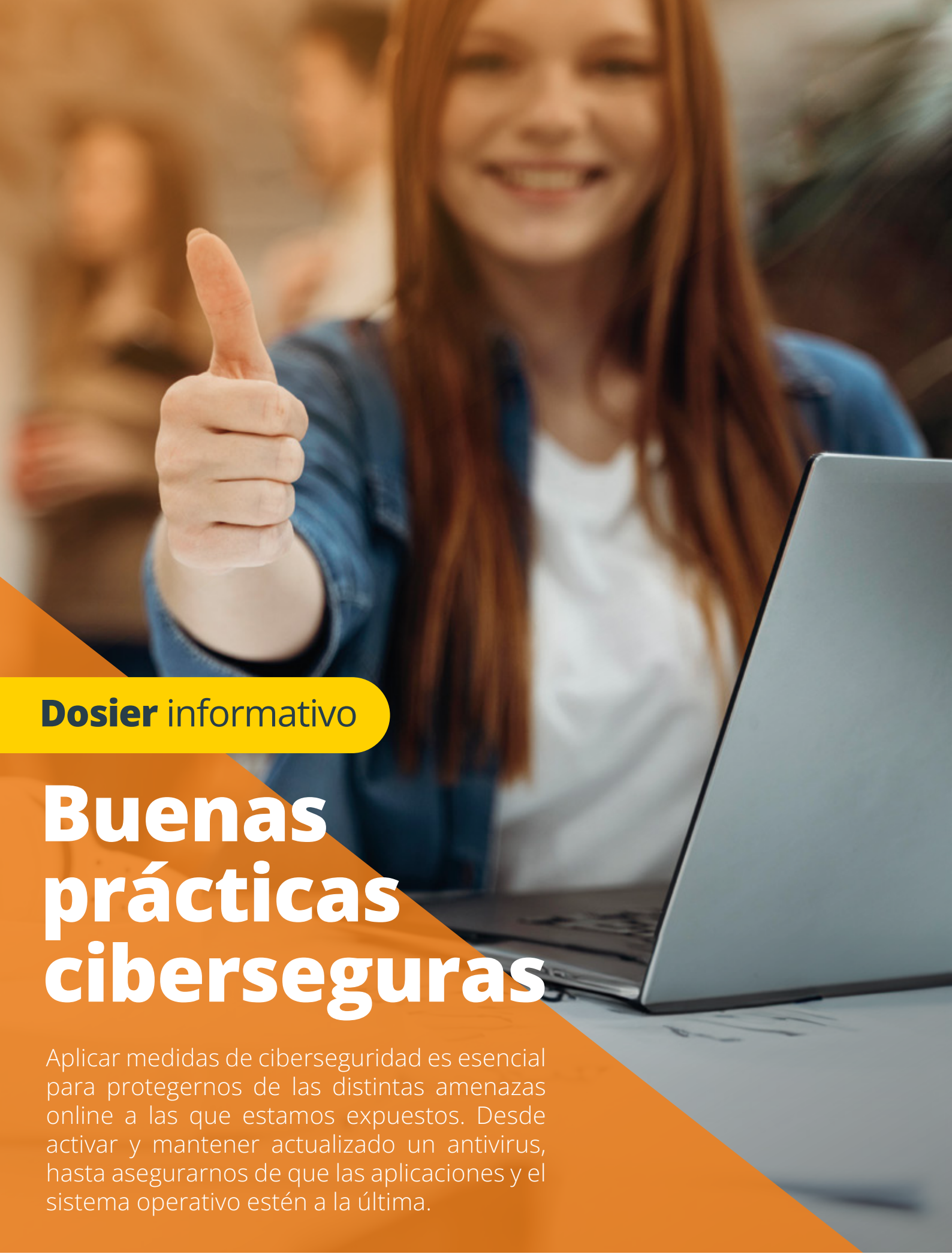


Dosier informativo

Buenas prácticas ciberseguras

Aplicar medidas de ciberseguridad es esencial para protegernos de las distintas amenazas online a las que estamos expuestos. Desde activar y mantener actualizado un antivirus, hasta asegurarnos de que las aplicaciones y el sistema operativo estén a la última.

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

OSI Oficina de Seguridad del Internauta

¿Te sientes **identificado** con alguna de las siguientes **situaciones de riesgo**?

