Ciberseguridad Básica para Preparacionistas: Proteger Datos y Comunicaciones

Autor: EA4IPV
Fecha: 23/03/2026
Categoría: Electrónica y Energía
Etiquetas: Sin etiquetas

Ciberseguridad Básica para Preparacionistas: Proteger Datos y Comunicaciones

En un escenario de crisis, la información personal, las comunicaciones del grupo y los datos de localización de recursos son activos tan valiosos como el agua o la comida. Un atacante que acceda al correo electrónico, las conversaciones de grupo o los archivos en la nube de un preparacionista puede conocer su ubicación, inventario, planes de evacuación y red de contactos. La ciberseguridad no es un lujo tecnológico: es una capa de seguridad operativa fundamental. Esta guía cubre las medidas prácticas que cualquier persona puede implementar sin conocimientos técnicos avanzados, dentro del marco legal del Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos Personales.

Gestión de Contraseñas y Autenticación

La contraseña es la primera línea de defensa digital y, estadísticamente, la más vulnerada. Según el Instituto Nacional de Ciberseguridad (INCIBE), el 80% de las brechas de seguridad involucran contraseñas débiles o reutilizadas. Una contraseña robada en una filtración de un servicio irrelevante puede dar acceso al correo principal si se usa la misma clave.

Gestor de contraseñas: Usar un gestor como KeePassXC (código abierto, offline, multiplataforma) o Bitwarden (código abierto, sincronización cifrada). KeePassXC es preferible para preparacionistas porque funciona sin conexión a internet y almacena la base de datos localmente. La contraseña maestra del gestor debe ser una frase larga (mínimo 20 caracteres): "MiPerroCorrePorElCampoEnMarzo2024" es mucho más segura y memorable que "P@ssw0rd!23".

Contraseñas únicas para cada servicio: Nunca reutilizar contraseñas entre servicios. El gestor genera contraseñas aleatorias de 20+ caracteres para cada cuenta. Si un servicio sufre una filtración, solo esa cuenta queda comprometida.

Autenticación de dos factores (2FA): Activar 2FA en todas las cuentas que lo permitan, especialmente correo electrónico, banca online y redes sociales. Preferir aplicaciones de autenticación (Aegis para Android, Raivo para iOS, ambas de código abierto) sobre SMS. Los SMS pueden interceptarse mediante ataques de SIM swapping.

Llaves de seguridad físicas: Las llaves FIDO2/WebAuthn (como YubiKey o SoloKeys) son el método más seguro de 2FA. Son dispositivos USB/NFC que verifican la identidad físicamente. Coste: 25-60 euros. Inmunes a phishing porque verifican el dominio del sitio web automáticamente. Tener siempre dos llaves: una de uso diario y otra de respaldo guardada en lugar seguro.

Copia de seguridad de los códigos 2FA: Al activar 2FA, el servicio proporciona códigos de recuperación. Estos códigos deben guardarse en papel (no digitalmente) en un lugar seguro, como una caja fuerte o sobre sellado. Si se pierde el teléfono y no hay códigos de respaldo, se pierde el acceso a la cuenta permanentemente.

Verificación de filtraciones: Comprobar periódicamente si las cuentas de correo han aparecido en filtraciones conocidas mediante el servicio haveibeenpwned.com (gestionado por el experto en seguridad Troy Hunt). Si una dirección aparece como comprometida, cambiar inmediatamente la contraseña de ese servicio y de cualquier otro donde se usara la misma clave.

Comunicaciones Cifradas

Las comunicaciones entre miembros de un grupo de preparación contienen información sensible: ubicaciones de recursos, planes de evacuación, inventarios, datos personales. Esta información debe protegerse tanto en tránsito (mientras viaja por la red) como en reposo (almacenada en el dispositivo).

Signal como estándar de mensajería: Signal ofrece cifrado de extremo a extremo verificado y auditado. Los mensajes solo pueden leerse en los dispositivos del emisor y receptor, ni siquiera Signal tiene acceso. Activar los mensajes efímeros (autodestrucción en 1-4 semanas) para reducir la superficie de exposición si un dispositivo es comprometido.

Correo electrónico cifrado: Para comunicaciones por email, usar ProtonMail (servidores en Suiza, cifrado de extremo a extremo entre usuarios ProtonMail) o Tutanota (servidores en Alemania, cifrado automático). Para comunicación con personas que usan proveedores convencionales, ProtonMail permite enviar mensajes cifrados con contraseña compartida previamente.

VPN para navegación: Una VPN (Red Privada Virtual) cifra todo el tráfico entre el dispositivo y el servidor VPN, impidiendo que el proveedor de internet o un atacante en la misma red wifi vea la actividad de navegación. Opciones recomendadas: Mullvad (acepta pago en efectivo por correo, no requiere email ni datos personales) o ProtonVPN (opción gratuita limitada disponible).

DNS cifrado: Cambiar los servidores DNS del router doméstico a opciones que soporten DNS sobre HTTPS (DoH) o DNS sobre TLS (DoT). Opciones: Quad9 (9.9.9.9, sin ánimo de lucro, bloquea dominios maliciosos) o Cloudflare (1.1.1.1). Esto impide que el ISP registre los dominios visitados.

