



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Taller “Seguridad y privacidad en servicios de Internet”



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

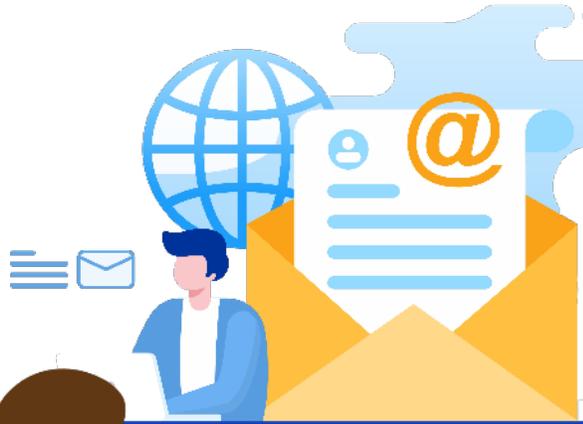
SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



TU AYUDA EN
CIBERSEGURIDAD
incibe_



Oficina
de Seguridad
del Internauta



Introducción

1. Seguridad y privacidad en servicios de correo electrónico y redes sociales.
2. Los riesgos de usar una única contraseña para todos los servicios.
3. Descarga de *software* / servicios de sitios oficiales.
4. Descarga de *apps* de sitios oficiales.
5. Almacenamiento en la nube.

Cuestionario de evaluación

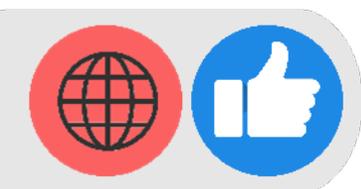
INTRODUCCIÓN

En este taller nos centraremos en las **buenas prácticas relacionadas con el uso seguro de los servicios web más populares.**



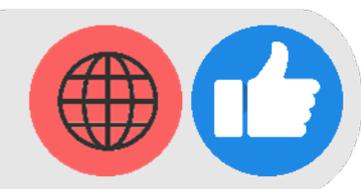
1. SEGURIDAD Y PRIVACIDAD DE CORREO ELECTRÓNICO Y REDES SOCIALES

La configuración de seguridad y privacidad de nuestros servicios es fundamental para protegernos frente las amenazas.



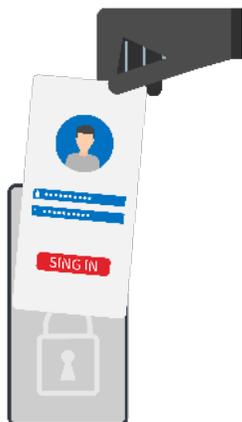
1.1 CONFIGURACIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LAS CUENTAS DE CORREO ELECTRÓNICO

Pautas para **minimizar los riesgos**:



1.2 IDENTIFICACIÓN DE RIESGOS EN REDES SOCIALES

Robos de datos y *malware*



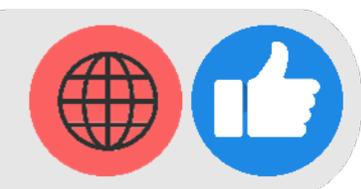
Suplantación de identidad



Fake News o bulos

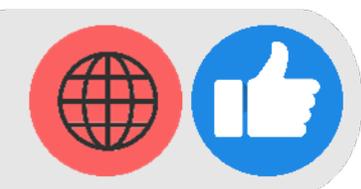
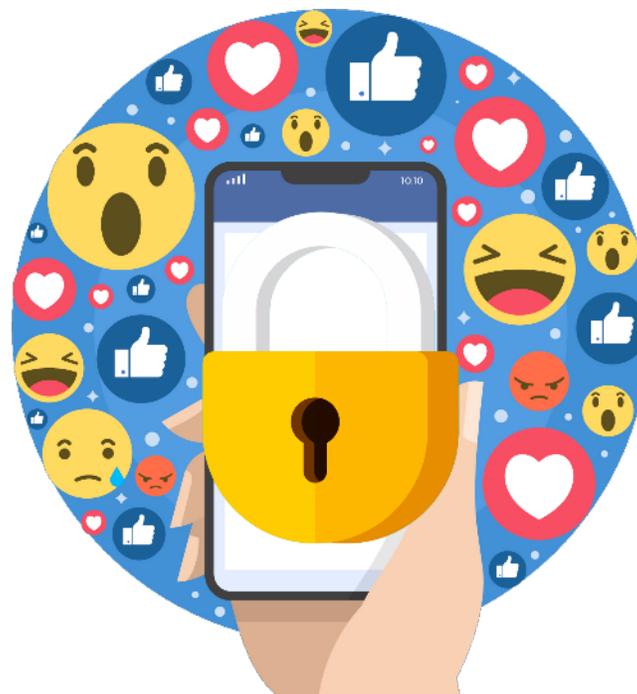


Acoso



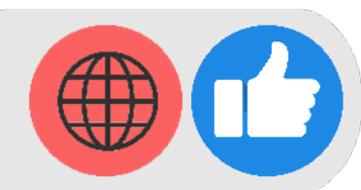
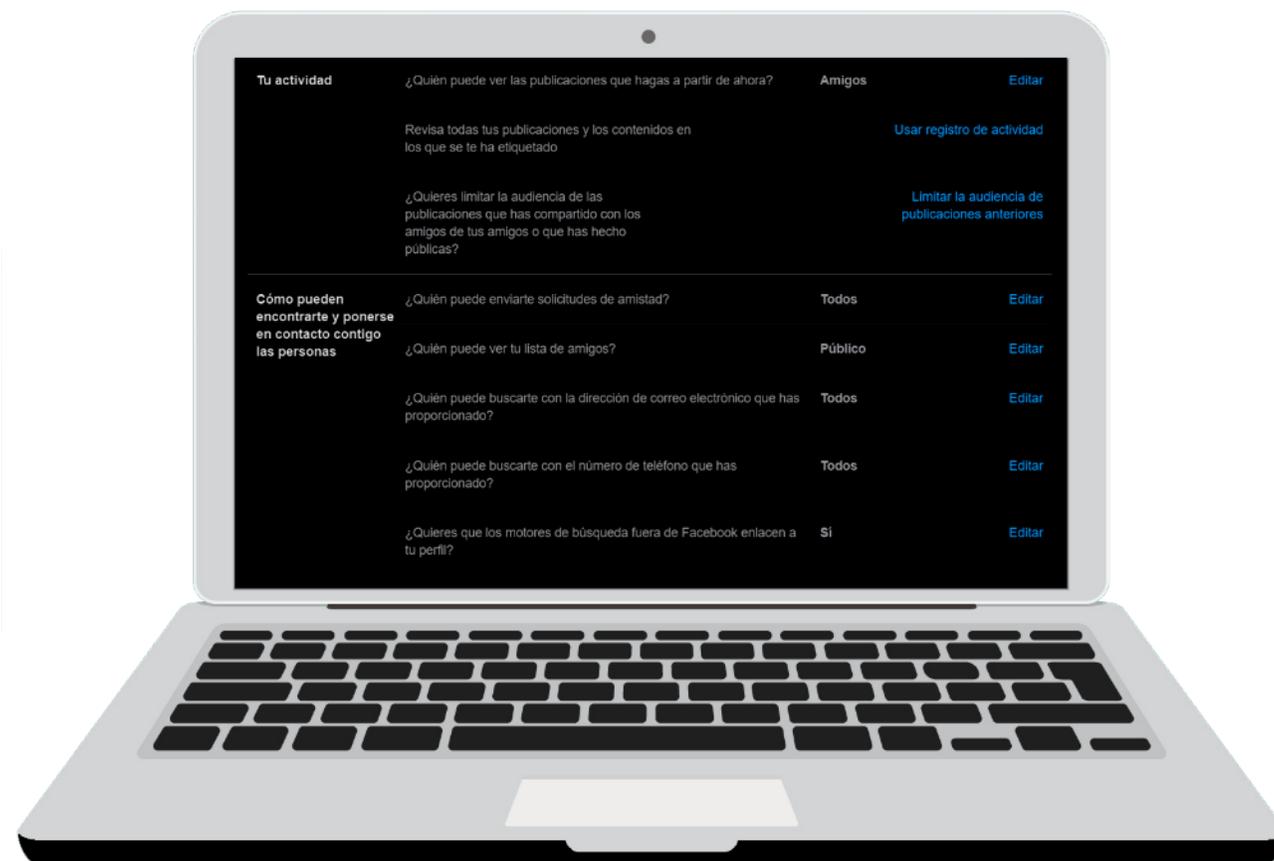
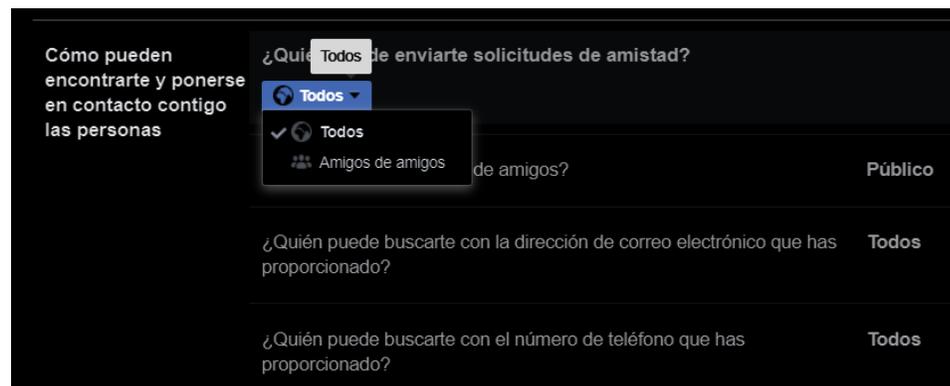
1.3 CONFIGURACIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LAS CUENTAS DE REDES SOCIALES