1. Te vas de viaje y...

- **te conectas a cualquier wifi.** El uso de redes wifi públicas o no seguras en hoteles, aeropuertos y cafeterías puede exponer tus datos a posibles ataques. Los ciberdelincuentes pueden interceptar tu tráfico y robar información confidencial.

- **pierdes o te roban el dispositivo.** Si pierdes tu teléfono, tablet u ordenador portátil mientras estás de viaje, tus datos personales pueden estar en peligro, especialmente si no están protegidos por contraseña o cifrados.

2. Haces planes y publicas dónde y qué estás haciendo...

- **dejando tu privacidad debilitada.** Compartir demasiada información en redes sociales sobre tu ubicación y planes de viaje puede hacer que seas un objetivo para planear ataques dirigidos y fraudes que tengan como finalidad el robo.

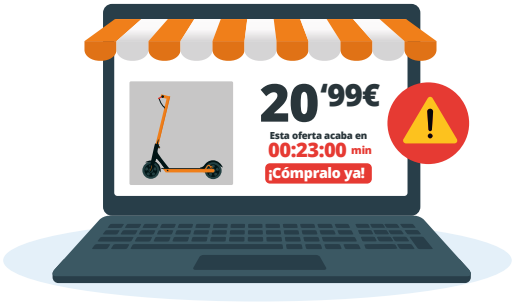
- **revelando información personal o sensible.** Compartir detalles sobre tus actividades y costumbres puede revelar información personal o suplantar tu identidad para engañar a otros usuarios.

3. Te toca teletrabajar y...

- **te conectas a cualquier wifi.** Si desconoces la configuración de una red wifi, la comunicación puede quedar comprometida facilitando que accedan a toda la información que compartes a través de dicha Red.

- **usas cualquier equipo para las funciones profesionales.** Los dispositivos personales utilizados para el trabajo, como ordenadores o teléfonos, pueden no tener los mismos niveles de seguridad implementados que los proporcionados por la empresa. No se recomienda su uso para este fin.

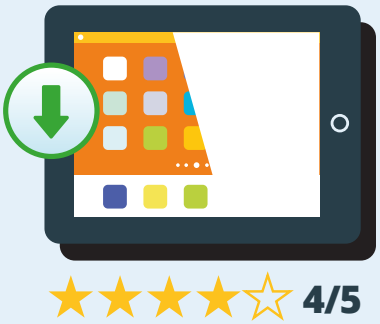
4. Compras un producto online...



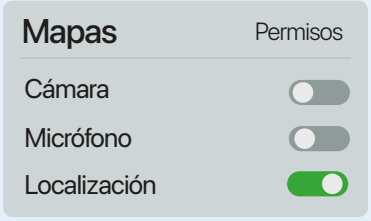
- **en una página donde el precio es irresistible.** Existe la posibilidad de que te encuentres con sitios web o vendedores falsos que intenten estafarte. Pueden ofrecer productos atractivos a precios bajos para atraer a los compradores y luego desaparecer.

- **y no lees las condiciones de entrega y devoluciones.** Si no tienes cuidado al elegir vendedores en línea, podrías enfrentar problemas relacionados con la entrega de los productos comprados o dificultades para realizar devoluciones y obtener reembolsos.

5. Descargas una aplicación en tu dispositivo...



- **sin revisar las valoraciones, comentarios ni opiniones que tiene.** No contrastar si se trata de una aplicación fiable y legítima puede derivar en problemas de privacidad y seguridad, si la app no tiene buenas intenciones.



- **y aceptas todos los permisos solicitados.** Muchas aplicaciones solicitan permisos que no son necesarios para su uso, se recomienda aceptar aquellos que son estrictamente necesarios para el correcto funcionamiento de la app.

¿Qué **medidas** puedes aplicar para estar **protegido**?

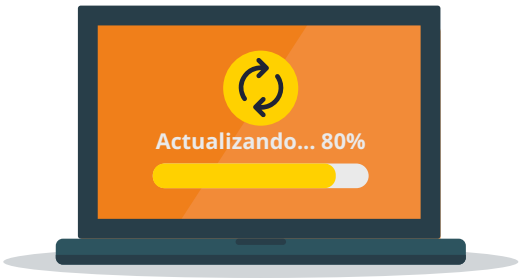
1 Activar una herramienta antivirus y cortafuegos

Imagina que tu ordenador es como tu casa y los virus son intrusos peligrosos. **Activar y mantener actualizado tu antivirus** es como asegurarte de que todas las puertas y ventanas de tu casa están cerradas y protegidas contra ladrones.

