Diez consejos de protección en el Día de Internet Segura 2026

«Seguridad Digital para Educar en tiempo de IA» es el lema elegido para el Día de Internet Segura 2026, un evento mundial que se celebra el segundo martes de febrero y que en España promueve INSAFE/INHOPE con el apoyo de la Comisión Europea y dentro de la red panaeuropea de Centros de Seguridad en Internet.

El objetivo general se repite de años anteriores: educar en ciberseguridad, concienciar de la necesidad de adoptar medidas proactiva de precaución y conseguir entre todos una Internet no solo más segura, también mejor, **responsable, respetuosa, crítica y creativa**.

Día de Internet Segura 2026

El evento se dirige especialmente a **niños y jóvenes**, imprescindibles como nueva generación para construir espacios digitales seguros y mejorados y ello pasa por el respeto, la protección de su reputación y la de los demás en la red de redes y buscando oportunidades positivas para crear, participar y compartir a través de Internet.

Otro grupo importante a los que se dirige este día son los **padres y tutores**, activos fundamentales con una misión no siempre sencilla para motivar e inculcar a sus hijos un uso responsable, respetuoso, crítico y creativo de la tecnología, bien sea estableciendo un diálogo abierto con sus hijos, educándolos en un uso seguro y positivo de la tecnología o actuando como referentes de comportamiento digital.

Los **profesores y educadores** son otro pilar fundamental para la creación de una Internet mejor capacitando a sus alumnos y estudiantes con competencias informáticas y ayudándolos a desarrollar habilidades que fomenten el pensamiento crítico, lo que les permitirá navegar mejor por Internet. Pueden animarlos a crear su propio contenido, tomar decisiones positivas en Internet y servir como ejemplo personal de comportamiento en la red a sus alumnos y estudiantes.

Las **empresas** también pueden colaborar en la creación de una Internet mejor creando contenido positivo y promoviendo servicios seguros en la red. Además, pueden fomentar que los usuarios sean capaces de hacer frente a los problemas que encuentren proporcionando consejos sobre el uso seguro de

Internet, una variedad de herramientas de seguridad que resulten fáciles de usar y un acceso rápido a la ayuda en caso de problemas.

Finalmente, **administraciones y gobiernos** también tienen mucho que hacer, proporcionando un entorno en el que todos los colectivos anteriores puedan trabajar y progresar, por ejemplo, asegurando que los planes educativos incluyan formación en materia de seguridad en Internet, que los padres y tutores puedan tener acceso a información adecuada y fuentes de apoyo, o asegurando que las empresas se comprometan a la autorregulación de sus contenidos y servicios. Asimismo, deben tomar la iniciativa legislativa para garantizar la seguridad y el bienestar de niños y jóvenes, como con el anuncio reciente de regulación de acceso a las redes sociales.

Consejos de protección en el Día de Internet Segura 2026

La celebración de esta jornada es un buen momento para recordar la necesidad de implementar a nivel de usuario una serie de **medidas proactivas para mejorar la seguridad en Internet**, fortalecer nuestras cuentas virtuales, el uso de aplicaciones y equipos.

Las amenazas están ahí y son cada vez peores. Exigen del usuario un **comportamiento proactivo y mucho sentido común**, entendiendo que la vida virtual hay que protegerla hoy tanto como la física y que las tareas domésticas se han mezclado peligrosamente con las profesionales. Garantizar la seguridad y privacidad al 100% no es posible en una red global, pero sí hay una serie de medidas que podemos adoptar para mejorarlas, que incluyen el fortalecimiento de las cuentas on-line, aplicaciones, equipos donde las usamos y las precauciones debidas en el uso de Internet y sus servicios.

Te las sabes de memoria porque forman parte de cualquier guía de ciberseguridad, pero ahí van una vez más como nuestro granito de arena para crear, juntos, una Internet mejor:

1. **Sentido común.** La prudencia es una barrera preferente contra el malware y por ello, debemos tener especial cuidado en el apartado de descargas e instalación de aplicaciones de sitios no seguros; en la navegación por determinadas páginas de Internet; en la apertura de correos electrónicos o archivos adjuntos no solicitados; en los que llegan de redes sociales o aplicaciones de

mensajería o en el uso de sistemas operativos y aplicaciones sin actualizar, que contienen vulnerabilidades explotables por los ciberdelincuentes para las campañas de malware.

