



INSTITUTO NACIONAL DE CIBERSEGURIDAD

# “Aprendiendo ciberseguridad en tiempos de confinamiento”

---

Ruth García Ruiz

 <p>GOBIERNO DE ESPAÑA</p>	<p>VICEPRESIDENCIA TERCERA DEL GOBIERNO MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL</p>	<p>SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL</p>
---	---	---



TU AYUDA EN CIBERSEGURIDAD  
incibe\_



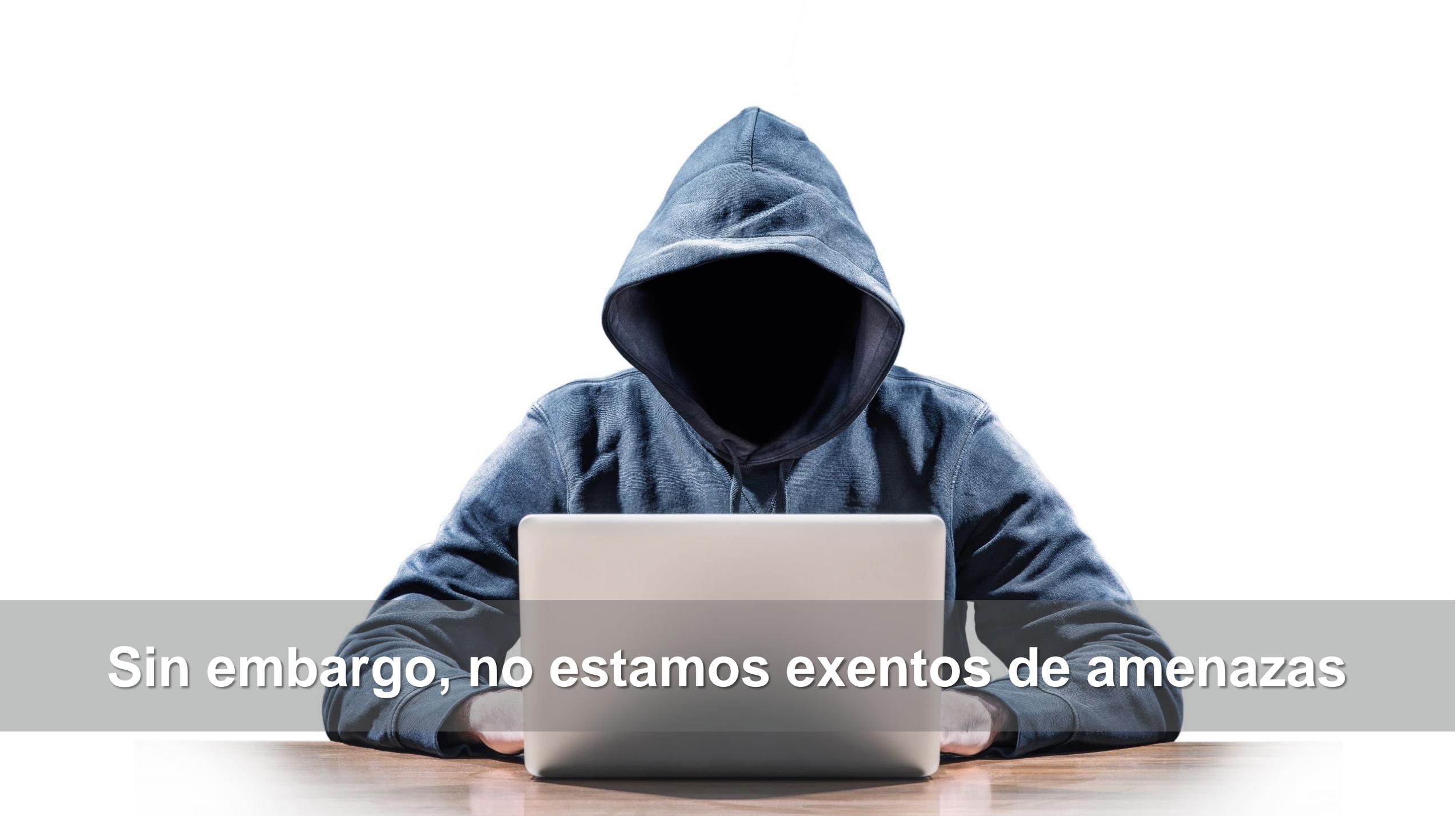
**Pongámonos en contexto antes de empezar**