Además, **configurar y activar un cortafuegos** es como tener un muro de seguridad alrededor de tu casa que impide que los intrusos se acerquen a tus puertas y ventanas. De esta manera, **estás creando una doble capa de protección** que mantiene tu dispositivo seguro de amenazas externas.

Virus y otras amenazas

2 Actualizar el sistema operativo y las aplicaciones



Las **actualizaciones** son como arreglar las cerraduras de tus puertas y ventanas. Si no las realizas, estás dejando abiertas las **posibilidades de que los ciberdelincuentes encuentren vulnerabilidades** en tus aplicaciones o sistema operativo para infiltrarse en tu dispositivo y causar problemas en tu vida digital.

Configuraciones básicas de seguridad

3 Crear cuentas de usuario

El uso de una cuenta específica para cada usuario en un dispositivo, además de **facilitar una experiencia individualizada**, es importante para **mantener la privacidad y seguridad de la información de cada usuario**, estableciendo claves únicas para el acceso que protegen la información personal de cada uno.

Cuentas de usuario

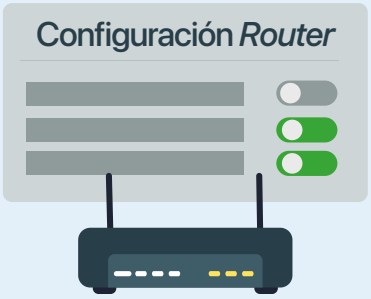
4 Gestionar correctamente las contraseñas

Son las llaves que te **dan acceso a tus cuentas en línea**, correos electrónicos y redes sociales. Si utilizas contraseñas débiles o las compartes, estás dejando las puertas abiertas a posibles accesos no autorizados a tus cuentas, lo que puede llevar a la suplantación de identidad o el robo de información personal.

Además, **activar la autenticación de dos factores (2FA)** es como agregar una cerradura adicional a tus puertas, requiriendo para su acceso no solo la llave (contraseña), sino también **un código adicional que solo tú posees**, dificultando que desconocidos accedan a ellas.

Contraseñas seguras

5 Configurar adecuadamente el *router*



Internet es lo que te permite acceder al mundo digital conectado. Si no proteges adecuadamente tu *router*, **estableciendo una contraseña segura** para su acceso o **configurando un protocolo de cifrado** para el intercambio de información seguro, entre otras acciones, estás facilitando que **otros usuarios se conecten a tu wifi** para cualquier fin.

Conexiones seguras

6 Hacer copias de seguridad

Realizar copias de seguridad de tus datos es como tener una caja de seguridad para tus documentos importantes. Si no lo haces, **puedes perder fotos, documentos y recuerdos** irreemplazables en caso de un fallo en el dispositivo, pérdida o debido a un ciberincidente.

Copias de seguridad

7 Cifrar la información

El cifrado garantiza que la información permanezca inaccesible para personas no autorizadas, es decir, la convierte en ilegible para aquellos que no dispongan de la clave de descifrado. Este proceso es **clave para la privacidad y seguridad**, ya que previene el robo de información y protege datos personales, financieros y comerciales durante su almacenamiento y su transmisión.

Cifrado de la información

¿Qué **otras prácticas** puedes aplicar?

1 Cuidar tu privacidad en las redes sociales

Las redes sociales son como un **escaparate de tu vida personal**. Si no revisas y configuras adecuadamente tus opciones de privacidad, **estás exponiendo tu información a extraños**, además de dejar pistas sobre tu ubicación, actividades, estilo de vida, nivel adquisitivo, etc.

Privacidad, identidad digital y reputación online

2 Contrastar la información que leas en Internet

La información en Internet es como un mar de datos. Si confías ciegamente en todo lo que lees, puedes caer en la trampa de la **desinformación o estafas**. Es esencial ser crítico y **verificar la fuente y la veracidad** de la información antes de tomar decisiones basadas en ella.