Podemos mejorar la seguridad y privacidad de nuestras cuentas.



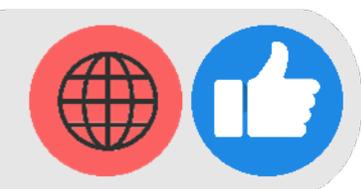
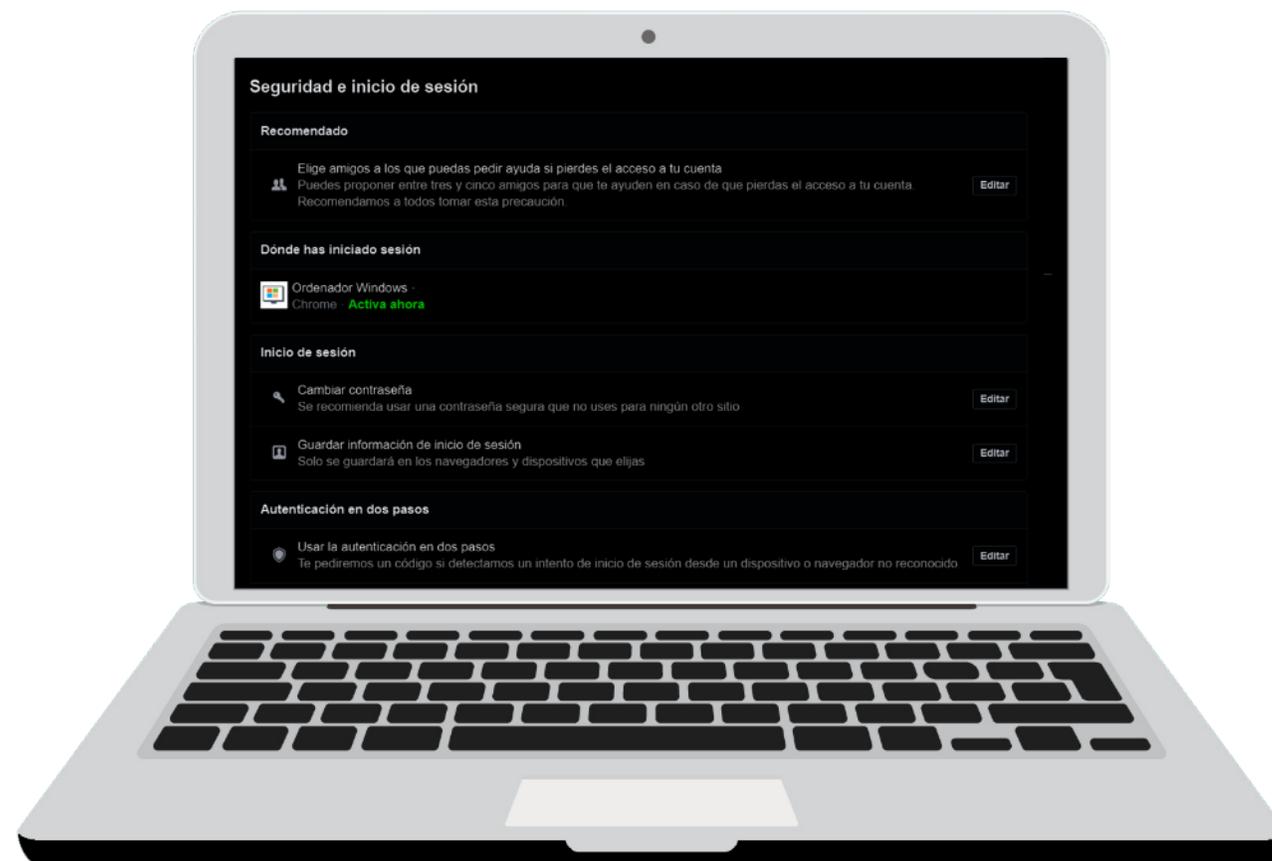
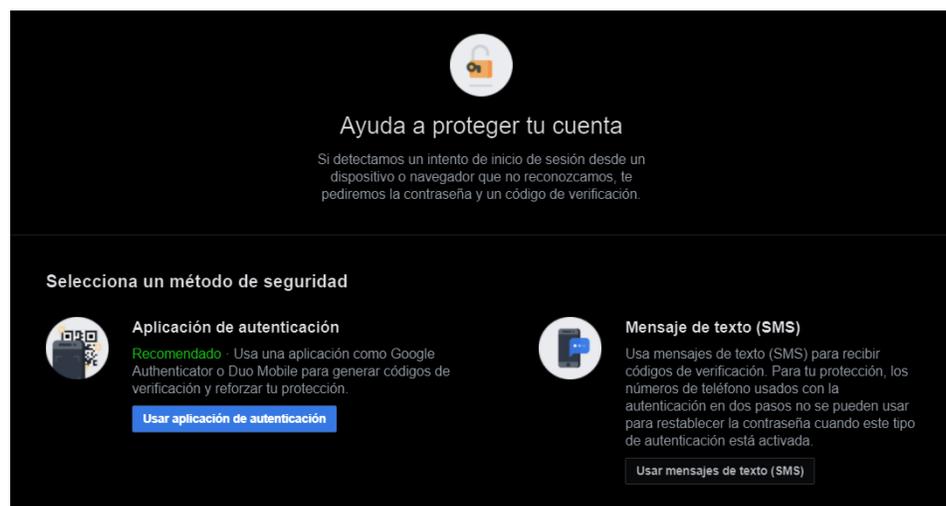
1.3.1 FACEBOOK