**Vivimos en una sociedad digital hiperconectada**

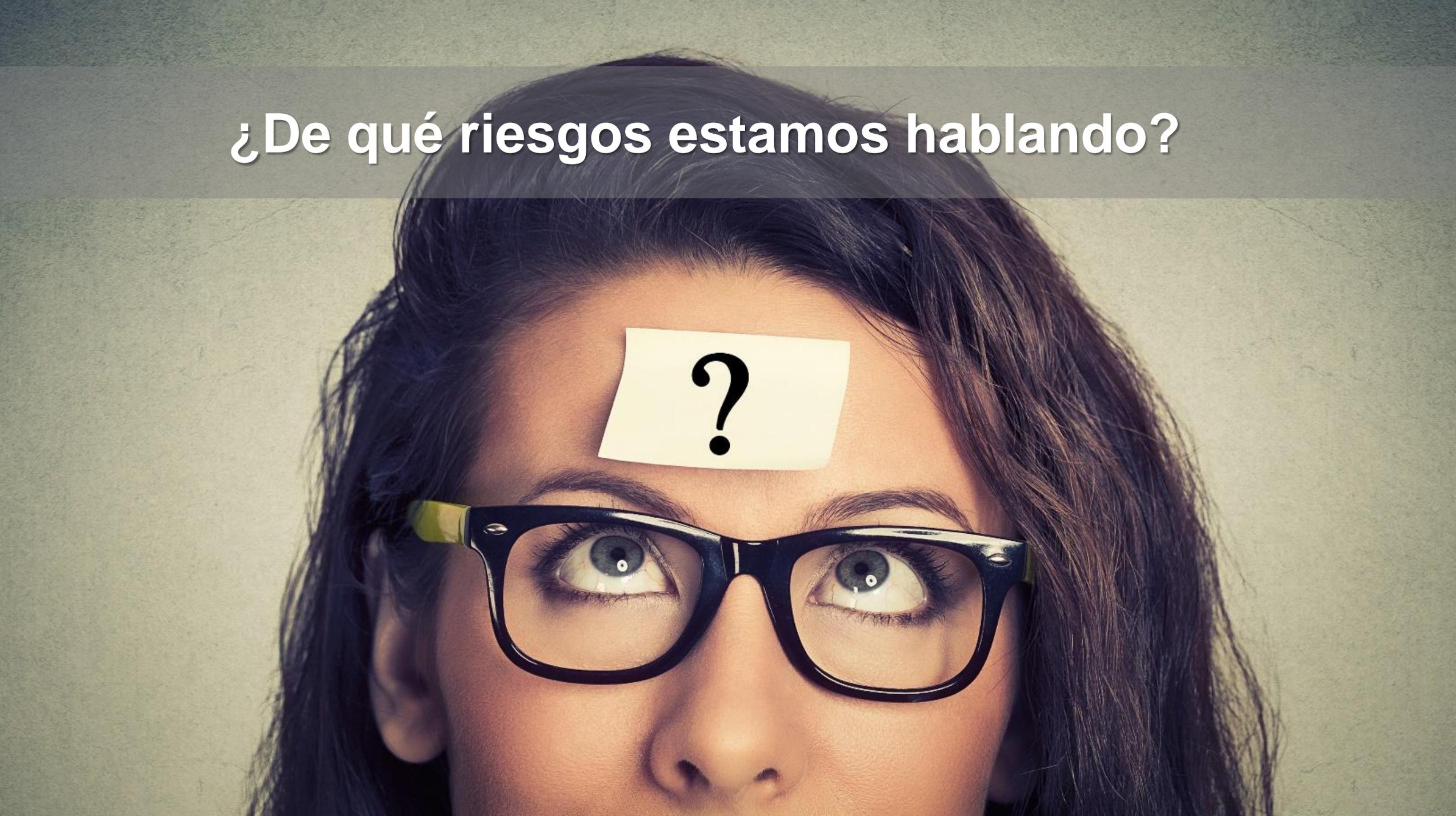


**Aparentemente todo son beneficios**

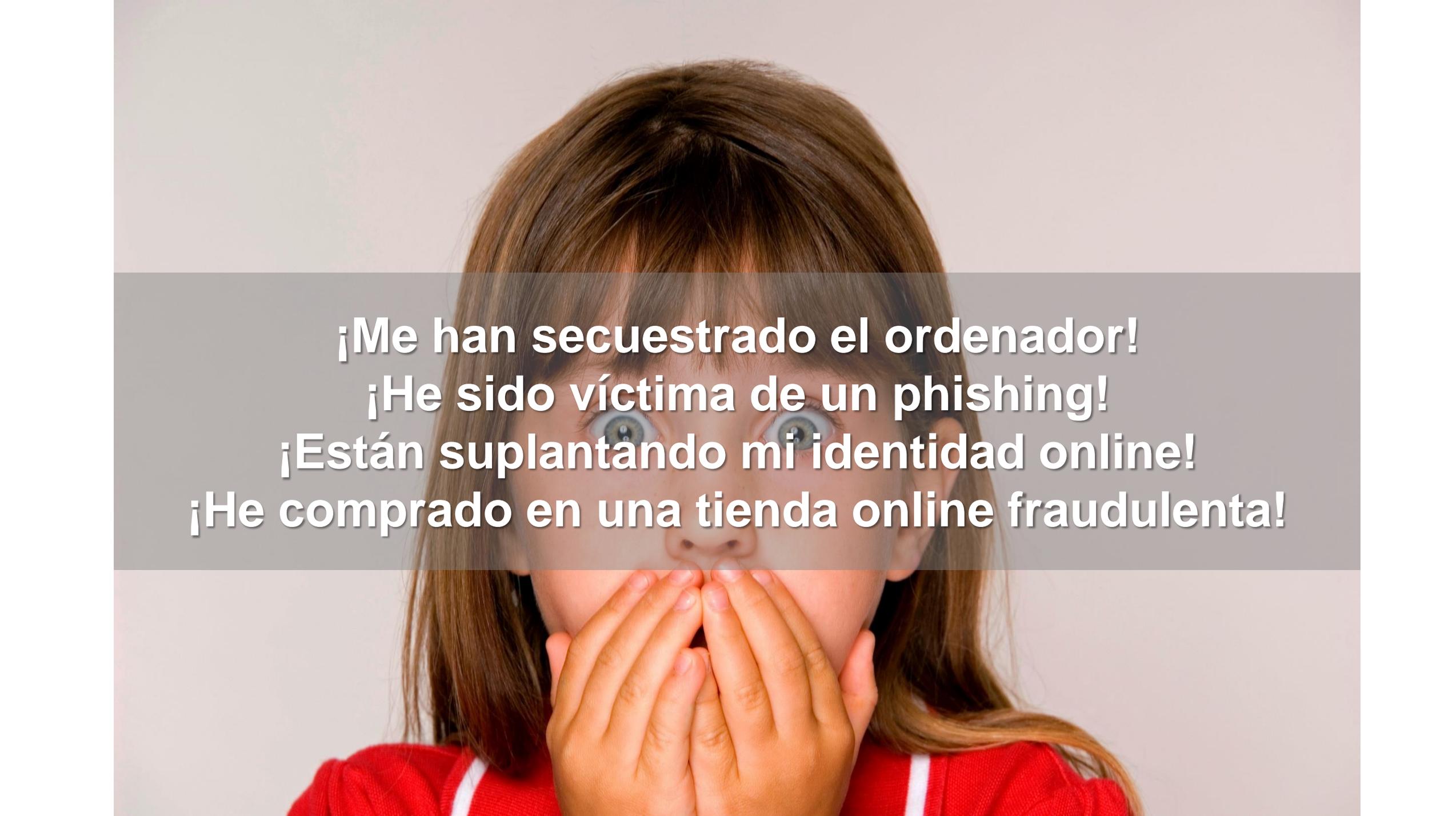
A person wearing a blue hoodie is sitting at a wooden desk, looking at a silver laptop. The person's face is completely obscured by the dark interior of the hoodie, symbolizing anonymity and hacking. The background is plain white.