Red Tor para anonimato: El navegador Tor enruta el tráfico a través de tres nodos cifrados, haciendo extremadamente difícil rastrear el origen de la conexión. Útil para consultas sensibles que no deben vincularse a la identidad del usuario. Velocidad muy reducida, no apto para uso diario. Descargar solo desde torproject.org.

Legalidad del cifrado en España: El uso de cifrado, VPN y Tor es completamente legal en España. La Constitución Española protege el secreto de las comunicaciones (art. 18.3). Solo un juez puede autorizar la intervención de comunicaciones privadas. No obstante, las autoridades pueden solicitar judicialmente la entrega de contraseñas en el contexto de una investigación criminal.

Protección de Dispositivos y Datos Almacenados

Un dispositivo robado o perdido es una puerta abierta a toda la información del propietario si no está adecuadamente protegido. El cifrado del almacenamiento convierte los datos en ilegibles sin la contraseña correcta.

Cifrado completo del disco: En Windows: activar BitLocker (disponible en versiones Pro y Enterprise). En Linux: LUKS durante la instalación. En macOS: FileVault. En Android: el cifrado es obligatorio desde Android 10. En iOS: activado por defecto con código de desbloqueo. Un dispositivo cifrado que se pierde o es robado no expone datos al atacante.

Copias de seguridad cifradas: La regla 3-2-1: tres copias de los datos importantes, en dos soportes diferentes, una copia fuera del domicilio. Cifrar las copias con VeraCrypt (contenedor cifrado) o con la función de cifrado del propio software de backup. Una copia externa puede estar en casa de un familiar de confianza.

Actualizaciones de seguridad: Mantener el sistema operativo y todas las aplicaciones actualizadas. Las actualizaciones de seguridad corrigen vulnerabilidades conocidas que los atacantes explotan activamente. Configurar actualizaciones automáticas siempre que sea posible.

Antivirus y firewall: Windows Defender (incluido en Windows) es suficiente para la mayoría de usuarios. Mantenerlo activo y actualizado. No desactivar el firewall del sistema. En Linux, configurar ufw (Uncomplicated Firewall) para bloquear conexiones entrantes no solicitadas.

Separación de dispositivos: Si es posible, usar dispositivos separados para actividades sensibles (comunicaciones del grupo, gestión de inventarios) y uso general (redes sociales, navegación casual). Un teléfono secundario dedicado a Signal y poco más reduce la superficie de ataque considerablemente.

Datos en la nube: Los archivos almacenados en Google Drive, iCloud o Dropbox son accesibles para el proveedor del servicio y pueden ser entregados a autoridades bajo requerimiento judicial. Si se almacenan datos sensibles en la nube, cifrarlos localmente antes de subirlos con Cryptomator (código abierto, compatible con los principales servicios de nube).

Seguridad Operativa (OPSEC) Digital

La seguridad operativa digital consiste en minimizar la información que se expone involuntariamente a través de la actividad online. No importa tener las mejores contraseñas si se publica en redes sociales la ubicación del refugio, fotos del almacén de suministros o la lista de miembros del grupo.

Metadatos de fotografías: Las fotos tomadas con móvil contienen metadatos EXIF que incluyen coordenadas GPS exactas, fecha, hora y modelo de dispositivo. Antes de compartir cualquier foto online, eliminar los metadatos. En Android: Scrambled Exif. En iOS: configurar Ajustes > Privacidad > Localización > Cámara > Nunca. En PC: ExifTool.

Huella digital del navegador: La combinación de sistema operativo, resolución de pantalla, fuentes

instaladas, plugins y configuración del navegador crea una huella digital única que permite rastrear al usuario sin cookies. Usar Firefox con las extensiones uBlock Origin (bloqueador de anuncios y rastreadores) y configurar la protección contra rastreo en modo estricto.

Redes sociales: Nunca publicar: ubicación del domicilio o refugio, fotografías de almacenes o inventarios, planes de viaje con fechas, ausencias del domicilio, detalles sobre el grupo de preparación. Lo que se publica en internet es permanente e indexable. Un perfil en redes sociales es un dossier gratuito para cualquier atacante.

Compras online: Las compras de material de preparación crean un perfil de consumo. Diversificar proveedores, usar direcciones de entrega alternativas cuando sea posible y pagar en efectivo en tiendas físicas para artículos que no se desea vincular a la identidad digital. Las tarjetas prepago (disponibles en estancos) permiten compras online sin vincular la tarjeta bancaria principal.

Correo electrónico desechable: Para registros en foros, tiendas online o servicios no críticos, usar alias de correo (SimpleLogin, compatible con ProtonMail) o direcciones temporales. Esto evita que el correo principal aparezca en filtraciones de servicios secundarios.

La OPSEC digital es un hábito, no una configuración puntual. Revisar periódicamente qué información personal es accesible buscando el propio nombre en Google, verificando la configuración de privacidad de las redes sociales y auditando los permisos de las aplicaciones móviles (especialmente localización, cámara y micrófono).

 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.