Configuración y privacidad > Configuración > Privacidad:



1.3.1 FACEBOOK (II)

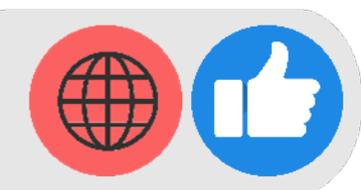
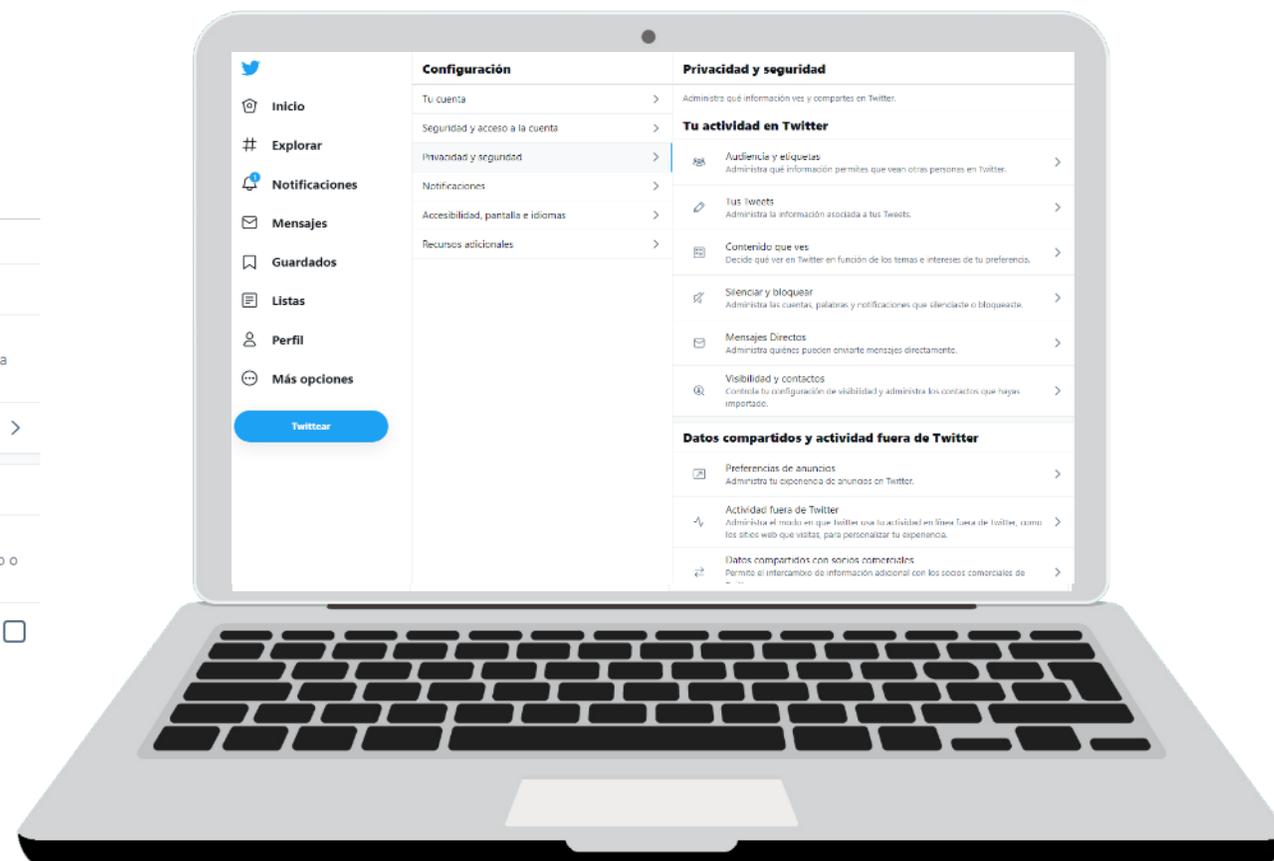
Desde **Configuración > Seguridad e inicio de sesión**:



1.3.2 TWITTER

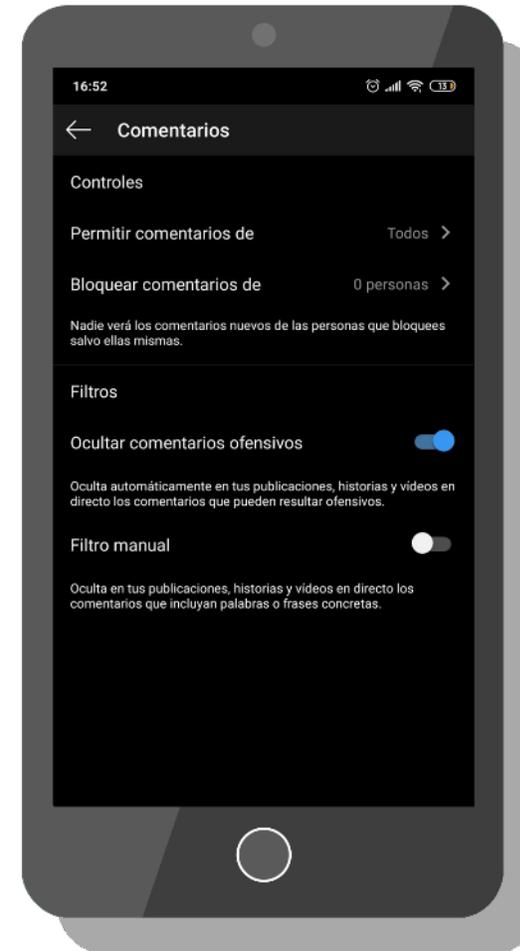
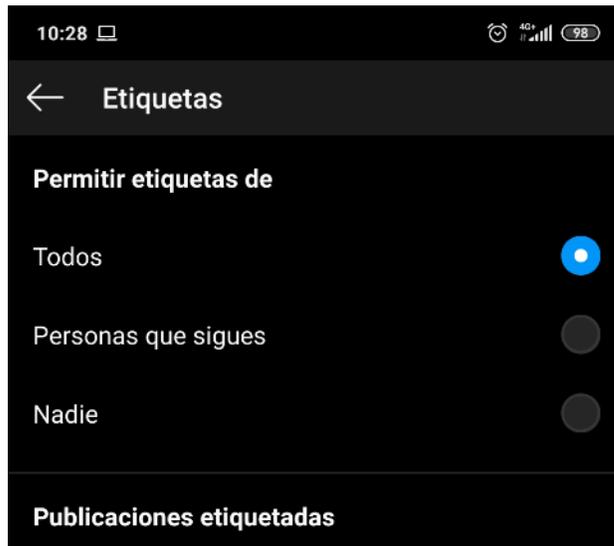
Más opciones (...) y luego en Configuración y privacidad > Privacidad y seguridad:

Configuración	← Seguridad
Tu cuenta >	Administra la seguridad de tu cuenta.
Seguridad y acceso a la cuenta >	Autenticación en dos fases
Privacidad y seguridad >	Ayuda a proteger tu cuenta contra el acceso no autorizado utilizando un segundo método de autenticación, además de tu contraseña de Twitter. Puedes elegir entre un mensaje de texto, una app de autenticación o una llave de seguridad. Más información
Notificaciones >	Autenticación en dos fases >
Accesibilidad, pantalla e idiomas >	
Recursos adicionales >	Protección con contraseña adicional
	Activar esta configuración aumenta la seguridad de tu cuenta, ya que se solicitará información adicional para restablecer tu contraseña. Si la activas, debes proporcionar el número de teléfono o la dirección de correo electrónico asociada a tu cuenta para poder restablecer tu contraseña.
	Protección de restablecimiento de la contraseña <input type="checkbox"/>



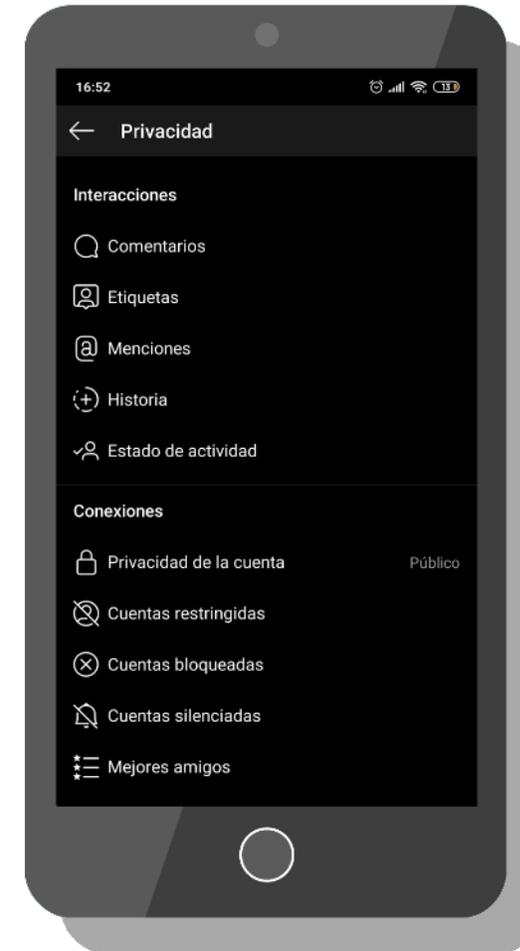
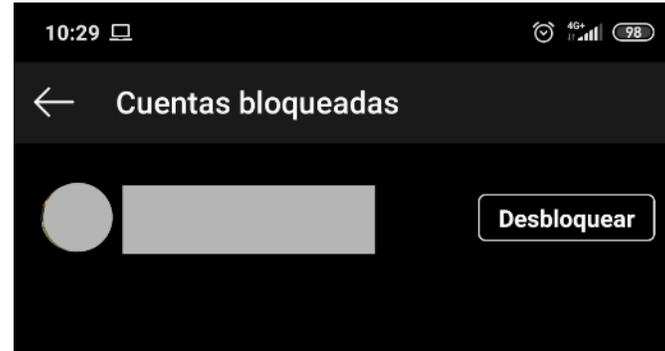
1.3.3 INSTAGRAM

Seleccionaremos las **opciones** y luego **Configuración > Privacidad:**



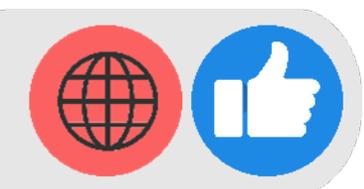
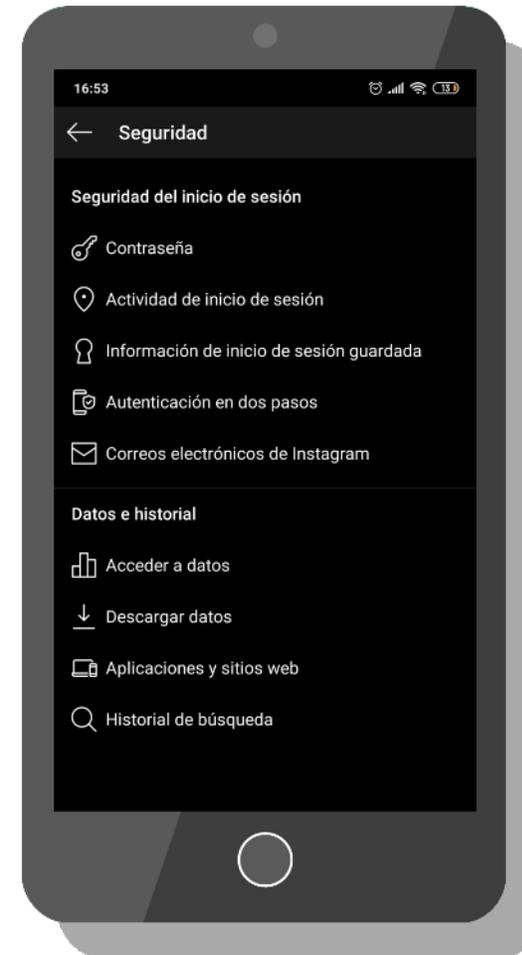
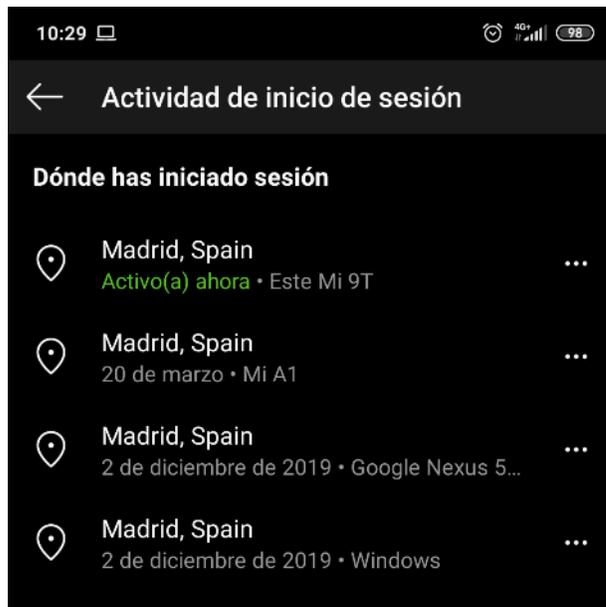
1.3.3 INSTAGRAM (II)

- ❖ Privacidad de la cuenta.
- ❖ Cuentas restringidas.
- ❖ Cuentas bloqueadas.
- ❖ Cuentas silenciadas.
- ❖ Mejores amigos.
- ❖ Cuentas que sigues.