2. **Cuidado con la desinformación.** Internet ha favorecido la llegada de una serie de personajes de los que debemos prevenirnos. **La desinformación**, las medias verdades, las noticias directamente falsas (fake news) o las que tienen una intención clara de manipular, son el pan nuestro de cada día. Cada vez son más peligrosas y llegan en un mayor número. Seamos responsables. Consultemos varias fuentes. No ayudemos a difundir toda esta basura que se usa para distribuir malware y para cosas peores.
3. **Protege los navegadores web.** Todos los navegadores web incluyen características avanzadas de seguridad cuya activación debemos revisar y configurar porque son las aplicaciones que usamos para acceder a Internet y sus servicios. Además de revisar el cifrado de extremo a extremo en la sincronización o el aislamiento de procesos (sandbox), debemos prestar atención a los avisos sobre sitios inseguros que muestran los navegadores. También revisar las extensiones instaladas porque algunas son una fuente frecuente de introducción de malware y valorar el uso del «Modo Privado», que aunque no es tanto como promete, puede mejorar la privacidad.
4. **Actualiza sistemas y aplicaciones.** Todos los sistemas operativos cuentan con herramientas para mantener actualizados sus equipos. Y son de uso obligado porque incluyen actualizaciones de seguridad contra amenazas conocidas. Tan importante -o más- que lo anterior es la actualización de aplicaciones instaladas a las últimas versiones ya que éstas suelen incluir parches de seguridad. Cuando las versiones son más antiguas, tienen mayor riesgo de ser atacadas por ciberdelincuentes que encuentran vulnerabilidades en el programa.
5. **Valora el uso de soluciones de seguridad.** Son múltiples los proveedores que ofrecen soluciones de seguridad tanto comerciales como gratuitas cuyo uso conviene valorar. Lo mismo con las aplicaciones nativas contra el malware que incluyen algunos sistemas operativos como el Microsoft Defender. Por muy prudentes que seamos, es difícil estar a salvo de todo el malware que llega a Internet. A nivel profesional, es obligatorio el uso de una suite de seguridad comercial integral que incluya herramientas como un firewall y herramientas especializadas contra ataques de Ransomware, Phishing, adware o spyware.

6. **Cuida las contraseñas.** El cuento de nunca acabar… Sí, son terribles en usabilidad, pero hasta que no tengamos una adopción masiva de técnicas avanzadas de identificación biométrica tendremos que usarlas con seguridad. Ya sabes, tienen que ser aleatorias, largas y complejas, y distintas para cada sitio web, especialmente los destinados a banca en línea y comercio electrónico. Valorar el uso de gestores de contraseñas capaces de hacer el trabajo por nosotros, reduciendo los errores humanos en su manejo y automatizando el proceso de generación y administración.
7. **Usa autenticación de dos factores.** Destinado a reforzar el uso de contraseñas, 2FA es un método de control de accesos que conocerás como «autenticación de dos factores», «doble identificación» o «verificación en dos pasos», que se ha convertido en uno de los mecanismos de seguridad más importantes de la industria tecnológica a la hora de autentificar usuarios y proteger identidades. Esta característica ya está disponible en la mayoría de servicios importantes de Internet y conviene utilizarla siempre que podamos, utilizando un código de verificación servido mediante una aplicación móvil o SMS.
8. **Valora el uso del cifrado.** El cifrado de unidad BitLocker es una característica de protección de datos del sistema operativo, disponible entre otras, en las ediciones Profesional y Enterprise de Windows 10 y 11. BitLocker permite cifrar o "codificar" los datos de tu equipo para mantenerlos protegidos haciendo frente a amenazas como el robo de datos o la exposición en caso de pérdida, el robo o la retirada inapropiada de equipos, y en definitiva mejorando la seguridad en línea.
9. **Cuidado con las redes inalámbricas gratuitas.** Los puntos de acceso gratuitos se han extendido por múltiples zonas en poblaciones, zonas de restauración, aeropuertos, estaciones de tren o metro, hoteles y en todo tipo de negocios. Investigadores de seguridad han demostrado la inseguridad intrínseca de las redes inalámbricas públicas. Por lo general, son fácilmente pirateables por lo que únicamente deberíamos utilizarlas para navegación ocasional.
10. **Utiliza una llave de seguridad hardware para cuentas vitales.** Para cuentas vitales, especialmente en entornos profesionales y empresariales, conviene hacer un esfuerzo adicional para protegerlas usando un mecanismo de seguridad por hardware. Generalmente es un dispositivo en formato pendrive que se conecta a un puerto USB y contiene

un motor de cifrado de alta seguridad. Todo el proceso se realiza dentro del hardware aumentando enormemente la seguridad general frente a las soluciones por software.

Muy Computer