**Sin embargo, no estamos exentos de amenazas**

¿De qué riesgos estamos hablando?

A close-up photograph of a woman with long, dark, wavy hair and blue eyes. She is wearing black-rimmed glasses. A small, rectangular piece of white paper is stuck to her forehead, featuring a large, bold black question mark. The background is a plain, light-colored wall.

?



**¡Me han secuestrado el ordenador!**  
**¡He sido víctima de un phishing!**  
**¡Están suplantando mi identidad online!**  
**¡He comprado en una tienda online fraudulenta!**



# ¿Qué vamos a aprender hoy?

- 
- **Cómo evitar virus, fraudes y desinformación**
  - **Cómo preparar un entorno de teletrabajo seguro**
  - **Cómo proteger nuestra privacidad, identidad digital y reputación online**



# Stop virus y fraudes

## **PREGUNTA: ¿Sabes qué es el phishing?**

1. El nombre por el que se conoce técnicamente a los virus y fraudes online.
2. Un tipo de virus que se descarga al visitar una página web maliciosa.
3. Un fraude que consiste en suplantar a alguna entidad o servicio con el fin de engañar al usuario con algún fin.

## Formulario de reembolso.

Interfaz de reembolso de la Tesorería General de la Seguridad Social.

Nº de referencia ES-A80105W  
Importe 345,76 €

\* Apellidos y nombre o razón social

\* NIF o NIE

Al marcar la casilla, usted a

## Formulario de reembolso.

Interfaz de reembolso de la Tesorería General de la Seguridad Social.

Apellidos y nombre o razón social

NIF o NIE

\* Numero de la tarjeta

\* Fecha de caducidad  /

\* Criptograma

Tarjetas admitidas  
VISA MasterCard

Siguiente »

# Phishing

De: Seguridad Social  
Enviado: miércoles, 29 de abril de 2020 3:54  
Para:   
Asunto: Se le envía un reembolso de Seguridad Social.

### Estimado Cliente.

Se le envía un reembolso de Seguridad Social.

Importe : **345,76 €**  
Referencia : **ES-A80105W**

Nuestro sistema de gestión de facturas detecta que tiene derecho a recibir este pago.  
Para aceptar pagos rápidos en línea, haga clic en el siguiente enlace y guarde la información de ree  
[https://sede.seg-social.gob.es/wps/GNFcfIAA\\_0buo!/L2dFBOSEh/](https://sede.seg-social.gob.es/wps/GNFcfIAA_0buo!/L2dFBOSEh/)

Por razones de seguridad y protección, tenga en cuenta que este documento web es temporalment  
el 10/05/2020.

Sinceramente,  
-----  
Tesorería General de la Seguridad Social.

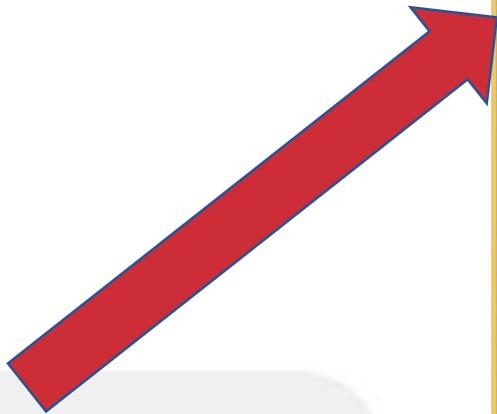
No responda a este correo electrónico, este buzón no se supervisa. Por lo tanto, no recibe una respuesta.

La Seguridad Social no te ha enviado ningún reembolso por correo electrónico

# Smishing

13:23

Hola, en relacion con la pandemia COVID19, el Estado destina 350-700 euros a sus ciudadanos.  
[https://\[redacted\].es](https://[redacted].es)



A screenshot of a web browser displaying a phishing website. The browser's address bar shows the URL 'estado2020.es/obtener-ayuda.html' and a warning icon with the text 'No es seguro'. The website header includes the Spanish flag and the text 'Fondo de Asistencia Financiera a Ciudadanos Españoles en la Lucha contra COVID-19'. A navigation menu contains 'ESTADO', 'QUIÉNES SOMOS', 'PREGUNTAS FRECUENTES', and a red button labeled 'OBTENER AYUDA'. A red arrow points from the SMS message to the 'OBTENER AYUDA' button. Below the navigation is a large heading 'OBTENER AYUDA' and a sub-heading 'Condicion... obtener ay...'. A modal form titled 'Tarjeta para inscribirse' is overlaid on the page, containing input fields for 'Número de tarjeta', 'Fecha de caducidad', and 'CVV', along with an 'ENVIAR' button. A red arrow points from the 'OBTENER AYUDA' button to this form. The background of the website shows a person's hands holding a document.