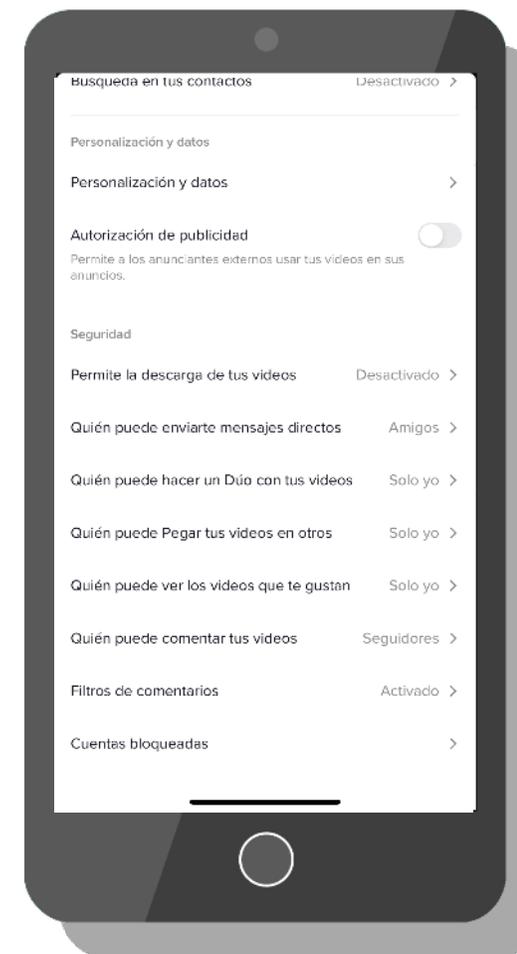
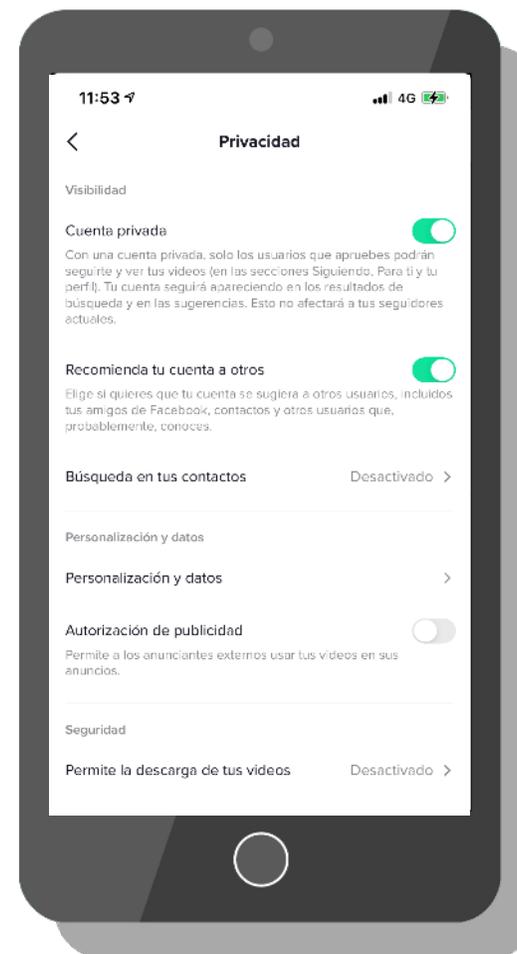
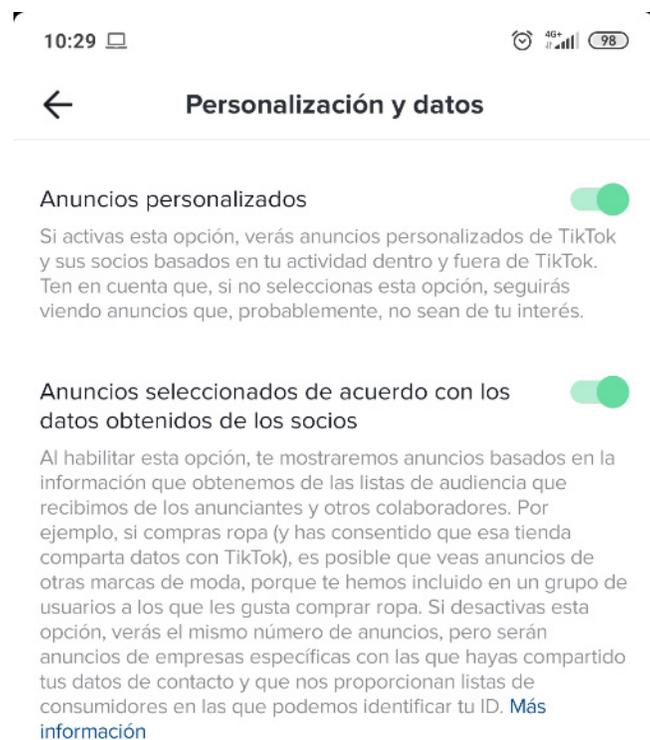
1.3.3 INSTAGRAM (III)

Desde **opciones > Configuración > Seguridad:**



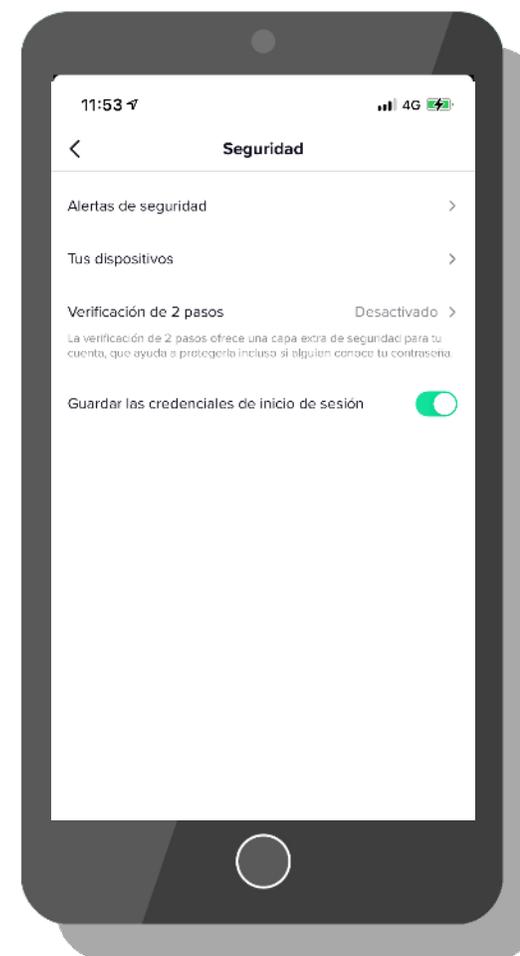
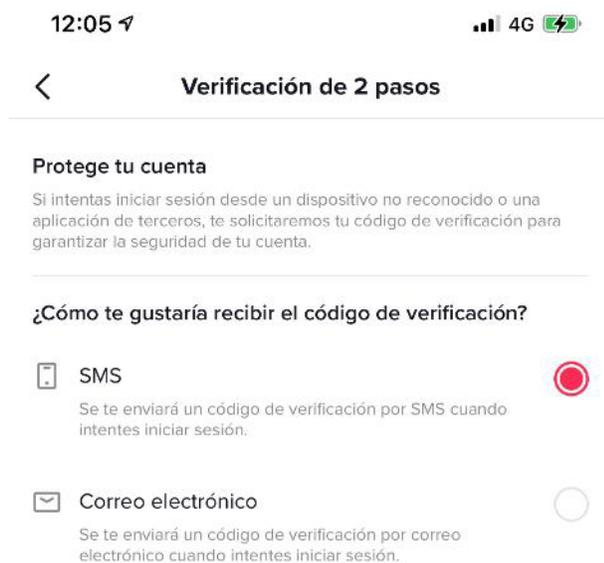
1.3.4 TIKTOK

Deberemos seleccionar las opciones y hacer clic en **Privacidad**.