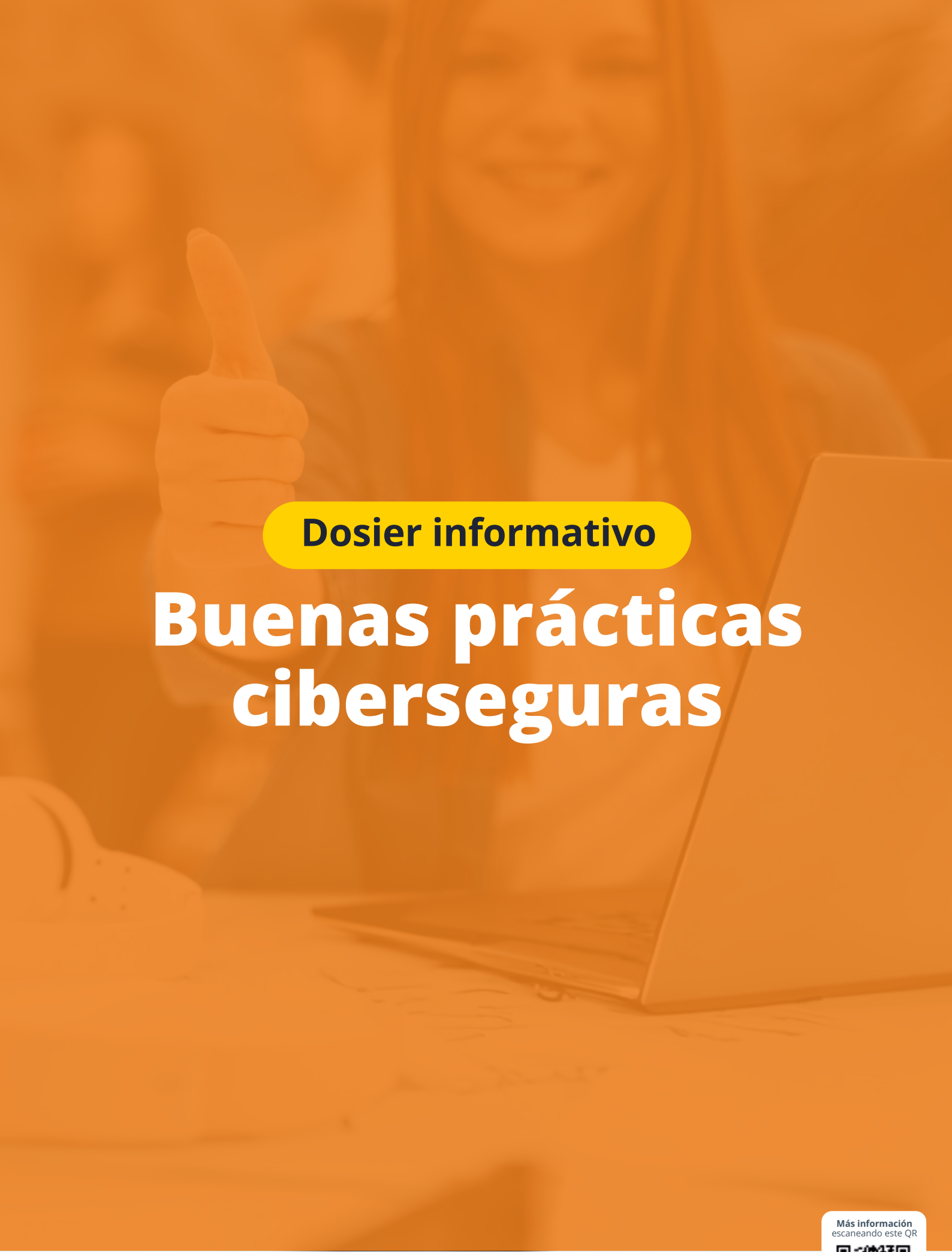
Bulos y noticias falsas

3 Realizar una compra cibersegura

A medida que el comercio electrónico se ha vuelto cada vez más popular, también **ha aumentado el número de estafas y fraudes en línea.**

Por eso, **es esencial que tengas en cuenta algunas precauciones** para asegurar que tus compras en Internet sean seguras.

Compras seguras online



Dosier informativo

Buenas prácticas ciberseguras

Más información
escaneando este QR

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

OSI Oficina de Seguridad del Internauta