Identificados SMS fraudulentos con enlace a una web para solicitar una supuesta ayuda económica de entre 350 y 700 euros

## Páginas fraudulentas

¡Solo por hoy! 50% de  
Descuento en Mascarillas  
Sanitarias de Seguridad  
de 3 Capas\*

Nivel de existencias : **Bajo**



★★★★★ | Concha |

Hace 1 día

Más vale prevenir y  
hacer acopio ahora que aún se pueden  
comprar a que te pille el toro en unos  
meses y ya sean imposibles de  
conseguir.

¡Solo por hoy! 50% de Descuento en Mascarillas Sanitarias de Seguridad de 3 Capas\*

Nivel de existencias : **Bajo** (en stock\*)

\*Solo 8 quedan en stock!



ÚLTIMA OPORTUNIDAD

**50%**  
Descuento

Último día disponible para esta Oferta

¡Activa tu Cupón del 50% de Descuento!

- Promoción válida sólo por hoy  
- Sujeto a disponibilidad de stock

Mascarillas X

Compra en España las mascarillas  
con la máxima protección contra  
el Coronavirus COVID 19

VER MASCARILLAS

[Identificadas páginas fraudulentas de venta de mascarillas y otros materiales sanitarios](#)

# Malware

Realize el test de autoevaluación Covid19 <http://xxxxx xxxxxx.net>

**Situación de COVID-19 en España**  
[Actualizado a 3 de mayo de 2020 a las 21:00 horas]  
Basada en la notificación diaria de casos agregados de COVID-19 al Ministerio de Sanidad

GOBIERNO DE ESPAÑA  
MINISTERIO DE SANIDAD  
MINISTERIO DE CIENCIA E INNOVACIÓN

Instituto de Salud Carlos III

**CASOS TOTALES (PCR+)** 218011

Casos últimas 24h (PCR+) 356

Recuperados 121343

Fallecidos 25428

**Haz tu autoevaluación del COVID-19**

Evalúa tu salud y recibe instrucciones y recomendaciones sobre el COVID-19 con la aplicación oficial del Gobierno de España, en cooperación con las Comunidades Autónomas adheridas, por el momento: Cantabria, Canarias, Castilla-La Mancha, Extremadura e Islas Baleares.

Realiza esta autoevaluación sólo si crees que tienes síntomas. El Ministerio de Sanidad es responsable del tratamiento de los datos y su finalidad es sanitaria.

**ENTENDIDO. REALIZAR AUTOEVALUACIÓN**

**Casos por CCAA**

CCAA	Total	Ult.24h	inc.14d
Andalucía	12194	19	14.24
Aragón	5188	24	40.48
Principado de Asturias	2306	1	12.22
Islas Baleares	1908	0	13.83
Canarias	2225	4	7.34
Cantabria	2206	1	40.10
Castilla y León	17334	51	106.40
Castilla La Mancha	16050	33	65.18
Cataluña	50366	132	113.22
Galicia	9011	44	55.68
C. Valenciana	10436	0	14.55
Extremadura	2849	5	14.70
Comunidad de Madrid	62395	1	69.23

**Statística**

Casos acumulados con PCR+ por fecha de notificación

Evolución diaria de COVID-19 en España según situación clínica

- Más información sobre la evolución de la pandemia de COVID-19 en España (Basada en la notificación diaria de casos agregados de COVID-19 al Ministerio de Sanidad).
- Informes COVID-19 del CNE (Basada en la notificación individualizada de casos de COVID-19).
- Vigilancia de la mortalidad diaria por todas las causas (MoMo).
- Más Información a tiempo real sobre el sistema MoMo.
- Página COVID-19 del Ministerio de Sanidad.

[SMS con enlace a una web para realizar una autoevaluación de COVID-19 que te descarga un malware](#)

# Aplicaciones maliciosas

La difusión de este tipo de aplicaciones generalmente se realiza a través de correos electrónicos que suplantan a entidades bancarias y contiene un enlace de descarga a la aplicación maliciosa.

Dichas apps aseguran tener la utilidad de facilitar un mapa para seguir la evolución del coronavirus.



[Detectadas aplicaciones maliciosas sobre la evolución del coronavirus](#)

# Sextorsión

**Correos electrónicos fraudulentos cuyo objetivo es extorsionar a los destinatarios con el envío a sus contactos de un supuesto vídeo íntimo con contenido sexual o con la infección de COVID19 a sus familiares.**

**En ambos casos, el ciberdelincuente amenaza con hacer efectiva su extorsión si no se realiza el pago de una determinada cantidad en bitcoins.**



iHola!