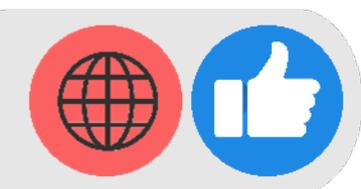
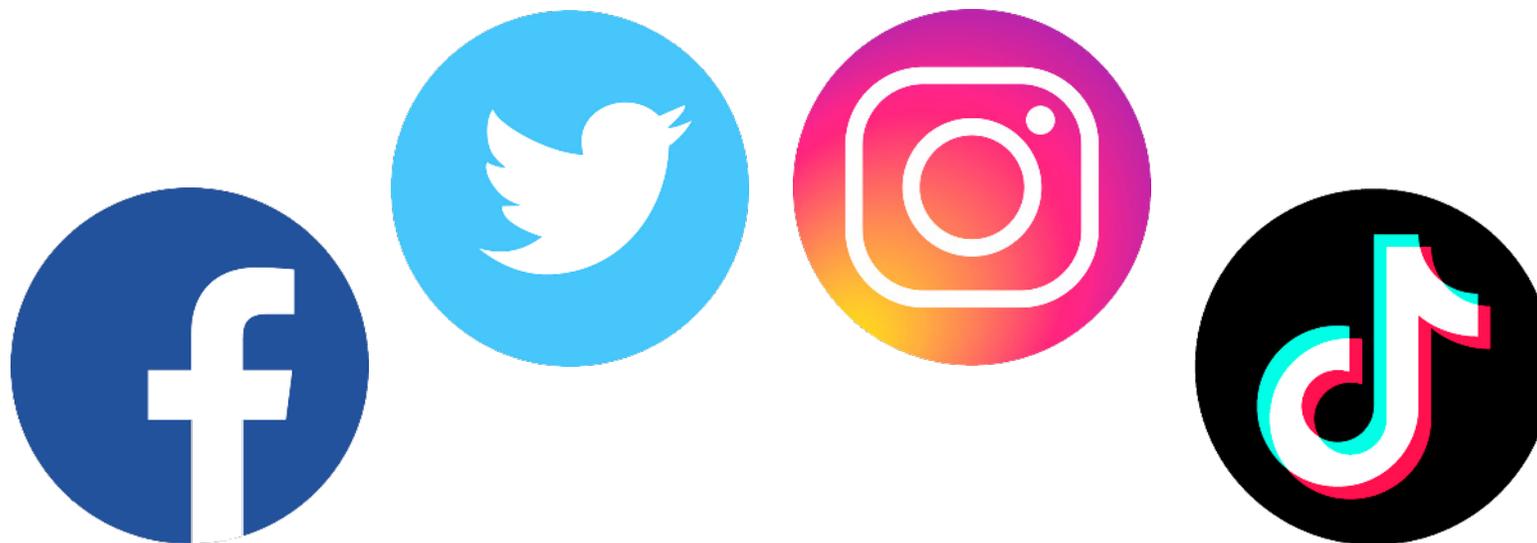
1.3.4 TIKTOK (II)

Deberemos seleccionar las opciones y hacer clic en **Seguridad**.



1.4 DENUNCIAR UNA SUPLANTACIÓN O ROBO DE CUENTA

Las redes sociales ponen a nuestra disposición un servicio para **denunciar cuentas**:



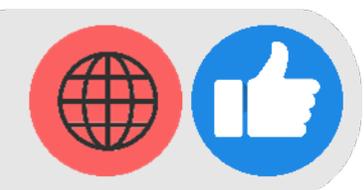
Actividad 1



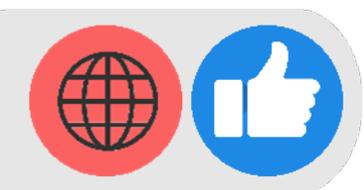
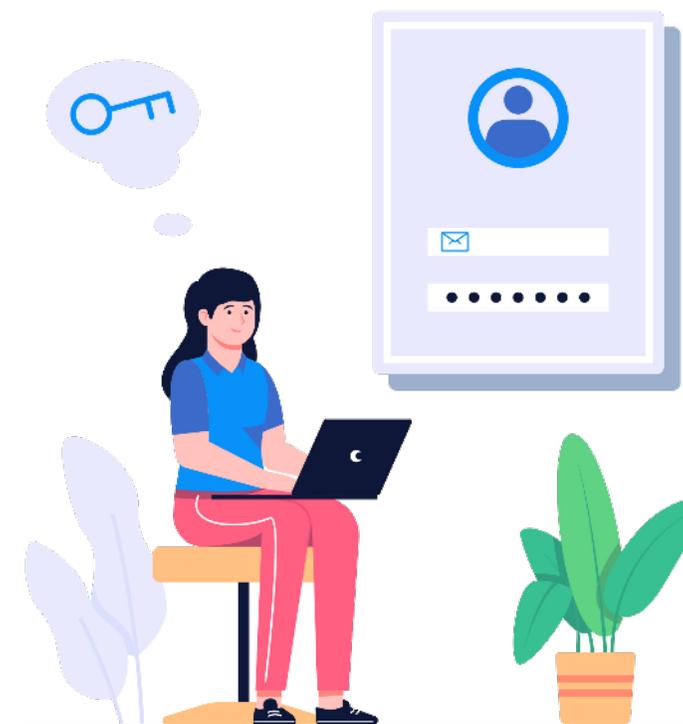
¿Crees que tienes configurada correctamente tu red social favorita? Ante la duda, la mejor opción es dedicar unos minutos a revisar los ajustes de seguridad y privacidad para evitar que terceros con malas intenciones vean nuestras publicaciones.

2. LOS RIESGOS DE UNA ÚNICA CONTRASEÑA PARA TODOS LOS SERVICIOS

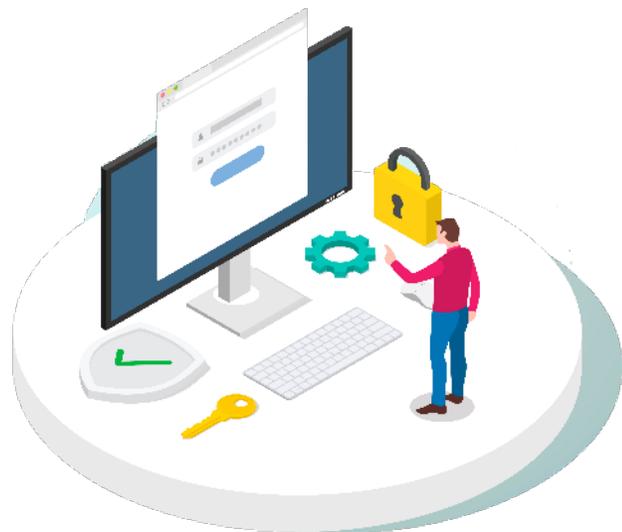
¿La misma contraseña para todo? ¡No lo pongamos tan fácil!



2.1 BUENAS PRÁCTICAS



2.1 BUENAS PRÁCTICAS (II)



1. ESCOGER UNA COMBINACIÓN DE PALABRAS

Contraseña

Seguridad

2. LAS UNIMOS Y AÑADIMOS ALGUNA MAYÚSCULA Y NÚMERO

C0ntraseñas3guridad

3. AÑADIMOS UN CARÁCTER ESPECIAL

C0ntraseñas3guridad!



