica en evacuaciones, triaje médico y coordinación de rescates.

Ley 17/2015, del Sistema Nacional de Protección Civil: Establece en su artículo 7 el deber de colaboración ciudadana y faculta a las autoridades a requerir información personal necesaria para la gestión de la emergencia. El ciudadano tiene derecho a que esos datos se destruyan una vez finalizada la situación de emergencia.

Artículo 9.2.c del RGPD: Permite el tratamiento de datos especialmente sensibles (salud, biometría) cuando sea necesario para proteger intereses vitales y el interesado no pueda dar su consentimiento. Esto ampara la consulta de historiales médicos por servicios de emergencia durante un rescate.

Atención legal: Aunque la legislación permite excepciones en emergencias, compartir datos personales de terceros sin necesidad vital sigue siendo una infracción del RGPD sancionable con multas de hasta 20 millones de euros. Comparte solo lo estrictamente necesario con las autoridades competentes.

⚠ Advertencia: Esta información es orientativa y educativa. En situaciones de emergencia real, consulte a profesionales cualificados siempre que sea posible. No ponga en riesgo su vida ni la de otros sin la formación adecuada.