Soy un hacker que tiene acceso a su sistema operativo.  
También tengo pleno acceso a su cuenta.  
Llevo observándole desde hace unos meses.  
Su equipo se infectó con un malware cuando visitó un sitio web para adultos.  
Se lo explicaré mejor por si no está familiarizado con este tema.  
El troyano me da acceso y control total sobre el ordenador o cualquier otro dispositivo.  
Esto significa que puedo ver todo lo que aparece en su pantalla y encender la cámara y el micrófono sin que usted se de cuenta.  
También tengo acceso a todos sus contactos y mensajes.  
¿Por qué su antivirus no detecta el malware?  
Respuesta: mi malware dirige el controlador y actualizo sus firmas cada 4 horas para que el antivirus se mantenga en silencio.  
He grabado un vídeo en el que sale usted satisfaciéndose en la parte izquierda de la pantalla y en la parte derecha se puede ver el vídeo que está mirando.  
Con un solo clic puedo enviar este vídeo a todos sus contactos de correo electrónico y de las redes sociales.  
También puedo publicar el acceso en todos sus mensajes de correos electrónico y de messenger.  
Si quiere evitarlo,  
transfiera 1000 \$ a mi dirección bitcoin (si no sabe cómo hacerlo, escriba en Google: "Comprar bitcoins").  
Mi dirección bitcoin (monedero de bitcoin) es: xxxxxxxxxxxxxxxvGCHxxxxxxxxvJBww  
Una vez que haya recibido el pago, borraré el vídeo y no volverá a saber nada de mí.  
Le doy 50 horas (más de 2 días) para pagar.  
Cuando lea esta carta recibiré un aviso y el temporizador se pondrá en marcha.  
Presentar una denuncia no tiene sentido porque este correo electrónico no puede ser rastreado, al igual que mi dirección de correo electrónico.  
Yo no cometo errores.  
Si descubro que ha compartido este mensaje con alguien más, el vídeo se distribuirá inmediatamente.



[Detectada oleada de falsos correos de sextorsión o infección de COVID19](#)

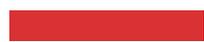


1. Remitente
2. Asunto
3. Objetivo del mensaje
4. Redacción
5. Enlaces
6. Adjuntos



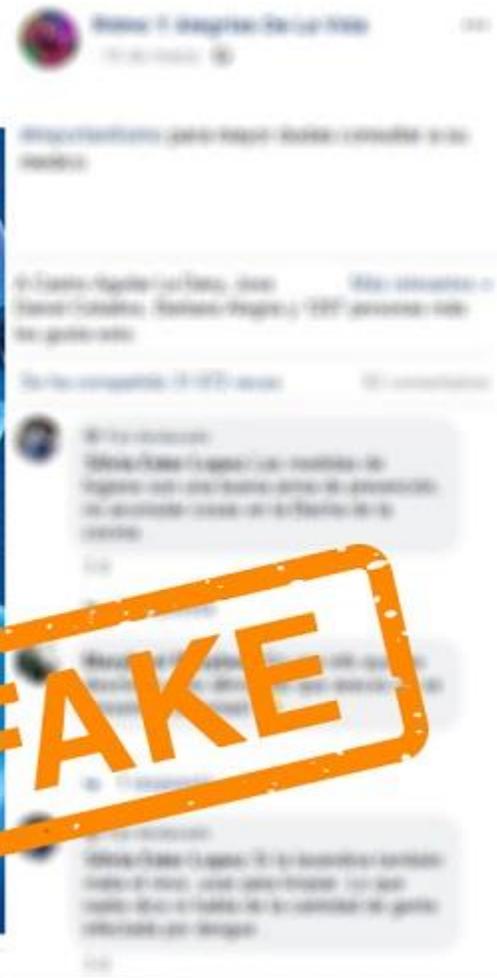
[Cómo identificar un correo electrónico malicioso](#)

## Bulos y fake news



### Evitemos más muertes

El Coronavirus antes de llegar a los pulmones permanece en la garganta durante cuatro días y en este momento la persona comienza a toser y a tener dolores de garganta. Si bebe mucha agua y hace gárgaras con agua tibia y sal o vinagre, elimina el virus. Difunda esta información porque puede salvar a alguien con esta información.



# Ponle freno a los bulos y hoax



- Busca la fuente y contrasta
- Revisa la URL
- Mira más allá del titular
- Comprueba el formato
- Aplica el sentido común



- 
- Maldito Bulo
  - Newtral
  - Snopes
  - Google Fact check tools

[¿Qué podemos hacer para detectarlos y prevenirlos?](#)



# ¿Te toca teletrabajar?



**PREGUNTA:** ¿qué aspectos consideras que son esenciales configurar?

1. Antivirus + actualizaciones de seguridad + cuentas de usuario
2. Copias de seguridad + cifrado de la información
3. Configuración router wifi
4. Todas las respuestas anteriores son correctas

# Creando un espacio de trabajo seguro

Identifica cada elemento y aplica estos consejos para garantizar la seguridad de la información de tu empresa.