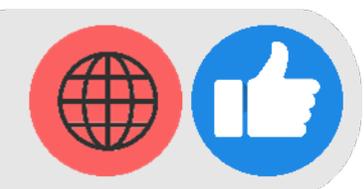
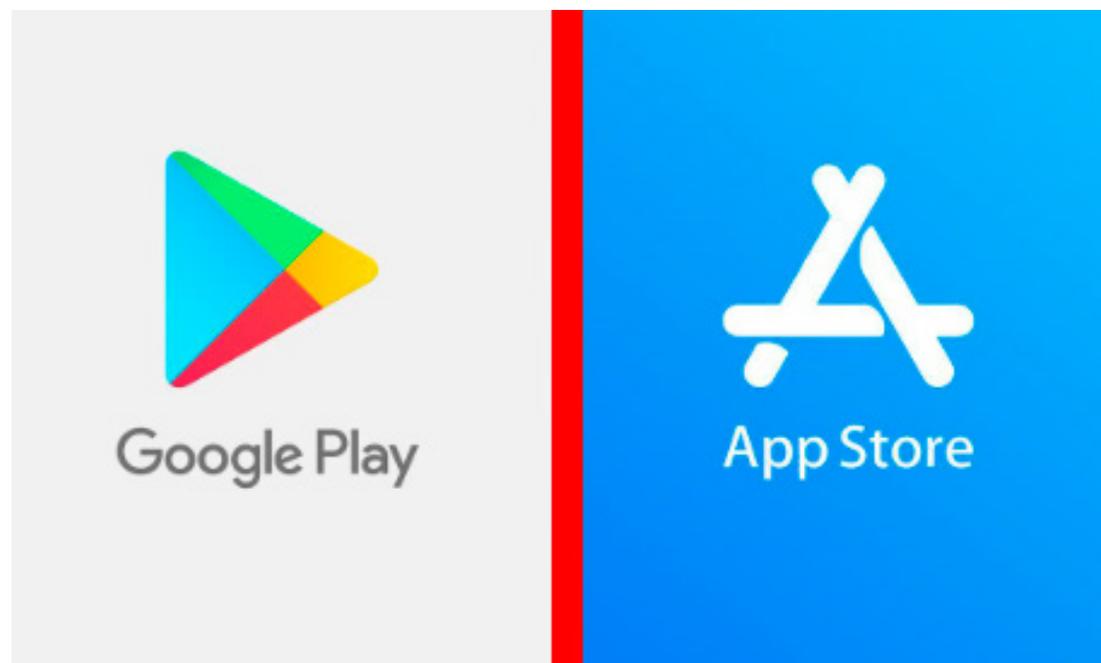
ACTIVIDAD 2



Los gestores de contraseñas son una herramienta muy útil para mantener nuestras cuentas seguras. Aprovecha, entra en la sección de herramientas de la OSI y descarga alguno de sus gestores de contraseñas. Prueba a configurarlo con tus contraseñas principales y verás lo útil que puede llegar a ser.

3. DESCARGA DE SOFTWARE / SERVICIOS DE SITIOS OFICIALES

A la hora de **descargar un software de Internet**, es fundamental que lo hagamos desde el **sitio web del fabricante o la web oficial**.



3.1 CÓMO DETECTAR FRAUDES



Dirección web o URL



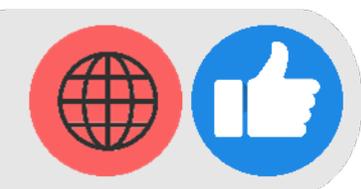
Anuncios y *banners*



Alertas de virus y actualizaciones



Precio



4. DESCARGA DE APPS DE SITIOS OFICIALES

Es fundamental utilizar las **tiendas oficiales**. Sin embargo, a veces **los filtros pueden fallar**.



ACTIVIDAD 3

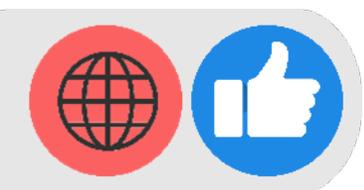
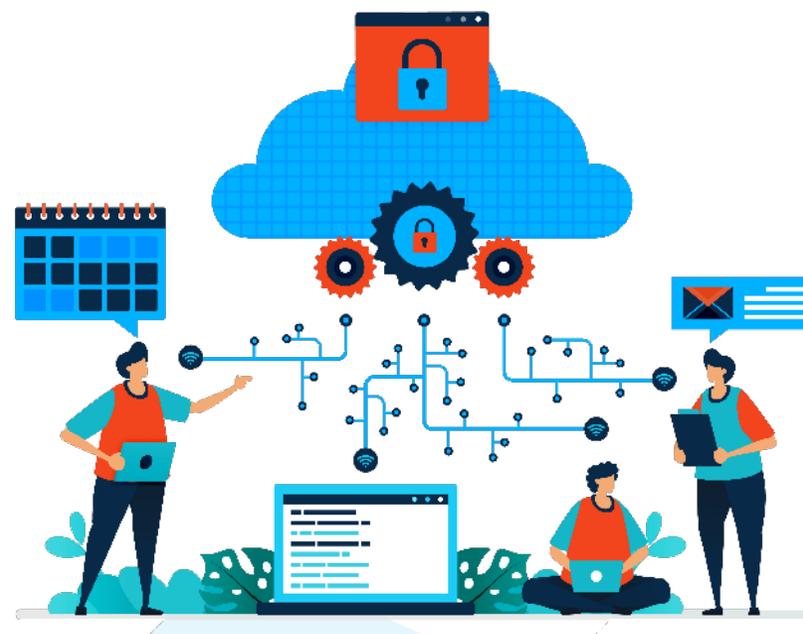
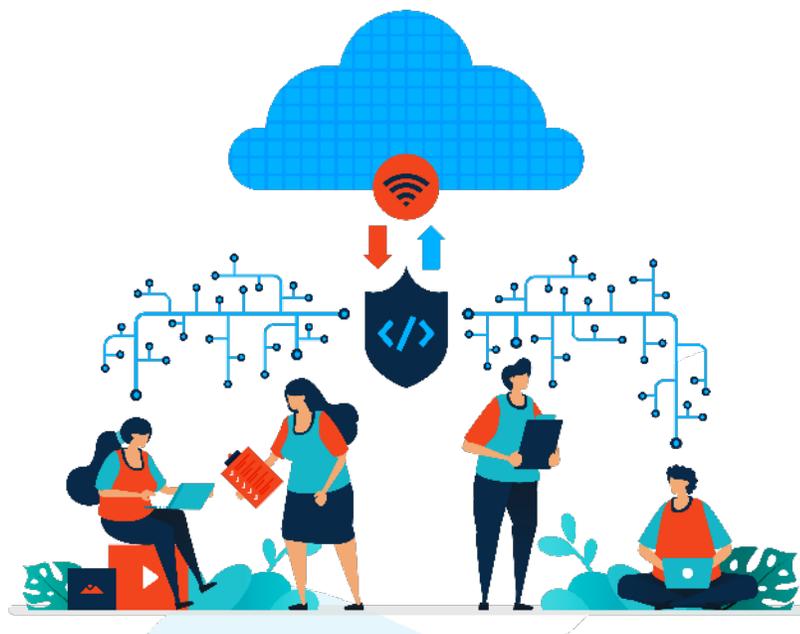


Seguro que has descargado alguna *app* en tu *smartphone* o *tablet* alguna vez. Como forma de poner en práctica los buenos hábitos recién explicados, entra en la tienda oficial de tu sistema operativo, busca una *app* y revisa los comentarios, el desarrollador y los permisos que pide al instalarla.

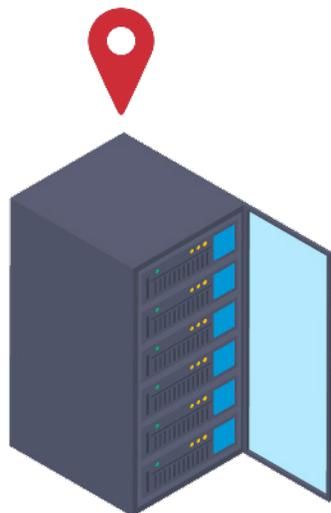
También, puedes acceder a las aplicaciones instaladas en tu dispositivo para analizar los permisos otorgados.

5. ALMACENAMIENTO EN LA NUBE

Es un hecho que la nube nos ofrece muchos **beneficios** pero, ¿están realmente a salvo estos datos?



5.1 USAR UN SERVICIO SEGURO



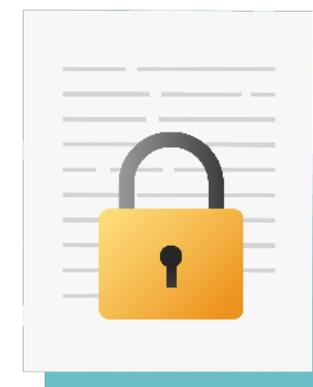
Ubicación de la información



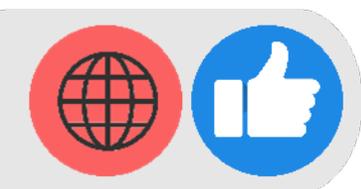
Presencia de terceros



Confidencialidad de la información



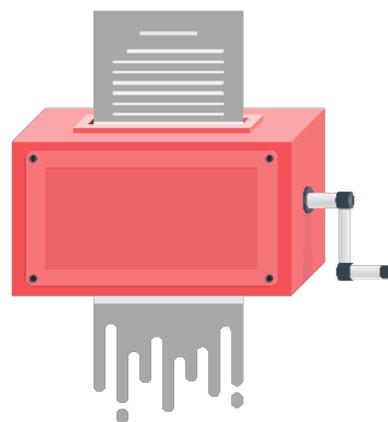
Mecanismos de cifrado



5.1 USAR UN SERVICIO SEGURO (II)



Políticas de seguridad y privacidad



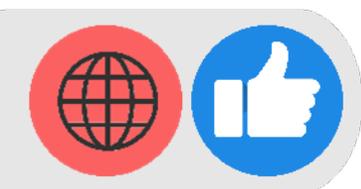
Eliminación segura



Condiciones de uso



Ejerce tus derechos



5.2 CIFRADO DE DATOS PERSONALES

¿Qué garantías de seguridad debemos comprobar antes de decantarnos por uno u otro servicio en la nube?

CONFIDENCIALIDAD INFORMACIÓN



5.2 CIFRADO DE DATOS PERSONALES - VIDEO



5.3 BUENAS PRÁCTICAS

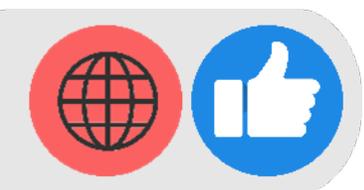
Para maximizar la seguridad y disponibilidad de nuestra información, deberemos:



Contraseña robusta



Copia de seguridad en soportes alternativos



5.3 BUENAS PRÁCTICAS (II)



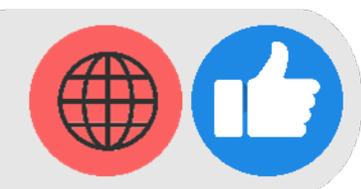
Compartir ficheros con quien quieres



Permisos



Clasificación de la información



ACTIVIDAD 4



Ahora que conoces los pasos a seguir para llevar a cabo el cifrado de archivos y carpetas, ¿por qué no lo intentas? Lleva a cabo el cifrado de alguna carpeta con varios archivos en su interior. Puede resultarte muy útil la próxima vez que crees tu copia de seguridad.

EN INCIBE TE AYUDAMOS



INSTITUTO NACIONAL DE CIBERSEGURIDAD

www.incibe.es



TU AYUDA EN CIBERSEGURIDAD



www.osi.es



www.is4k.es



www.incibe.es



Programas de formación



Recursos: servicios, herramientas, guías, juegos, etc.



CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



1. Los mensajes no deseados, generalmente de publicidad se conocen con el nombre de:

- A. *Spam.*
- B. *Phishing.*
- C. *Smishing.*

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



2. A través de nuestras interacciones en redes sociales, las empresas pueden:

- A. Crear patrones de comportamiento.
- B. Crear perfiles de consumidor.
- C. Ambas opciones.

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



3. El tipo de acoso donde se extorsiona a otra persona mediante el uso de fotografías de carácter íntimo o sexual se conoce como:

- A. *Sexting.*
- B. *Sextorsión.*
- C. *Grooming.*

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



4. ¿Cuál de las siguientes opciones puede ser configurada desde el perfil de nuestras redes sociales?

- A. El número de seguidores.
- B. Filtrar datos sensibles que publiquemos.
- C. Quién puede ver nuestras publicaciones.

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



5. Si queremos mejorar la seguridad y privacidad de nuestra cuenta en una red social, la mejor opción es:

- A. Utilizar una contraseña robusta.
- B. Poner nuestro perfil en privado.
- C. Ambas opciones.

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



6. Ante un caso de suplantación de identidad en una red social, deberemos:

- A. Denunciarlo a la red social y a las Fuerzas y Cuerpos de Seguridad.
- B. Denunciarlo a la red social y confrontar al usuario.
- C. Confrontar al usuario pues las redes sociales no ayudan.

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



7. De las siguientes opciones, ¿cuál es la mejor para comenzar a construir nuestra contraseña?

- A. Números.
- B. Nuestro cumpleaños.
- C. Una combinación de palabras.

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



8. ¿Cuál de las siguientes opciones es la menos efectiva para identificar una app maliciosa?

- A. Comprobar los comentarios de otros usuarios.
- B. Ver si permite los micropagos.
- C. Analizar los permisos que solicita.

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



9. El derecho que nos permite solicitar la supresión o eliminación de los datos publicados en Internet se conoce como:

- A. Oposición.
- B. Rectificación.
- C. Cancelación.

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



10. Antes de subir nuestros archivos a la nube, una medida de seguridad es:

- A. Eliminarla de nuestro dispositivo.
- B. Subir solo la información no personal.
- C. Cifrar la información.



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Gracias por vuestra atención



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



TU AYUDA EN
CIBERSEGURIDAD
incibe_



Oficina
de Seguridad
del Internauta

LICENCIA DE CONTENIDOS

La presente publicación pertenece a Instituto Nacional de Ciberseguridad (INCIBE) y está bajo licencia Reconocimiento-No Comercial-CompartirIgual 4.0 Internacional de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento.** El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa a INCIBE y su sitio web: <https://www.incibe.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial.** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- **Compartir Igual.** Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



TU AYUDA EN
CIBERSEGURIDAD
incibe_



Oficina
de Seguridad
del Internauta