## COPIAS DE SEGURIDAD

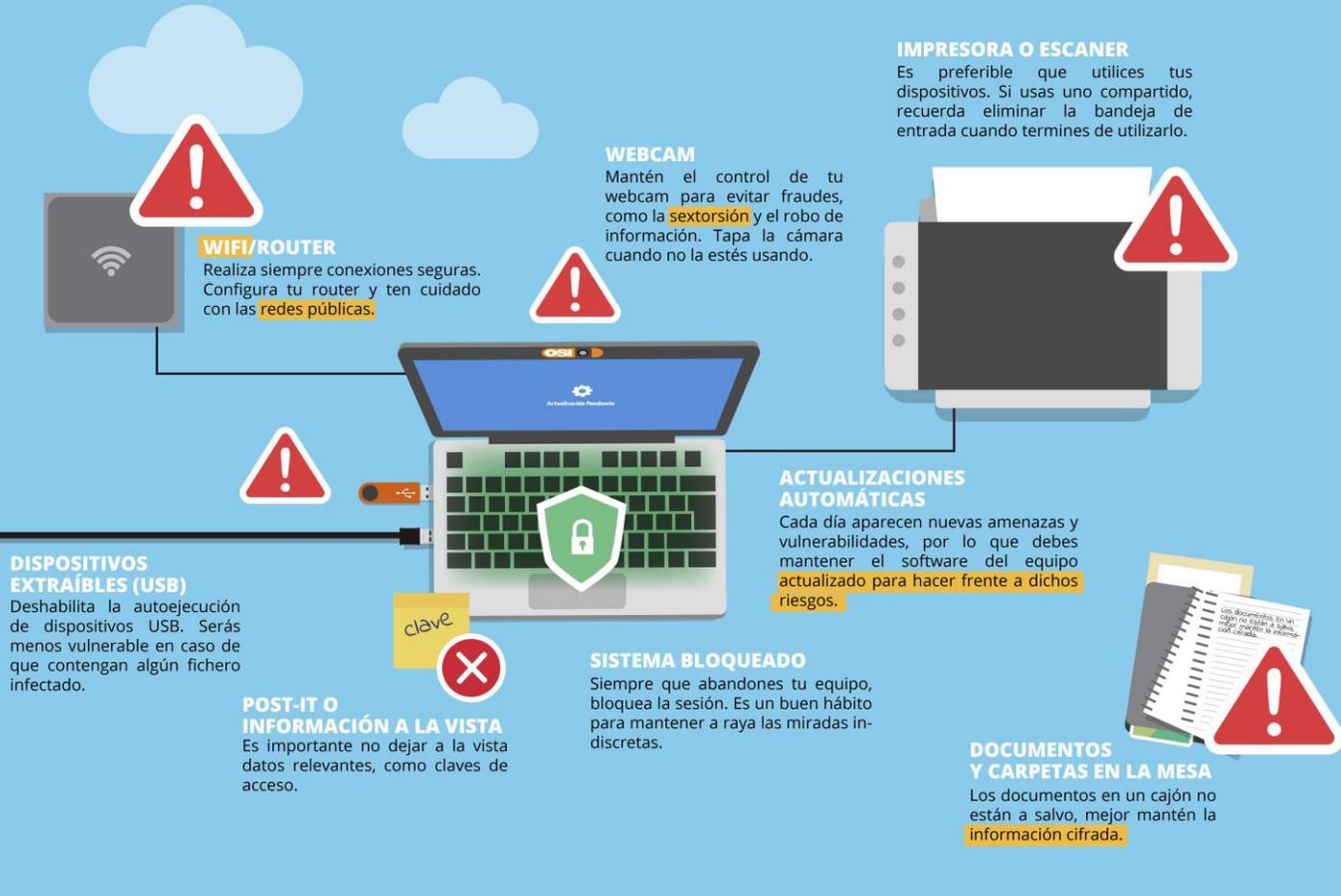
Te ayudan a proteger la información y a disponer de una versión de respaldo en caso de perder la original. Aplica la regla 3-2-1.

## DISPOSITIVOS IOT

Los dispositivos inteligentes son cada vez más comunes en las casas, pero si no están bien configurados pueden ser la puerta de entrada a una gran cantidad de amenazas.



#CiberCOVID19



VPN ON



## RED PRIVADA VIRTUAL (VPN)

Si tu empresa no te facilita ninguna VPN concreta para teletrabajar, te recomendamos que instales una para añadir una capa extra de seguridad a tus conexiones.

¡Sigue estas pautas y disfruta de un entorno de trabajo seguro!



GOBIERNO DE ESPAÑA

VICEPRESIDENCIA TERCERA DEL GOBIERNO  
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe

INSTITUTO NACIONAL DE CIBERSEGURIDAD



@INCIBE



INCIBE



@INCIBE



Mantente al día con nuestras campañas de concienciación para estar informado.

¡Es nuestra mejor defensa!

[www.incibe.es](http://www.incibe.es) | [www.osi.es](http://www.osi.es)

OSI

Oficina de Seguridad del Internauta



@osiseguridad



osiseguridad

# Pon a punto tu dispositivo para trabajar con él



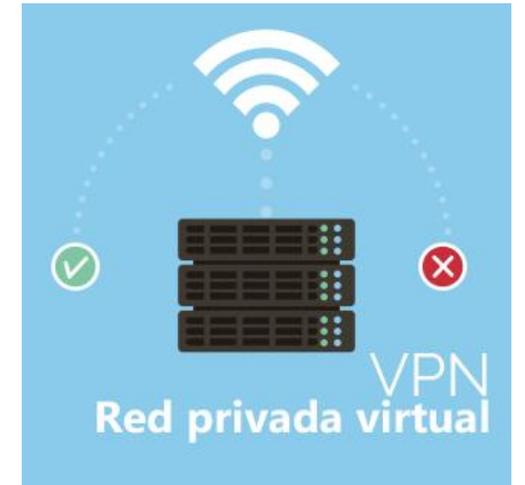
Instala una herramienta antivirus



Actualiza el sistema operativo así como el resto de programas



Crea una cuenta de usuario diferente



Instala un Red Privada Virtual (VPN)

## Haz copias de seguridad

# 5 Razones

por las que hacer copias de seguridad

COPIANDO 75%

Todos tenemos información que queremos **proteger, guardar y preservar en el tiempo**. Para ello, lo mejor es crear copias de seguridad.

1 Estás prevenido en caso de deterioro del dispositivo

2 Proteges la información

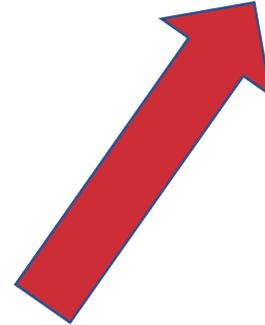
3 La preservas en el tiempo



4 Liberas espacio

5 La proteges de ti mismo

# Cifra la información

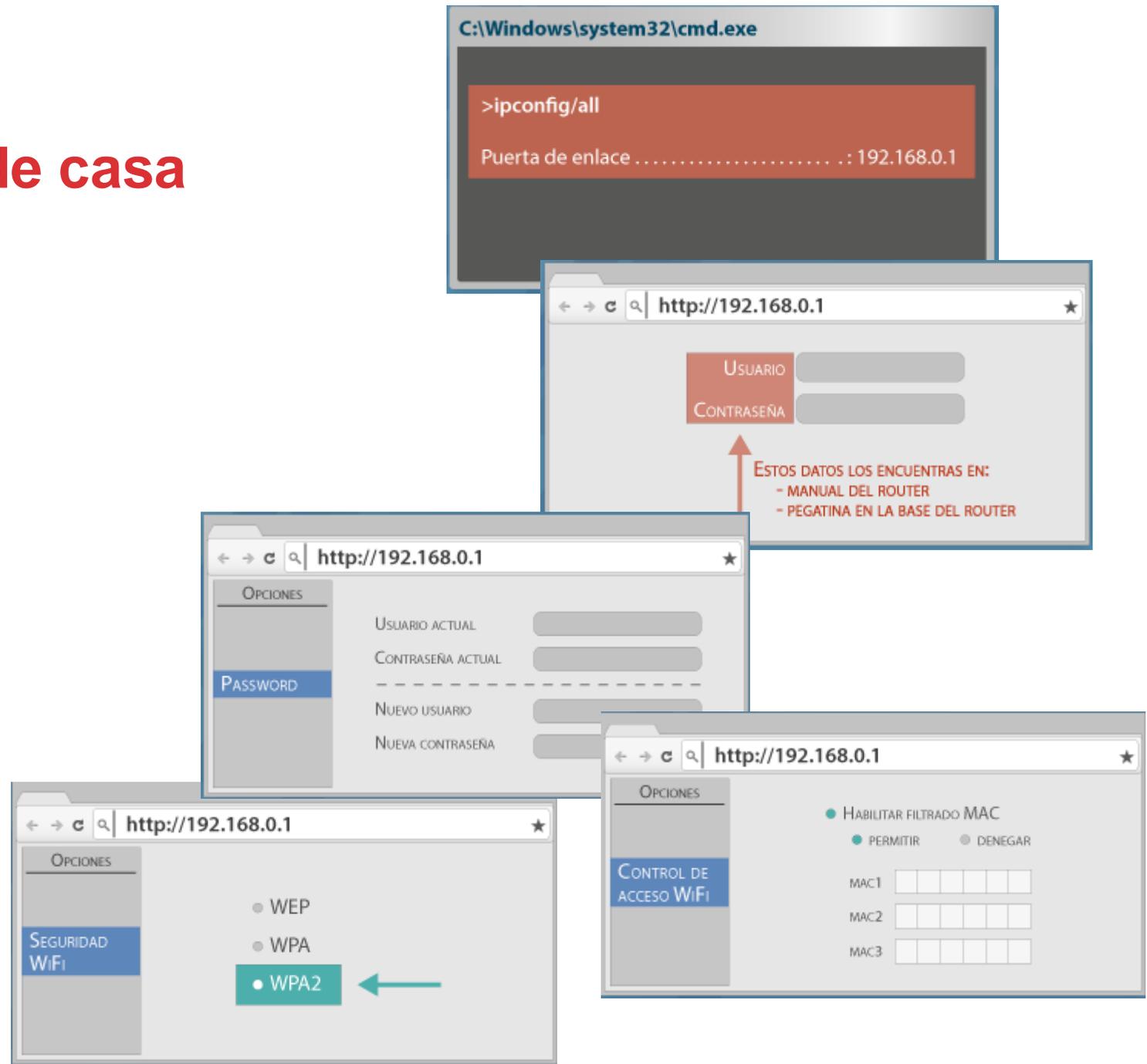


- Utiliza alguna herramienta específica. Ej: VerCrypt
- Apóyate en las opciones que incluyen los distintos sistemas operativos:
  - Windows 10: BitLocker
  - MAC OS: FileVault
  - iOS: cifrado por defecto.
  - Android: cifrado por defecto version 6 o superior. Adiantum para versiones inferiores.

Hacer que la información no sea accesible para aquellos que no están autorizados para leerla, modificarla o borrarla

# Configura tu router wifi de casa

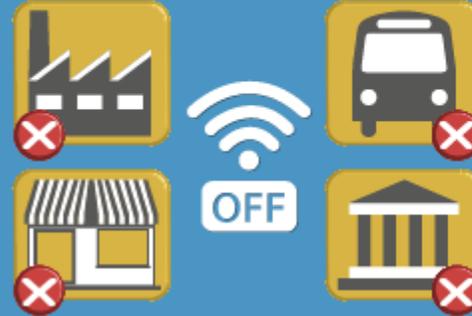
1. Cambia la contraseña de acceso a la configuración del router.
2. Actualiza la contraseña para conectarte a la red.
3. Asignar el sistema de seguridad WPA2.
4. Modifica el nombre de la wifi o SSID.
5. Habilita el filtrado por MAC (o dirección física).



# Sé cauto con las redes a las que te conectas



1. Evita la conexión automática y elimina los accesos a las redes WiFi una vez haya finalizado su uso.



2. Evita realizar compras online o intercambiar información sensible.



3. Comprueba que la red gratuita disponible es la oficial del lugar en el que estás.



4. ¡En cualquier lugar público hay mirones! Protege tu pantalla de miradas indiscretas.



5. Sé precavido y mantén actualizados tus dispositivos y sus aplicaciones.



6. Siempre que estén disponibles, conéctate a páginas con certificado de seguridad, con https://



## Y de manera adicional...



[Buenas prácticas ciberseguras](#)



# Ahora más que nunca, cuida tu privacidad, identidad y reputación online

## **PREGUNTA:** ¿Sabes qué es la identidad digital?

1. Es la información que Internet muestra sobre nosotros y que voluntariamente hemos compartido en Internet.
2. Es la información que sobre nosotros se sube a Internet, tanto por nosotros mismos, como por amigos, familiares, compañeros o cualquier otra persona.
3. Es la información que está disponible en Internet sobre nosotros y que ha sido compartida por familiares, amigos y conocidos.



**¿Qué pasa con tu privacidad online?**



pau\_eche

Seguir

7,318 publicaciones 2.9m seguidores 1,004 seguidos

Paula Echevarria  
Change is the only constant... 🌍es  
Contacto: ana@anatenorio.com  
[www.paulaechevarria.com](http://www.paulaechevarria.com)

# ¿Cuánta información existe sobre ti en Internet?

Friends

MamiDani...

Food

TRAVEL

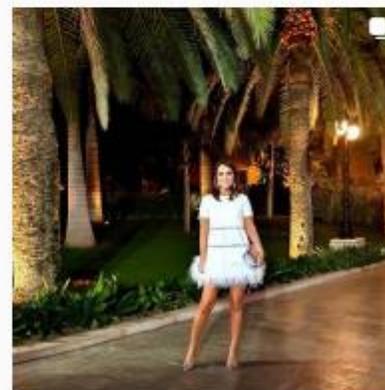
Family

Música

Training

PUBLICACIONES

ETIQUETADAS





¿Tienes una identidad digital positiva?



¿Configuras adecuadamente tus perfiles?

A close-up photograph of a woman with long brown hair, wearing a light-colored top, looking down at her smartphone. Overlaid on the image are three white speech bubble icons: one with a person icon and '4k', one with a red heart icon and '5k', and one with a blue speech bubble icon and '11'. A semi-transparent grey banner at the bottom contains the text '¿Quiénes son tus contactos online?'.

¿Quiénes son tus contactos online?

A woman with dark hair, wearing a bright pink long-sleeved shirt, is lying on her back on a bed with white patterned bedding. She is holding a smartphone in her right hand, positioned high above her head as if taking a selfie. Her left hand is near her face. The scene is dimly lit, suggesting an indoor setting at night.

**¿Conoces los riesgos asociados al sexting?**

We Are  
here to  
—help—



# Oficina de Seguridad del Internauta



# Oficina de Seguridad del Internauta



Información y actualidad

Campañas de concienciación temáticas



#OSlavis

Avisos de seguridad



Blog  
Historias reales



Los ciberdelincuentes, ¿quiénes son?



Dispositivos móviles



IoT, los riesgos de un mundo hiperconectado



Redes Sociales



¡Contraseñas seguras!



VICEPRESIDENCIA  
TERCERA DEL GOBIERNO  
MINISTERIO  
DE ASUNTOS ECONÓMICOS  
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO  
DE DIGITALIZACIÓN  
E INTELIGENCIA ARTIFICIAL



# Oficina de Seguridad del Internauta



## Servicios de soporte



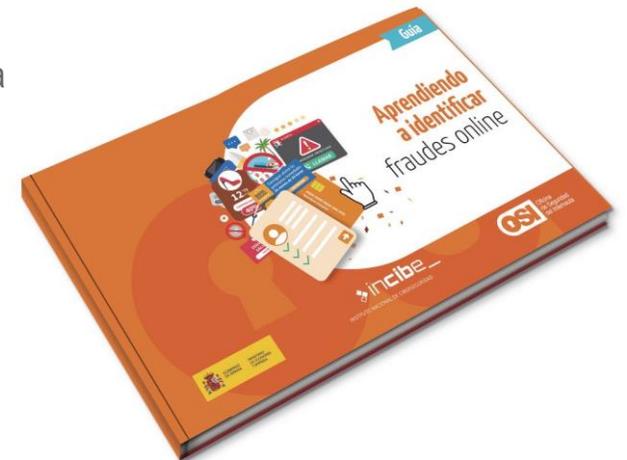
**OSi** Oficina de Seguridad del Internauta  
Servicio **ANTIBOTNET**



Guías, videotutoriales para configurar la **PRIVACIDAD** y **SEGURIDAD**:



Conan mobile





¿Sigues necesitando ayuda?

# Línea de ayuda en ciberseguridad





INSTITUTO NACIONAL DE CIBERSEGURIDAD

# Gracias por tu atención.

---



GOBIERNO  
DE ESPAÑA

VICEPRESIDENCIA  
TERCERA DEL GOBIERNO  
MINISTERIO  
DE ASUNTOS ECONÓMICOS  
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO  
DE DIGITALIZACIÓN  
E INTELIGENCIA ARTIFICIAL



TU AYUDA EN  
CIBERSEGURIDAD  
incibe\_